

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

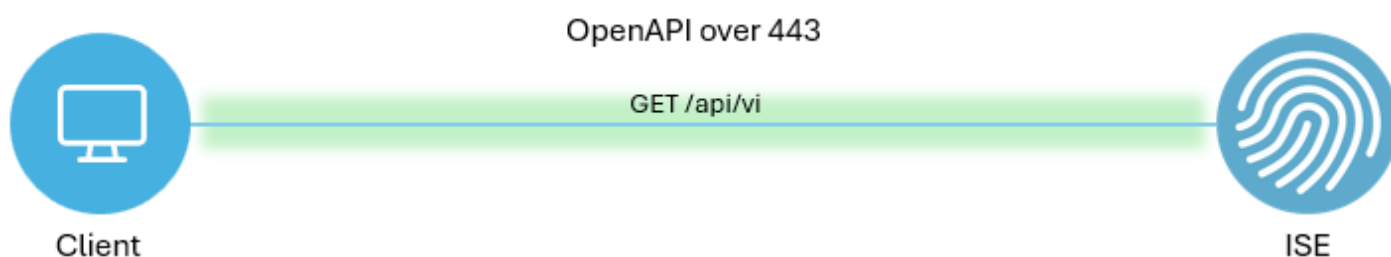
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

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.

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

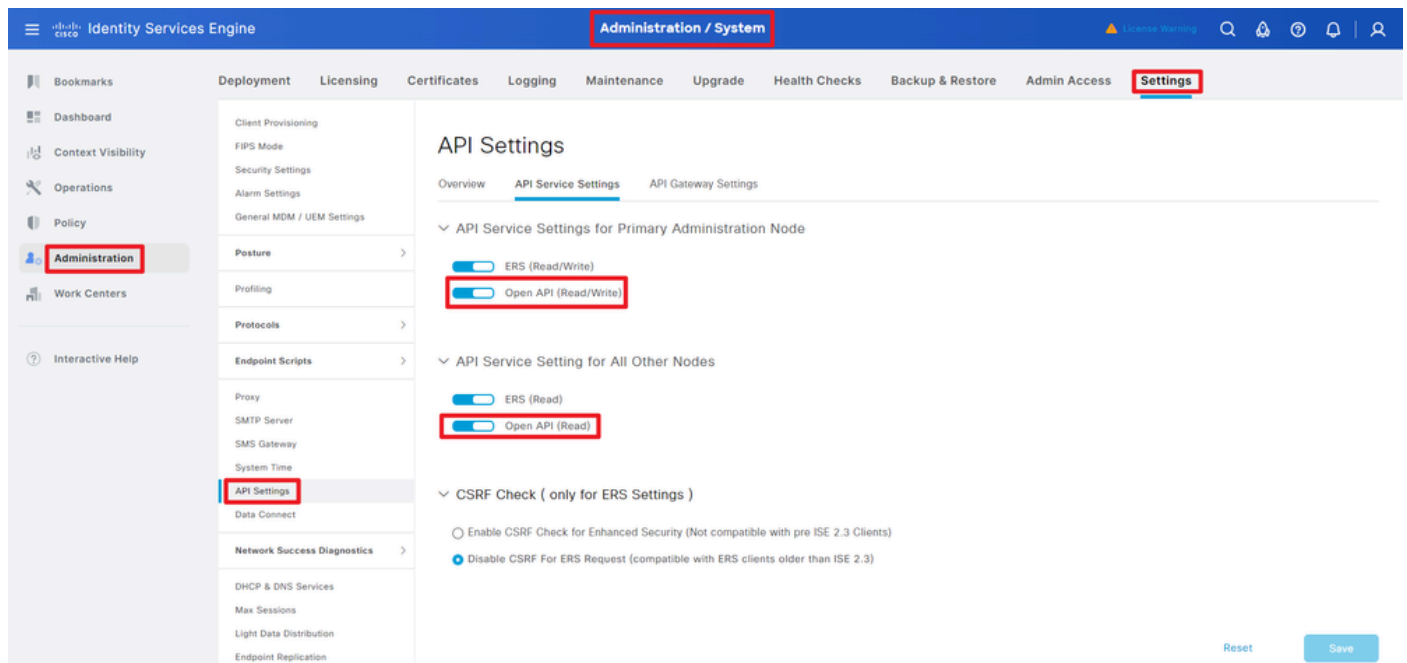
Administrators

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.

