Use OpenAPI to Retrieve ISE Policy Information on ISE 3.3

Contents

Introduction

This document describes the procedure for utilizing OpenAPI to manage Cisco Identity Services Engine (ISE) Policy.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

- ISE 3.3
- Python 3.10.0

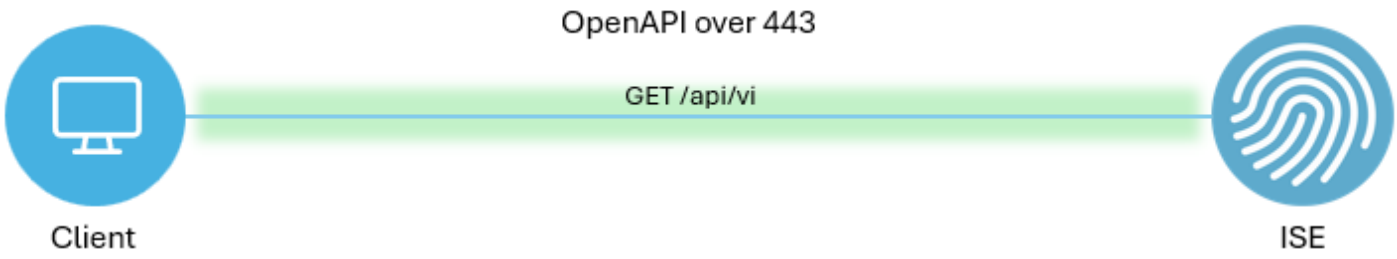
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

From Cisco ISE 3.1 onwards, newer APIs are available in the OpenAPI format. Management policy optimizes network security and management by enhancing interoperability, improving automation efficiency, strengthening security, fostering innovation, and reducing costs. This policy allows ISE to seamlessly integrate with other systems, achieve automated configuration and management, provide granular access control, encourage third-party innovation, and simplify management processes, thereby reducing maintenance costs and increasing overall return on investment.

Configure

Network Diagram

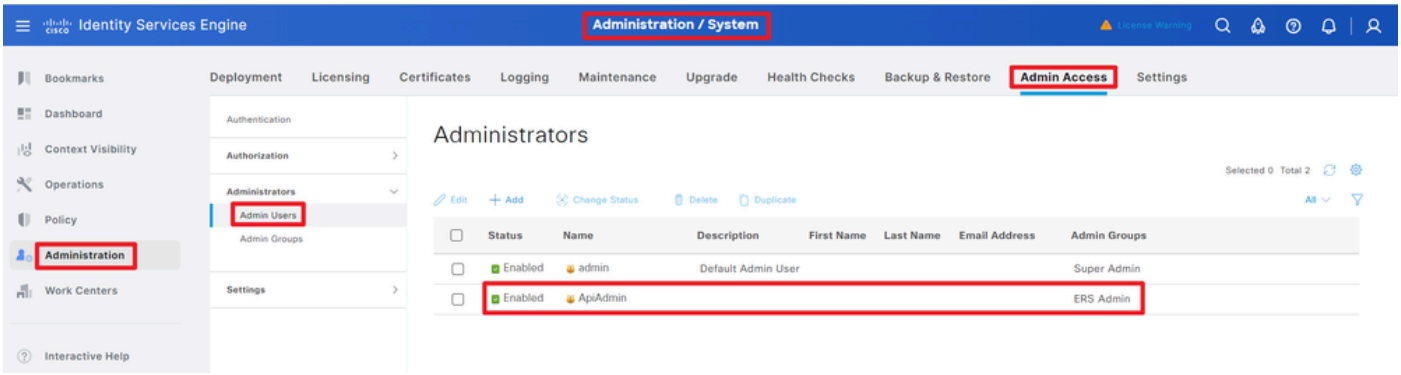


Topology

Configuration on ISE

Step 1. Add anOpenAPI admin account.

