

Uso de OpenAPI para recuperar información sobre políticas de ISE en ISE 3.3

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración en ISE](#)

[Ejemplos de Python](#)

[Device Admin - Lista De Conjuntos De Políticas](#)

[Device Admin - Obtener reglas de autenticación](#)

[Device Admin - Obtener reglas de autorización](#)

[Acceso A La Red: Lista De Conjuntos De Políticas](#)

[Acceso a la red - Obtener reglas de autenticación](#)

[Acceso a la red - Obtener reglas de autorización](#)

[Troubleshoot](#)

Introducción

Este documento describe el procedimiento para utilizar OpenAPI para administrar Cisco Identity Services Engine (ISE) Política.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

- ISE 3.3
- Python 3.10.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

A partir de Cisco ISE 3.1, las API más recientes están disponibles en el formato OpenAPI. La política de gestión optimiza la seguridad y la gestión de la red al mejorar la interoperabilidad, mejorar la eficacia de la automatización, reforzar la seguridad, fomentar la innovación y reducir los costes. Esta política permite que ISE se integre sin problemas con otros sistemas, logre una configuración y gestión automatizadas, proporcione un control de acceso granular, fomente la innovación por parte de terceros y simplifique los procesos de gestión, reduciendo así los costes de mantenimiento y aumentando el retorno de la inversión general.

Configurar

Diagrama de la red



Topología

Configuración en ISE

Paso 1. Agregue una cuenta de administrador OpenAPI.

Para agregar un administrador de API, vaya a Administración > Sistema > Acceso de administrador > Administradores > Usuarios de administración > Agregar.

La captura de pantalla muestra la interfaz de usuario de Cisco ISE. El menú lateral izquierdo incluye 'Administration' (destacado con un cuadro rojo), 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Work Centers' y 'Interactive Help'. El menú superior incluye 'Identity Services Engine', 'Administration / System' (destacado con un cuadro rojo), 'License Warning', 'Search', 'Notifications' y 'User'. La sección central titulada 'Administrators' muestra una lista de usuarios de administración. Los usuarios listados son:

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

Administrador de API

Paso 2. Habilite OpenAPI en ISE.

API abierta está desactivada de forma predeterminada en ISE. Para activarla, vaya a Administration > System > Settings > API Settings > API Service Settings. Active o desactive las opciones de OpenAPI. Haga clic en Guardar.

The screenshot shows the 'API Settings' page in the Cisco ISE web interface. The 'API Service Settings' tab is active. In the 'API Service Settings for Primary Administration Node' section, the 'Open API (Read/Write)' toggle button is highlighted with a red box. In the 'API Service Setting for All Other Nodes' section, the 'Open API (Read)' toggle button is also highlighted with a red box. At the bottom right, there are 'Reset' and 'Save' buttons.

Habilitar OpenAPI

Paso 3. Explore ISE OpenAPI.

Vaya a Administration > System > Settings > API Settings > Overview. Haga clic en OpenAPI para visitar el enlace.

The screenshot shows the 'API Settings' page in the Cisco ISE web interface. The 'Overview' tab is active. The 'API Services Overview' section contains text about ERS and OpenAPI services. It mentions that both services are disabled by default and provides links to ERS_V1 documentation and the OpenAPI Swagger UI. The 'ERS APIs' link is highlighted with a red box.

Visite OpenAPI

Ejemplos de Python

Device Admin - Lista De Conjuntos De Políticas

Esta API recupera información de conjuntos de políticas de administración de dispositivos.

Paso 1. Información necesaria para una llamada de API.

Método	GET
URL	<a href="https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set">https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set
Credenciales	Utilice las credenciales de la cuenta OpenAPI.
Encabezados	Aceptar : Aplicación/JSON Tipo de contenido : Aplicación/JSON

Paso 2. Localice la URL que se utiliza para recuperar la información de los conjuntos de políticas de administración de dispositivos.