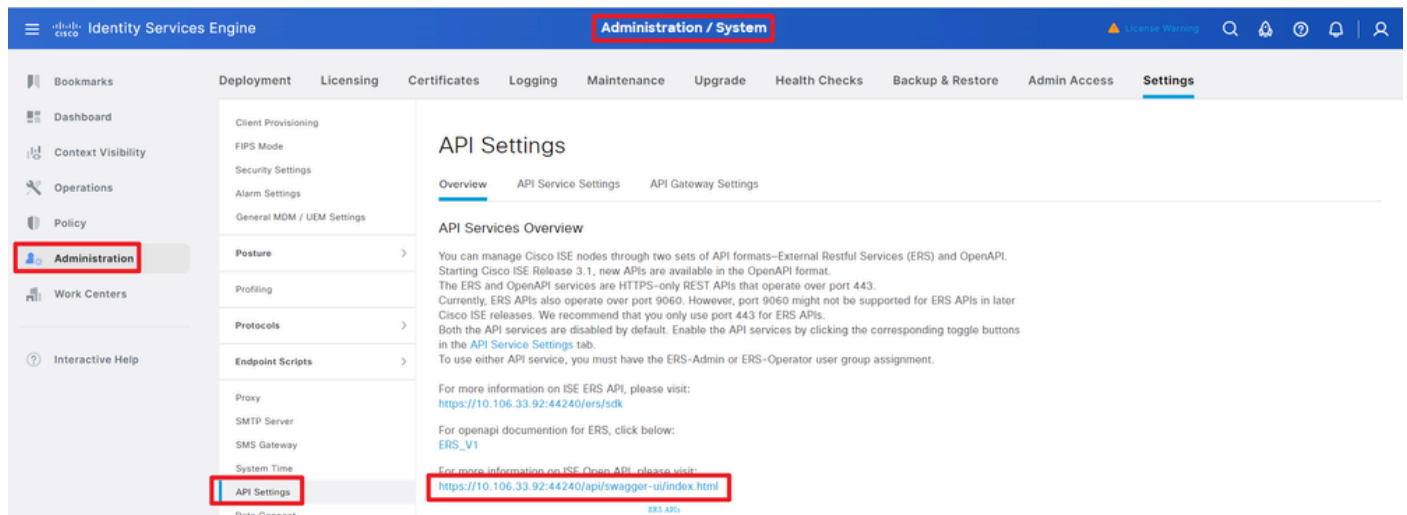
API abierta está desactivada de forma predeterminada en ISE. Para activarlo, vaya a Administration > System > Settings > API Settings > API Service Settings. Active o desactive las opciones de OpenAPI. Haga clic en Guardar.



Habilitar OpenAPI

Paso 3. Explore ISE OpenAPI.