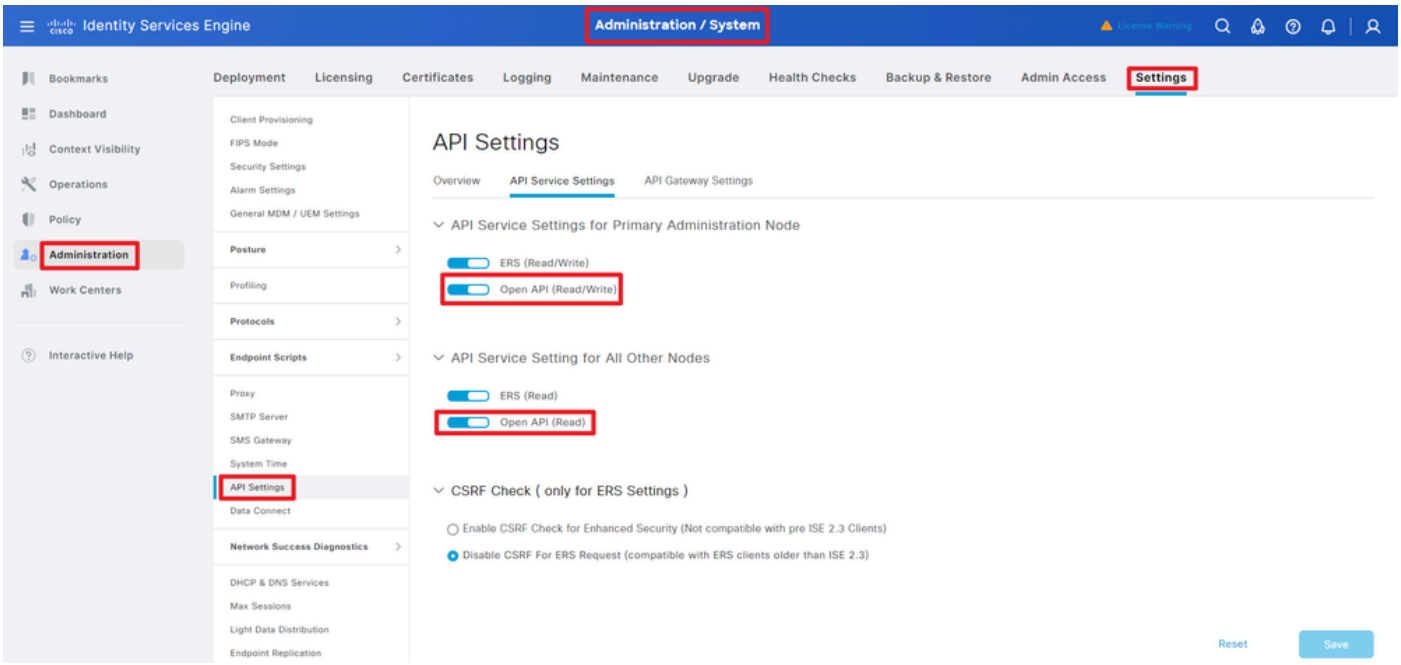
To add an API admin, navigate to**Administration > System > Admin Access > Administrators > Admin Users > Add**.



API Admin

Step 2. Enable OpenAPI on ISE.

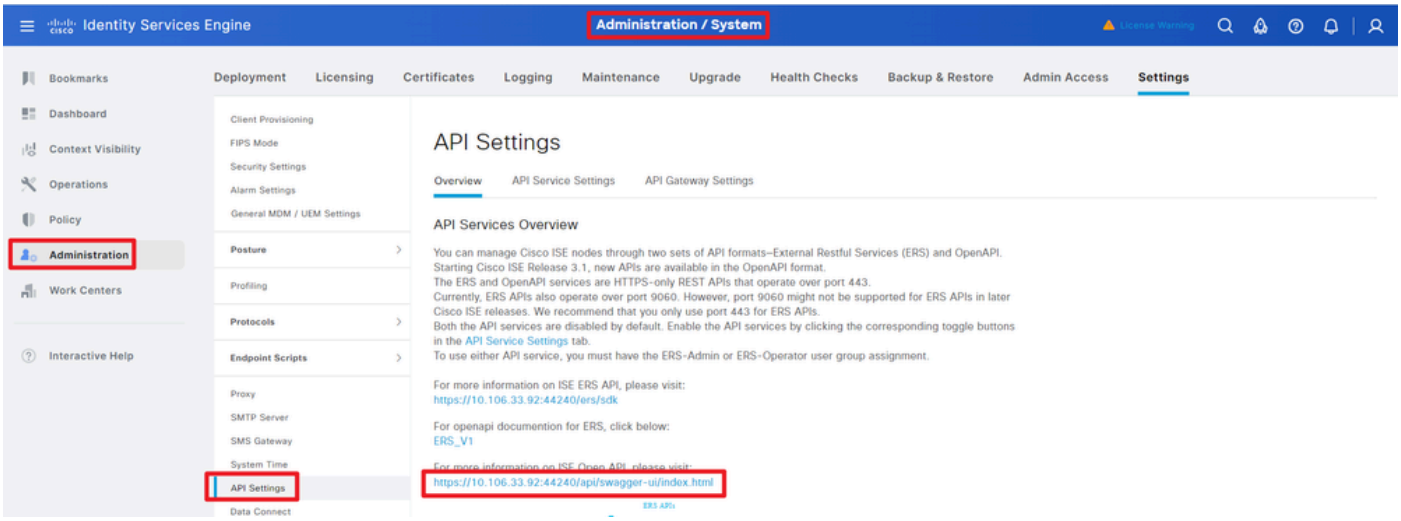
Open API is disabled by default on ISE. To enable it, navigate to **Administration > System > Settings > API Settings > API Service Settings**. Toggle the OpenAPI options. Click **Save**.