The screenshot shows the Swagger UI for the Cisco ISE API - Policy. At the top, there is a dropdown menu labeled "Select a definition" with "Policy" selected. Below the header, the title "Cisco ISE API - Policy" is displayed along with its version "1.0.0" and "OAS3". A "Servers" dropdown shows the URL "https://10.106.33.92:44240/api/v3/api-docs?group=Policy". On the right side, there is a green "Authorize" button with a lock icon. The main content area lists various API endpoints under "device-admin-api-controller" and "network-access-api-controller". Under "Device Administration", several sections are listed: "Command Sets", "Conditions", "Dictionary Attributes List", "Identity Stores", "Network Conditions", and "Policy Sets". The "Policy Sets" section is highlighted with a red box. Below it, a blue box highlights the "GET /api/v1/policy/device-admin/policy-set" endpoint, which is described as "Device Admin - List of policy sets".

URI DE API

Paso 3. Este es un ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP de ISE, el nombre de usuario y la contraseña. Guardar como archivo python para ejecutar.

Garantizar una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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/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())

```

Este es el ejemplo de resultados esperados.

```
Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{ 'default': True, 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'name': 'Default', 'desc': 'Default authentication policy set', 'rule': { 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'order': 1, 'type': 'Authentication', 'value': 'radius' } } ]}
```

DDevice Admin - Obtener reglas de autenticación

Esta API recupera las reglas de autenticación de un conjunto de políticas determinado.

Paso 1. Información necesaria para una llamada de API.

Método	GET
URL	<a href="https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authentication">https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authentication
Credenciales	Utilice las credenciales de la cuenta OpenAPI.
Encabezados	Aceptar : Aplicación/JSON Tipo de contenido : Aplicación/JSON

Paso 2. Busque la dirección URL que se utiliza para recuperar la información de la regla de autenticación.

The screenshot shows the Cisco ISE API - Policy documentation page. At the top, there's a navigation bar with 'Swagger' and 'Select a definition' dropdown set to 'Policy'. Below the header, the title 'Cisco ISE API - Policy' is displayed with a version of '1.0.0 OAS3' and a link to 'https://10.106.33.92:44240/api/v3/api-docs?group=Policy'. A 'Servers' dropdown shows 'https://10.106.33.92:44240 - Inferred Url'. On the right, there's an 'Authorize' button with a lock icon.

The main content area lists various API endpoints under 'Device Administration' with expandable sections. One section, 'Device Administration - Authentication Rules', is highlighted with a red border. Below it, a specific endpoint is shown:

```

GET /api/v1/policy/device-admin/policy-set/{policyId}/authentication
Device Admin - Get authentication rules.

```

Below the endpoint details, a note says 'Device Admin - Get authentication rules.'

URI DE API

Paso 3. Este es un ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP de ISE, el nombre de usuario y la contraseña. Guardar como archivo python para ejecutar.

Garantizar una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de Python.

```
<#root>
```

```

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":
    url = ""