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



Visite OpenAPI

Ejemplos de Python

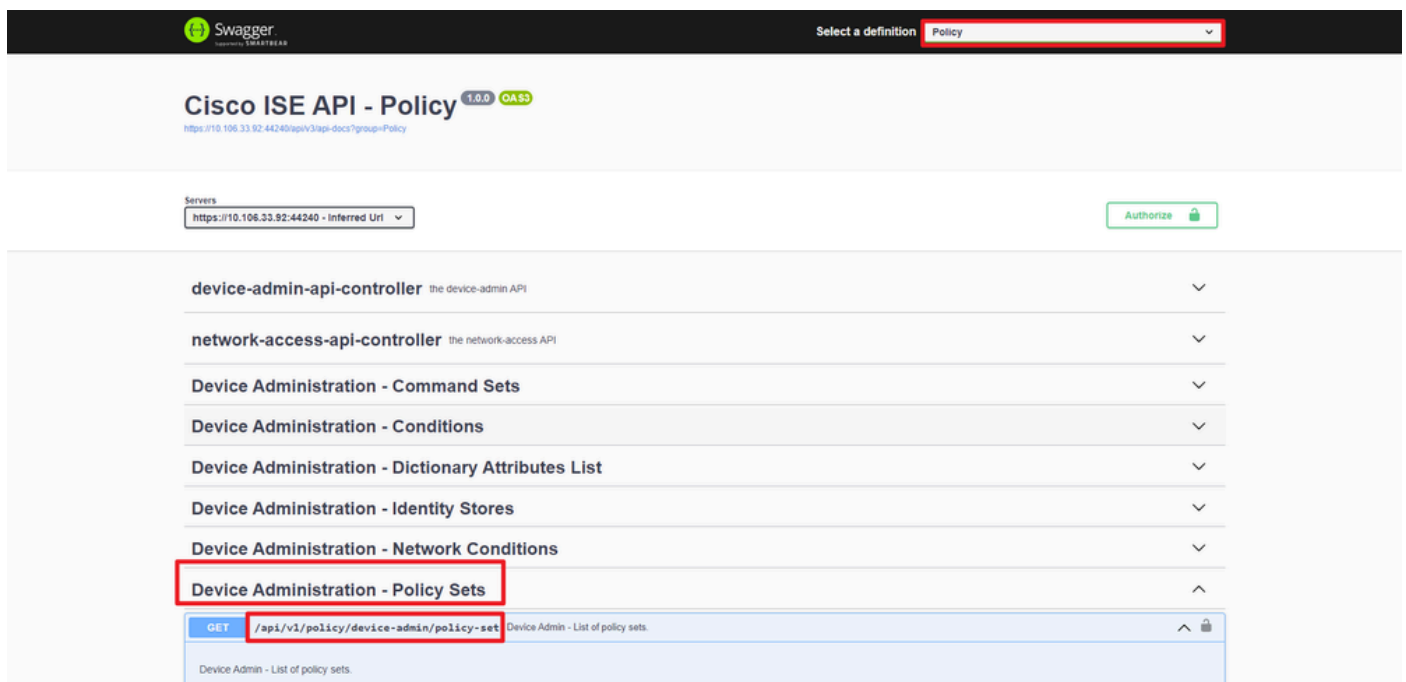
Device Admin - Lista De Conjuntos De Políticas

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

Paso 1. Información necesaria para una llamada de API.

Método	GET
URL	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.



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', 'descr

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	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 Swagger UI for the Cisco ISE API - Policy. At the top, there's a 'Select a definition' dropdown menu with 'Policy' selected. Below that, the title 'Cisco ISE API - Policy' is displayed with version '1.0.0' and 'OAS3' tags. The 'Servers' section shows the URL 'https://10.106.33.92:44240 - Inferred Uri'. An 'Authorize' button is visible. The main content area lists various API endpoints under the 'Device Administration - Authentication Rules' category, which is highlighted with a red box. The selected endpoint is 'GET /api/v1/policy/device-admin/policy-set/{policyId}/authentication'.

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()