Enable OpenAPI

Step 3. Explore ISE OpenAPI.

Navigate to **Administration > System > Settings > API Settings > Overview**. Click **OpenAPI** to visit link.



Visit OpenAPI

Python Examples

Device Admin - List Of Policy Sets

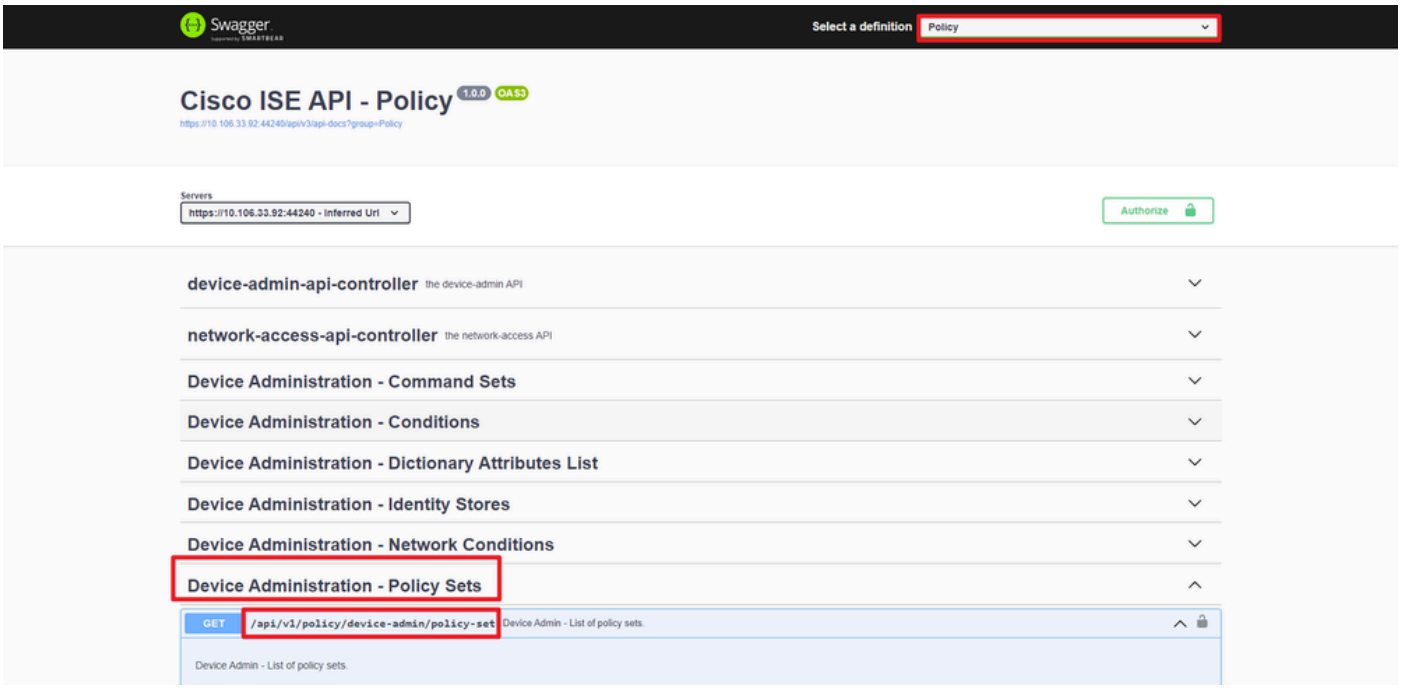
This API retrieves device admin policy sets information.

Step 1. Required information for an API call.

Method	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set

Credentials	Use OpenAPI account credentials.
Headers	Accept : application/json Content-Type : application/json

Step 2. Locate the URL that is utilized to retrieve device admin policy sets information.



API URI

Step 3. This is an example of Python code. Copy and paste the content. Replace the **ISE IP**, **username**, and **password**. **Save** as a python file to execute.

Ensure good connectivity between ISE and the device running the python code example.