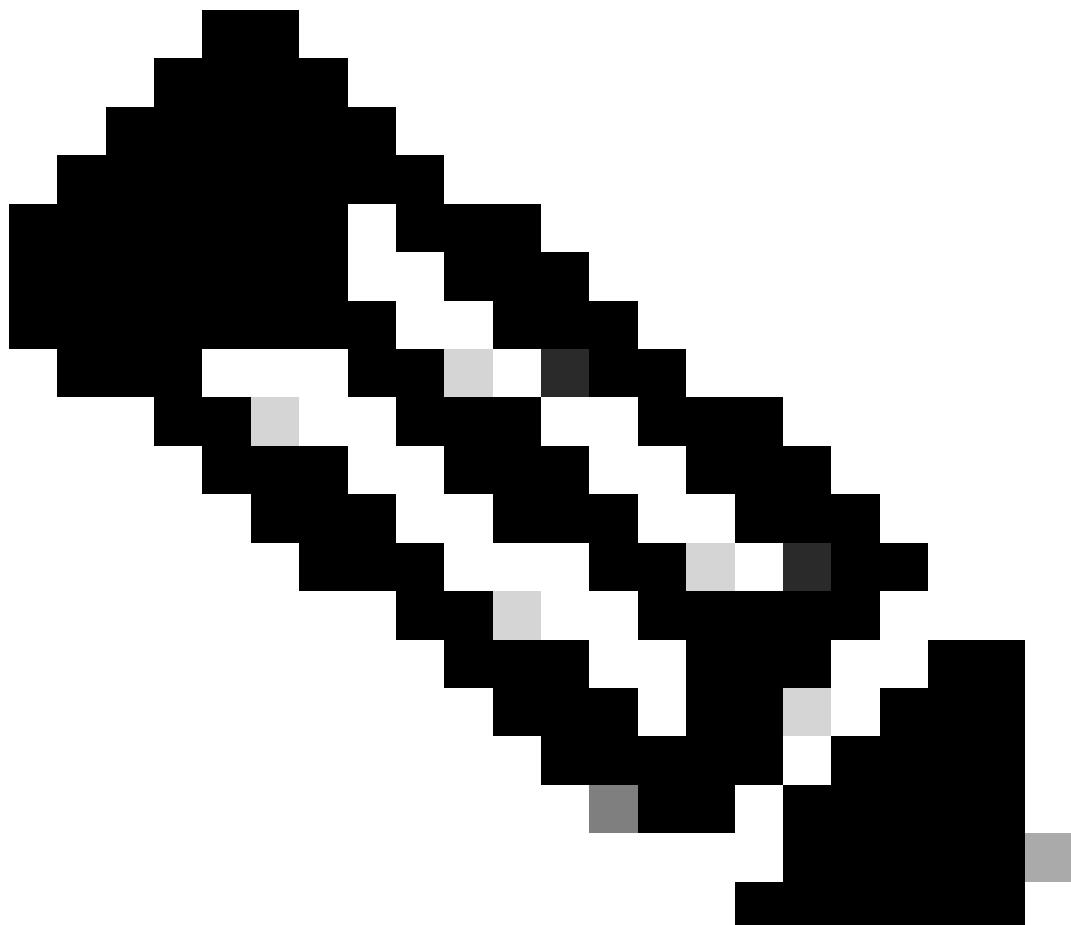
    https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authentication