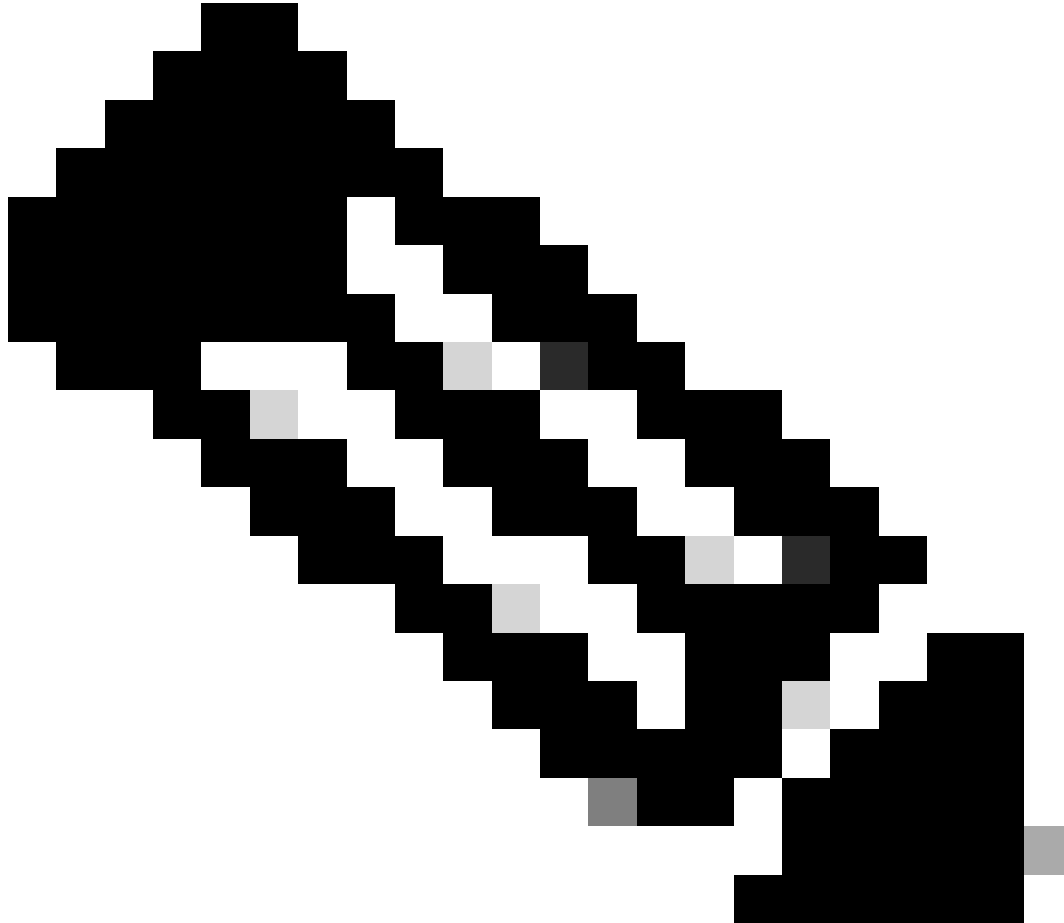
if __name__ == "__main__":

    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'}

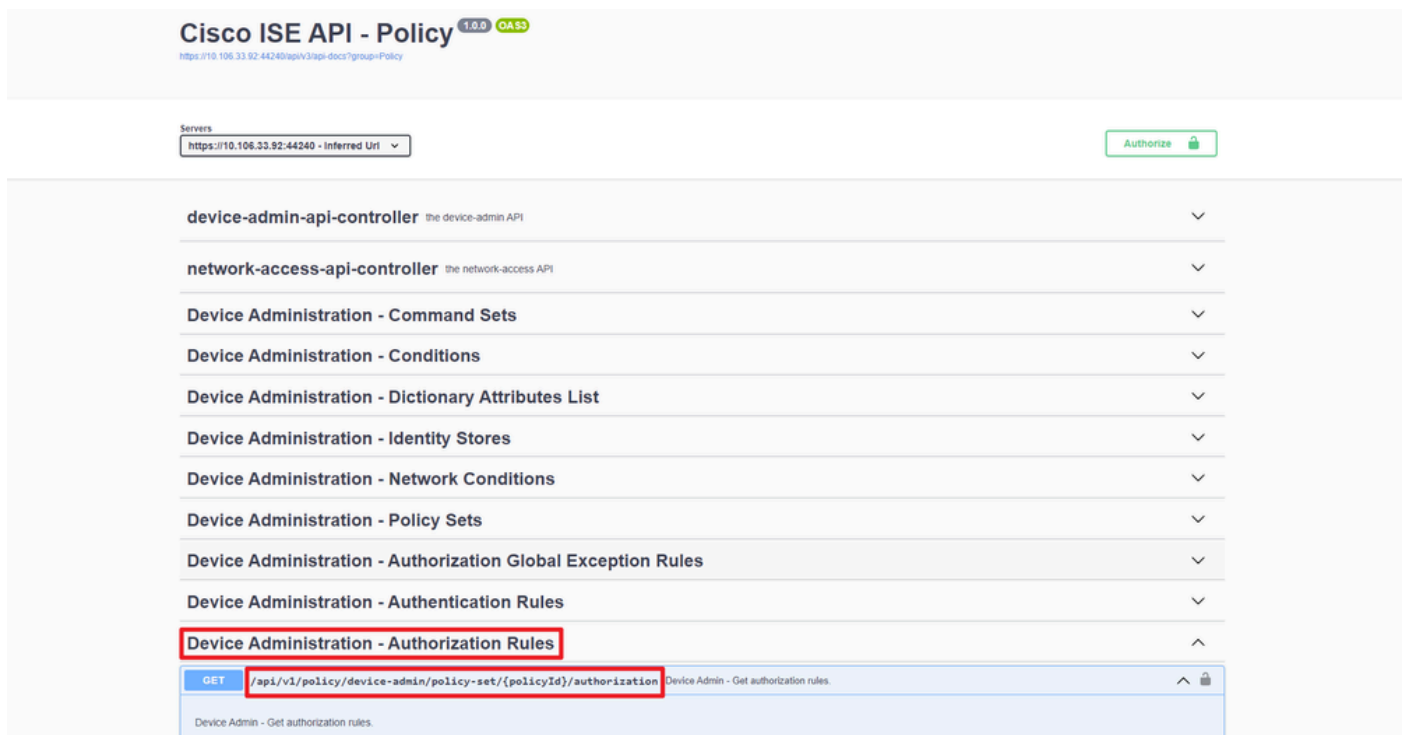
Device Admin - Obtener reglas de autorización