<#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())
```

This is the example of expected outputs.

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

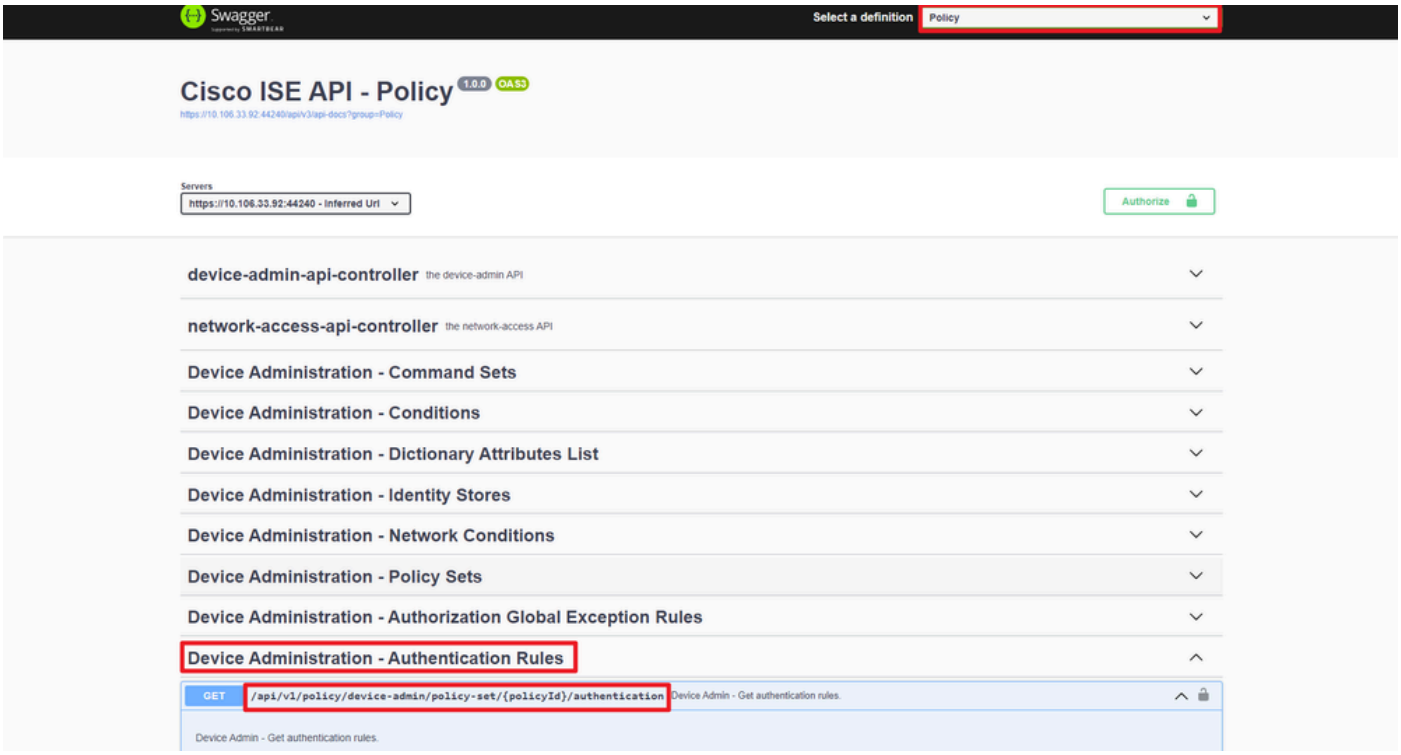
Device Admin - Get Authentication Rules

This API retrieves authentication rules of a particular policy set.

Step 1. Required information for an API call.

Method	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authentication
Credentials	Use OpenAPI account credentials.
Headers	Accept : application/json Content-Type : application/json

Step 2. Locate the URL that is utilized to retrieve authentication rule information.



API URI

Step 3. This is an example of Python code. Copy and paste the content. Replace the **ISE IP**, **username**, and **password**. **Save** as a python file to execute.

Ensure good connectivity between ISE and the device running the python code example.

<#root>

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

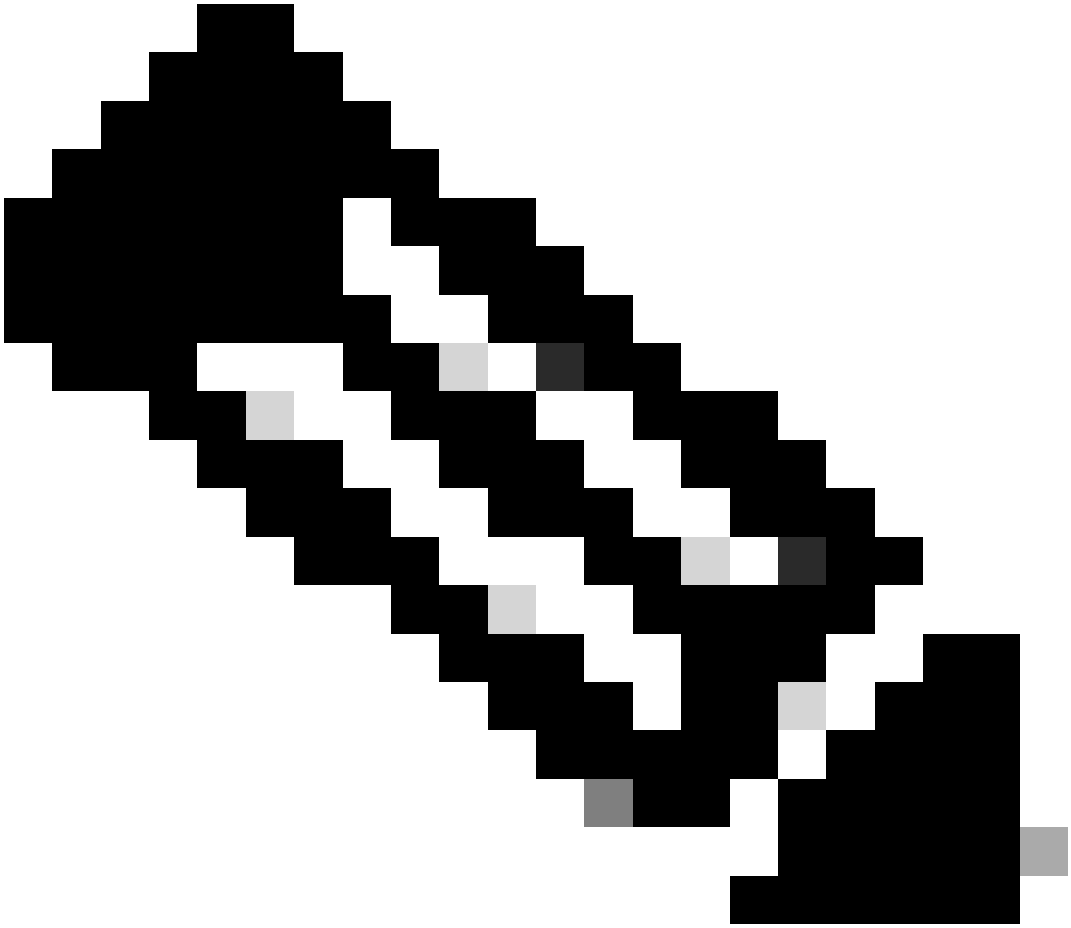
url = "

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

"