    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())
```



Nota: El ID proviene de las salidas de la API en el paso 3 de Device Admin - List Of Policy Sets. Por ejemplo, 41ed8579-429b-42a8-879e-61861cb82bbf es un conjunto de políticas TACACS predeterminado.

Este es el ejemplo de resultados esperados.

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

Device Admin - Obtener reglas de autorización

Esta API recupera las reglas de autorización de un conjunto de políticas determinado.

Paso 1. Información necesaria para una llamada de API.

Método	GET
URL	<a href="https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authorization">https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authorization
Credenciales	Utilice las credenciales de la cuenta OpenAPI.
Encabezados	Aceptar : Aplicación/JSON Tipo de contenido : Aplicación/JSON

Paso 2. Busque la dirección URL que se utiliza para recuperar la información de la regla de autorización.

The screenshot shows the Cisco ISE API - Policy OpenAPI Specification (OAS) interface. At the top, it displays the title "Cisco ISE API - Policy" with version 1.0.0 and OAS3 status. Below the title, there is a "Servers" dropdown set to "https://10.106.33.92:44240" and an "Inferred Url" dropdown. A green "Authorize" button is visible. The main content area is organized into sections under "device-admin-api-controller": "network-access-api-controller", "Device Administration - Command Sets", "Device Administration - Conditions", "Device Administration - Dictionary Attributes List", "Device Administration - Identity Stores", "Device Administration - Network Conditions", "Device Administration - Policy Sets", "Device Administration - Authorization Global Exception Rules", "Device Administration - Authentication Rules", and "Device Administration - Authorization Rules". The "Device Administration - Authorization Rules" section is highlighted with a red box. Below this section, a "GET" method is listed with the endpoint "/api/v1/policy/device-admin/policy-set/{policyId}/authorization". A tooltip for this endpoint states "Device Admin - Get authorization rules." There is also a lock icon and a copy icon next to the endpoint.

URI DE API

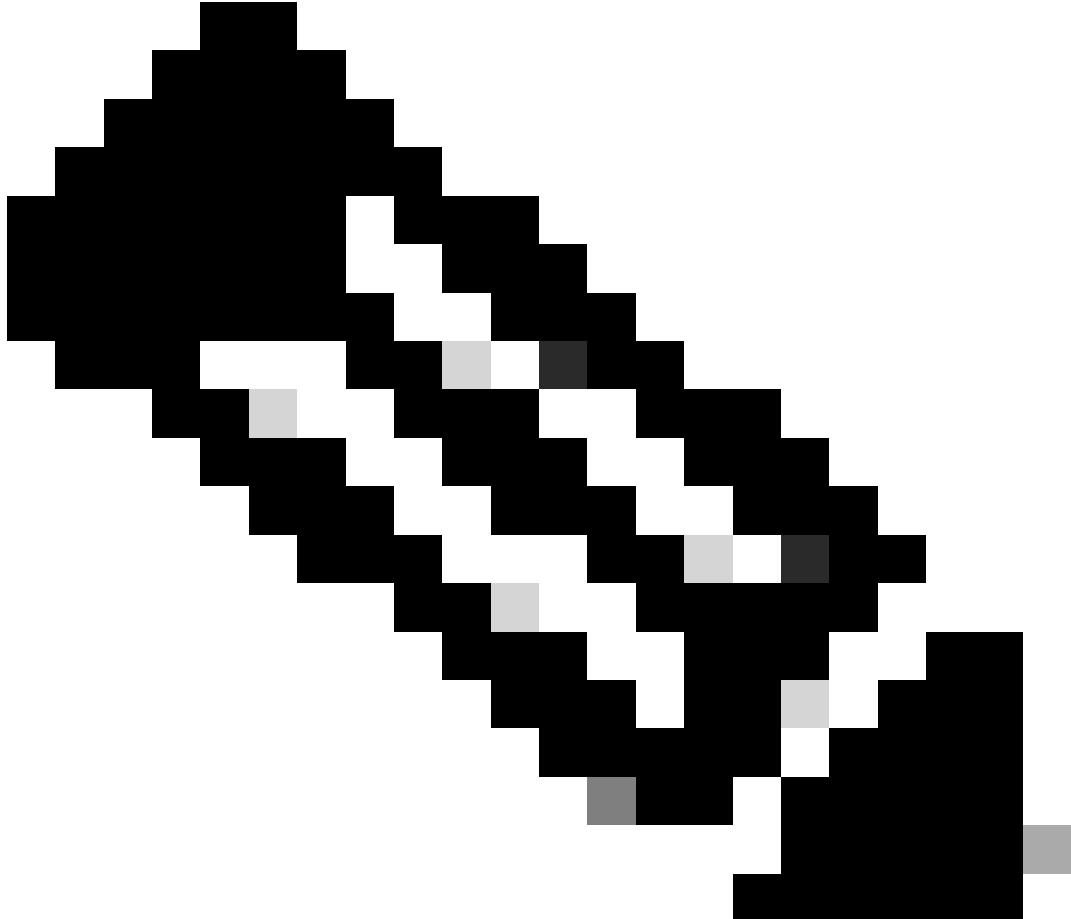
Paso 3. Este es un ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP de ISE, el nombre de usuario y la contraseña. Guardar como archivo python para ejecutar.

Garantizar una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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/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:")
```



Nota: El ID proviene de las salidas de la API en el paso 3 de Device Admin - List Of Policy Sets. Por ejemplo, 41ed8579-429b-42a8-879e-61861cb82bbf es un conjunto de políticas TACACS predeterminado.