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	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.



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.

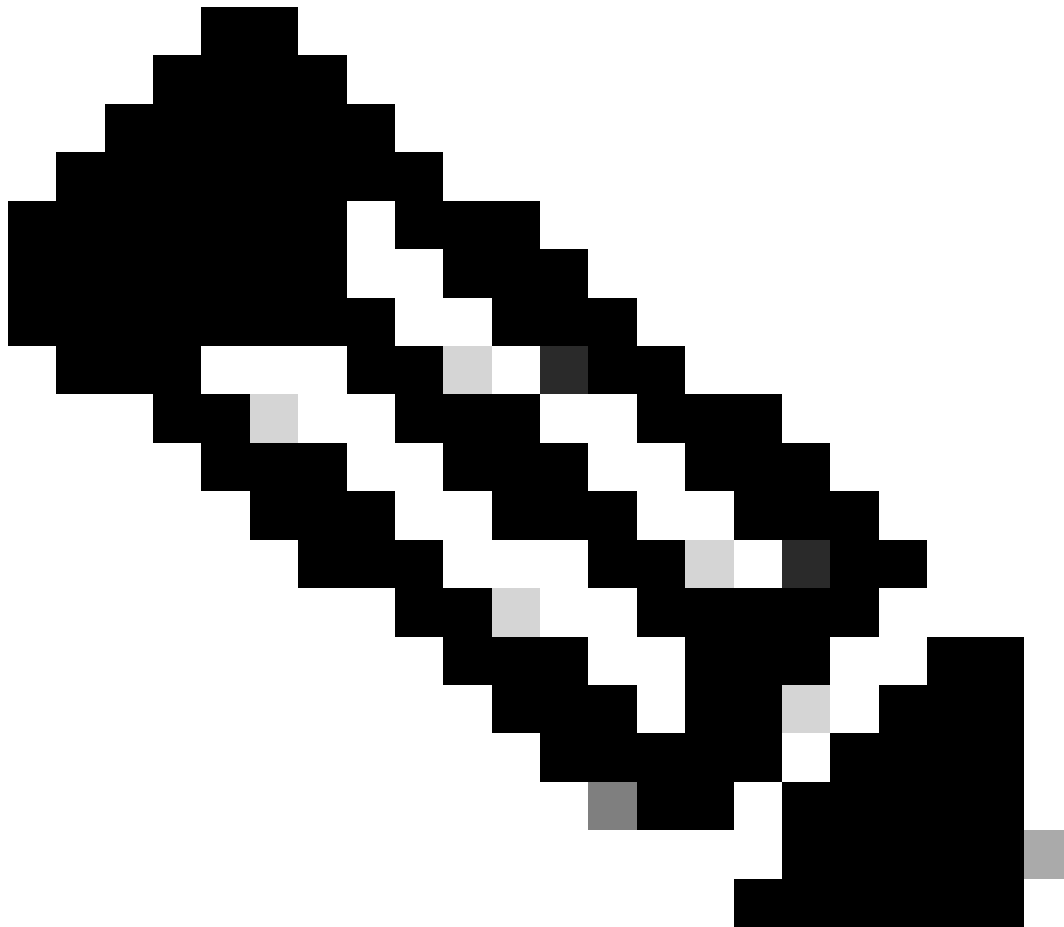
Garantizar una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de Python.