```
    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())
```



Note: The ID is from API outputs in step 3 of Device Admin - List Of Policy Sets. For example, 41ed8579-429b-42a8-879e-61861cb82bbf is TACACS Default policy set.

This is the example of expected outputs.

Return Code:
200
Expected Outputs:
{'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '73461597-0133-45ce-b4cb-6511ce56f262', 'name': 'Default', 'hitCounts': 0, 'rank': 0, 'state': 'enabl

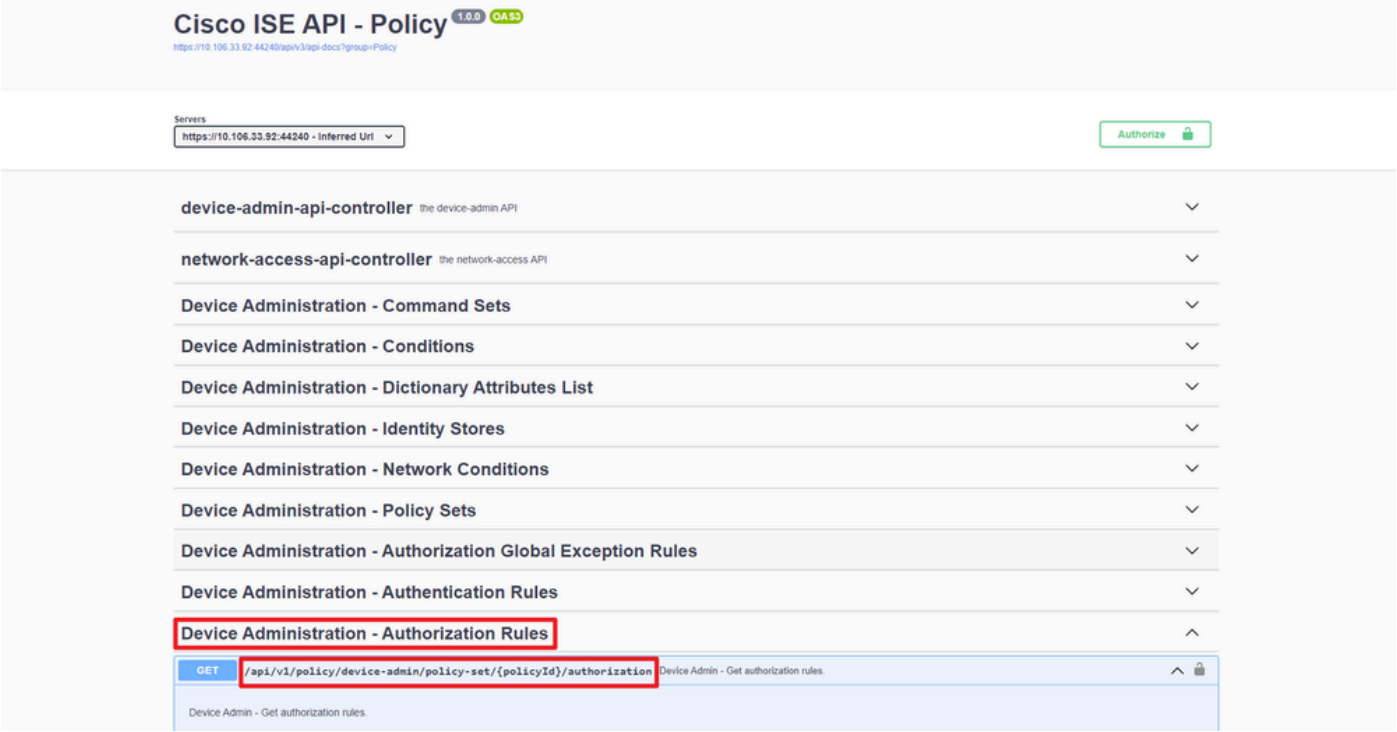
Device Admin - Get Authorization Rules

This API retrieves authorization rules of a particular policy set.

Step 1. Required information for an API call.

Method	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authorization
Credentials	Use OpenAPI account credentials.
Headers	Accept : application/json Content-Type : application/json

Step 2. Locate the URL that is utilized to retrieve the authorization rule information.



API URI

Step 3. This is an example of Python code. Copy and paste the content. Replace the **ISE IP**, **username**, and **password**. **Save** as a python file to execute.

Ensure good connectivity between ISE and the device running the python code example.

<#root>

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

url = "

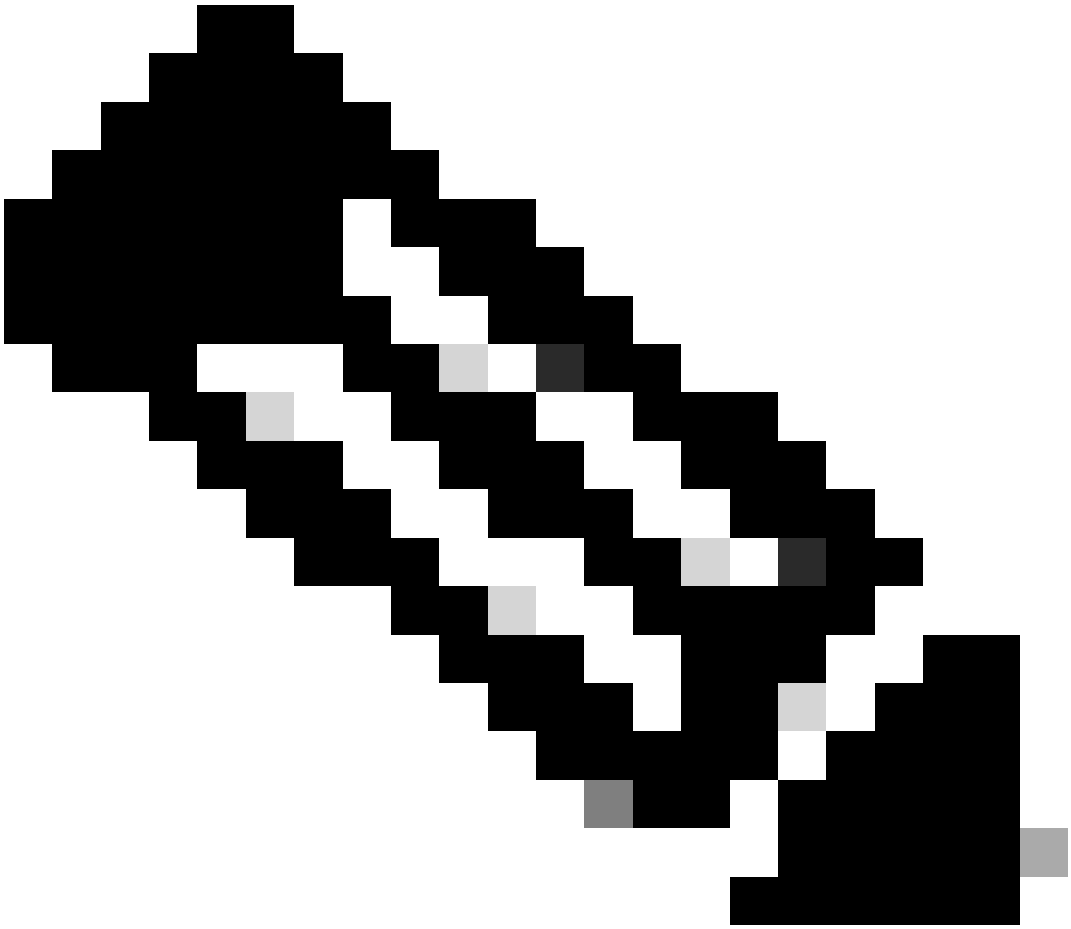
https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authoriz

"