Este es el ejemplo de resultados esperados.

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'}}

Acceso A La Red: Lista De Conjuntos De Políticas

Esta API recupera conjuntos de políticas de acceso a la red de implementaciones de ISE.

Paso 1. Información necesaria para una llamada de API.

Método	GET
URL	<a href="https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set">https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set
Credenciales	Utilice las credenciales de la cuenta OpenAPI.
Encabezados	Aceptar : Aplicación/JSON Tipo de contenido : Aplicación/JSON

Paso 2. Localice la URL que se utiliza para recuperar la información específica del nodo de ISE.

The screenshot shows a web interface for managing policy sets. At the top, there's a header bar with the title "Network Access - Policy Sets". Below it, a search bar contains the URL "https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set". To the left of the URL, the word "GET" is highlighted in blue. To the right, there's some small text about the endpoint. The main content area has a light blue background and contains the instruction "Get all network access policy sets.".

URI DE API

Paso 3. Este es un ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP de ISE, el nombre de usuario y la contraseña. Guardar como archivo python para ejecutar.

Garantizar una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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/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())

```

Este es el ejemplo de resultados esperados.

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

Acceso a la red - Obtener reglas de autenticación

Esta API recupera las reglas de autenticación de un conjunto de políticas determinado.

Paso 1. Información necesaria para una llamada de API.

Método	GET
URL	<a href="https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authentication">https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authentication
Credenciales	Utilice las credenciales de la cuenta OpenAPI.
Encabezados	Aceptar : Aplicación/JSON Tipo de contenido : Aplicación/JSON

Paso 2. Busque la dirección URL que se utiliza para recuperar la información de la regla de autenticación.

The screenshot shows a web interface for an API endpoint. The title bar says "Network Access - Authentication Rules". Below it, there's a blue button labeled "GET" and a red box highlights the URL field which contains the path "/api/v1/policy/network-access/policy-set/{policyId}/authentication". To the right of the URL, there's a small description: "Network Access - Get authentication rules." There are also some icons for expanding and locking the view.

URI DE API

Paso 3. Este es un ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP de ISE, el nombre de usuario y la contraseña. Guardar como archivo python para ejecutar.

Garantizar una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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/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())
```



Nota: El ID proviene de las salidas de la API en el paso 3 de Network Access - List Of Policy Sets (Acceso a red - Lista de conjuntos de políticas). Por ejemplo, ba71a417-4a48-4411-8bc3-d5df9b115769 es BGL_CFMEO2-FMC.

Este es el ejemplo de resultados esperados.

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

Acceso a la red - Obtener reglas de autorización

Esta API recupera las reglas de autorización de un conjunto de políticas determinado.

Paso 1. Información necesaria para una llamada de API.

Método	GET
--------	-----

URL	<a href="https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authorization">https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authorization
Credenciales	Utilice las credenciales de la cuenta OpenAPI.
Encabezados	Aceptar : Aplicación/JSON Tipo de contenido : Aplicación/JSON

Paso 2. Busque la dirección URL que se utiliza para recuperar la información de la regla de autorización.

URI DE API

Paso 3. Este es un ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP de ISE, el nombre de usuario y la contraseña. Guardar como archivo python para ejecutar.