<#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'}
```

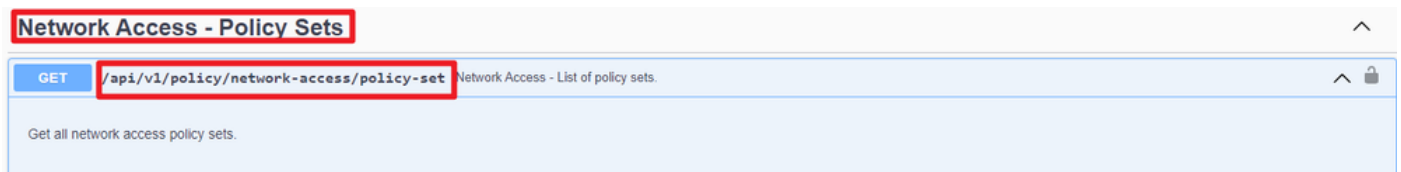
Acceso A La Red: Lista De Conjuntos De Políticas

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	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.



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_CFME0

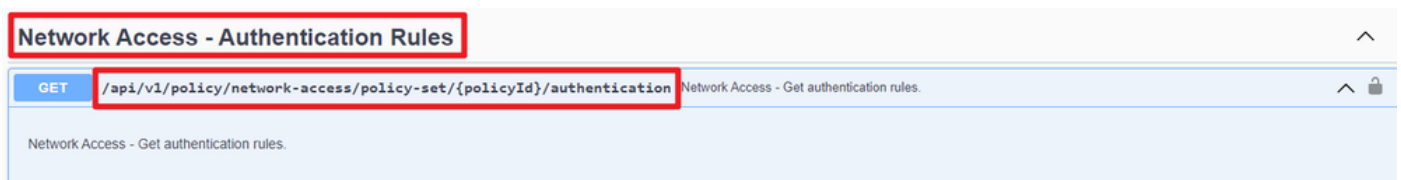
Acceso a la red - Obtener reglas de autenticación

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	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.



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/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())
```

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_CFME02-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

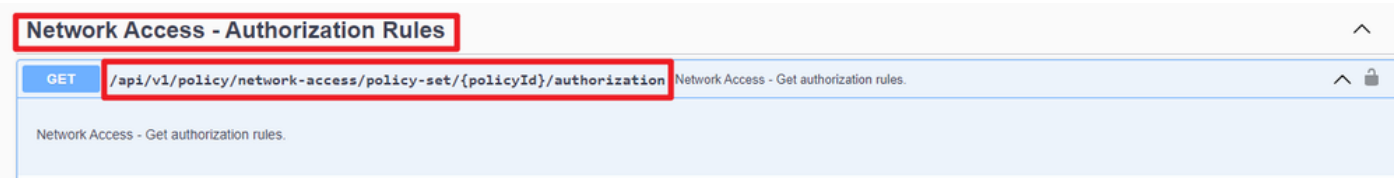
Esta API recupera las reglas de autorización de un conjunto de políticas determinado.

Paso 1. Información necesaria para una llamada de API.

Método	GET
--------	-----

URL	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/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())
```



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_CFME02-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 apiservicecomponent 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.

The screenshot shows the Identity Services Engine 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 Level Configuration' and contains a table with the following data:

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	
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.

The screenshot shows the Identity Services Engine interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar has 'Operations' highlighted. The main content area is titled 'Download Logs' and contains a table with the following data:

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

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).