```
    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:")
    print(response.status_code)
    print("Expected Outputs:")
    print(response.json())
```



Note: The ID is from API outputs in step 3 of Device Admin - List Of Policy Sets. For example, 41ed8579-429b-42a8-879e-61861cb82bbf is TACACS Default policy set.

This is the example of expected outputs.

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

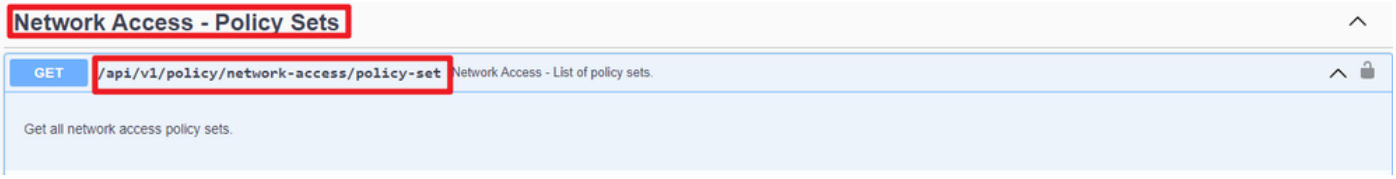
Network Access - List Of Policy Sets

This API retrieves network access policy sets of ISE deployments.

Step 1. Required information for an API call.

Method	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set
Credentials	Use OpenAPI account credentials.
Headers	Accept : application/json Content-Type : application/json

Step 2. Locate the URL that is utilized to retrieve the specific ISE node information.



API URI

Step 3. This is an example of Python code. Copy and paste the content. Replace the **ISE IP**, **username**, and **password**. **Save** as a python file to execute.

Ensure good connectivity between ISE and the device running the python code example.

<#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())
```