Garantizar una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de Python.

```
<#root>

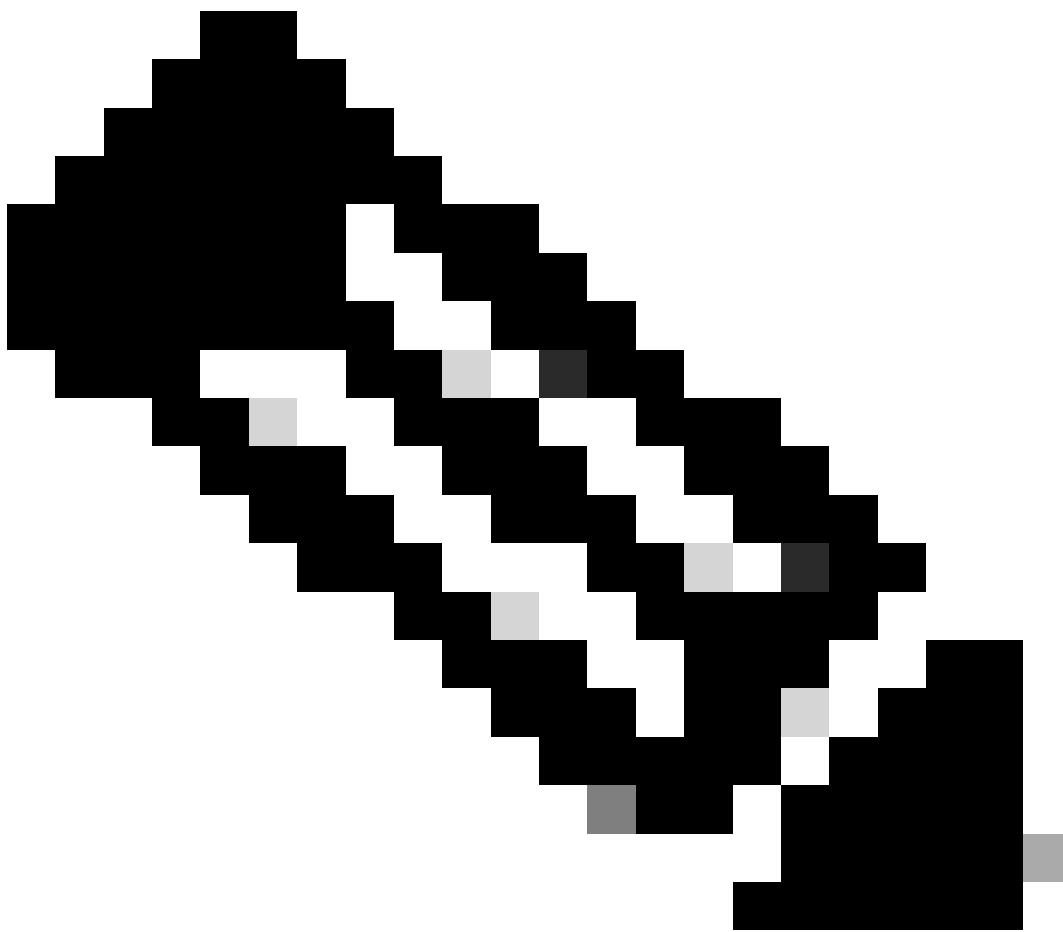
from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":
    url = ""

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



Nota: El ID proviene de las salidas de la API en el paso 3 de Network Access - List Of Policy Sets (Acceso a red - Lista de conjuntos de políticas). Por ejemplo, ba71a417-4a48-441-8bc3-d5df9b115769 es BGL_CFMEO2-FMC.

Este es el ejemplo de resultados esperados.

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

Troubleshoot

Para resolver problemas relacionados con las API abiertas, establezca el Nivel de registro para el componente apbservicecomponent en DEBUG en la ventana Configuración del registro de depuración.

Para habilitar la depuración, vaya a Operaciones > Solución de problemas > Asistente de depuración > Configuración del registro de depuración > Nodo ISE > apiservice.

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

Depuración del servicio API

Para descargar el archivo de registro de depuración, navegue hasta Operaciones > Solución de problemas > Descargar registros > ISE PAN Node > Registros de depuración.

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)		
	api-service (all logs)		208 KB
	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

Descargar registros de depuración

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).