This is the example of expected outputs.

Return Code:
200
Expected Outputs:
{'version': '1.0.0', 'response': [{'default': False, 'id': 'ba71a417-4a48-4411-8bc3-d5df9b115769', 'name': 'BGL_CFME02-FMC', 'description': None, 'hitCoun

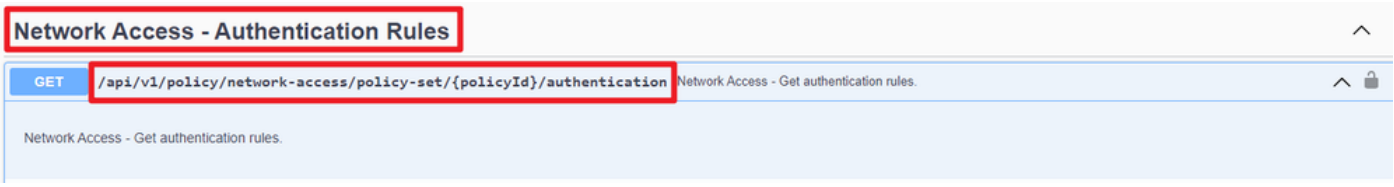
Network Access - Get Authentication Rules

This API retrieves authentication rules of a particular policy set.

Step 1. Required information for an API call.

Method	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authentication
Credentials	Use OpenAPI account credentials.
Headers	Accept : application/json Content-Type : application/json

Step 2. Locate the URL that is utilized to retrieve the authentication rule information.



API URI

Step 3. This is an example of Python code. Copy and paste the content. Replace the **ISE IP**, **username**, and **password**. **Save** as a python file to execute.

Ensure good connectivity between ISE and the device running the python code example.

<#root>

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

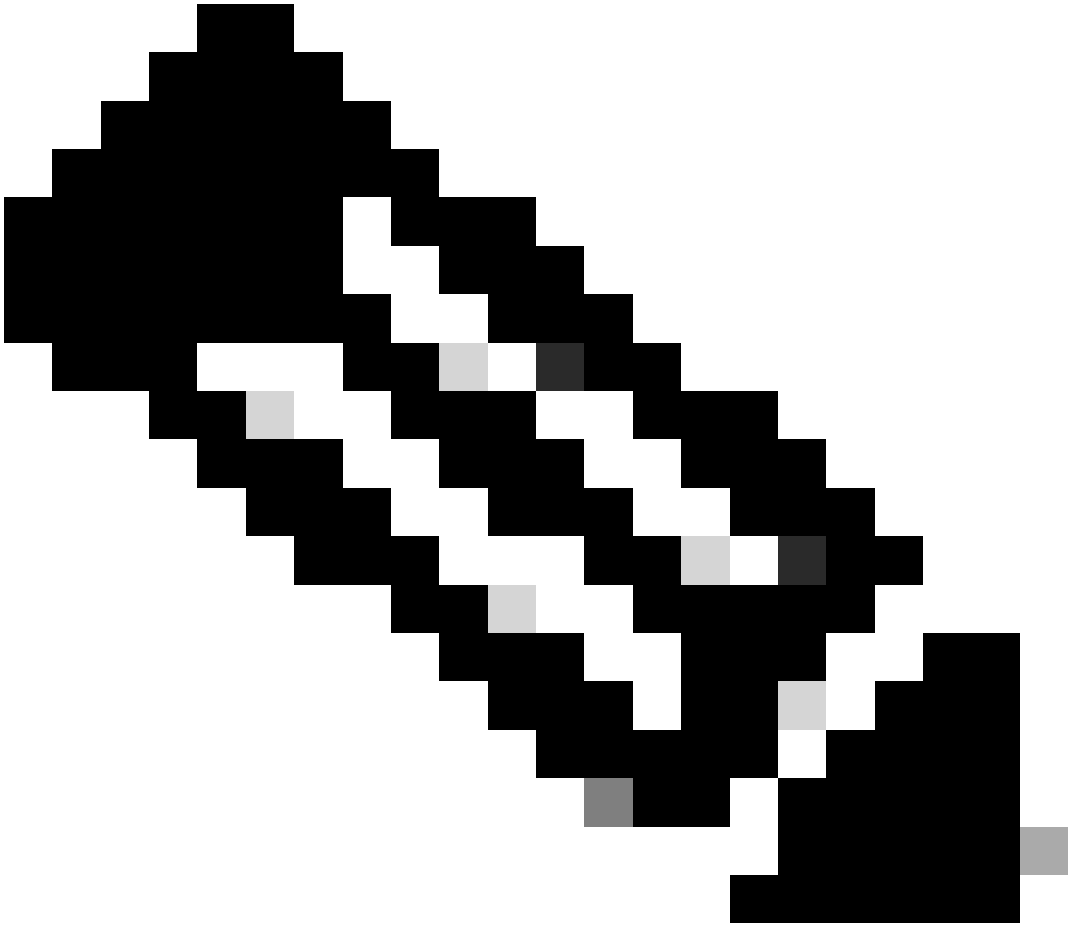
url = "

https://10.106.33.92/api/v1/policy/network-access/policy-set/ba71a417-4a48-4411-8bc3-d5df9b115769/auther

"

```
    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())
```



Note: The ID is from API outputs in step 3 of Network Access - List Of Policy Sets. For example, ba71a417-4a48-4411-8bc3-d5df9b115769 is BGL_CFME02-FMC.

This is the example of expected outputs.

Return Code:
200
Expected Outputs:
{'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default', 'hitCounts': 0, 'rank': 0, 'state': 'enabl

Network Access - Get Authorization Rules

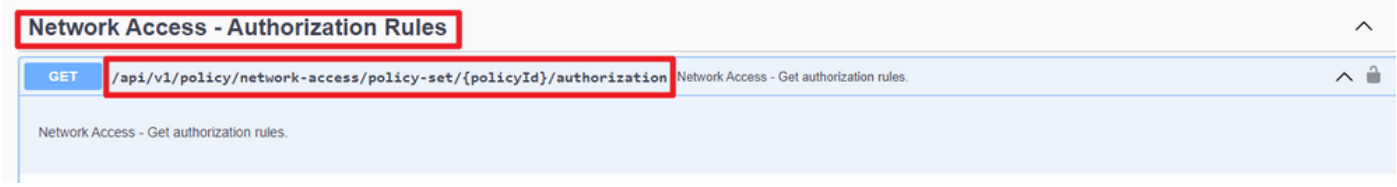
This API retrieves authorization rules of a particular policy set.

Step 1. Required information for an API call.

Method	GET

URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authorization
Credentials	Use OpenAPI account credentials.
Headers	Accept : application/json Content-Type : application/json

Step 2. Locate the URL that is utilized to retrieve the authorization rule information.



API URI

Step 3. This is an example of Python code. Copy and paste the content. Replace the **ISE IP**, **username**, and **password**. **Save** as a python file to execute.

Ensure good connectivity between ISE and the device running the python code example.

<#root>

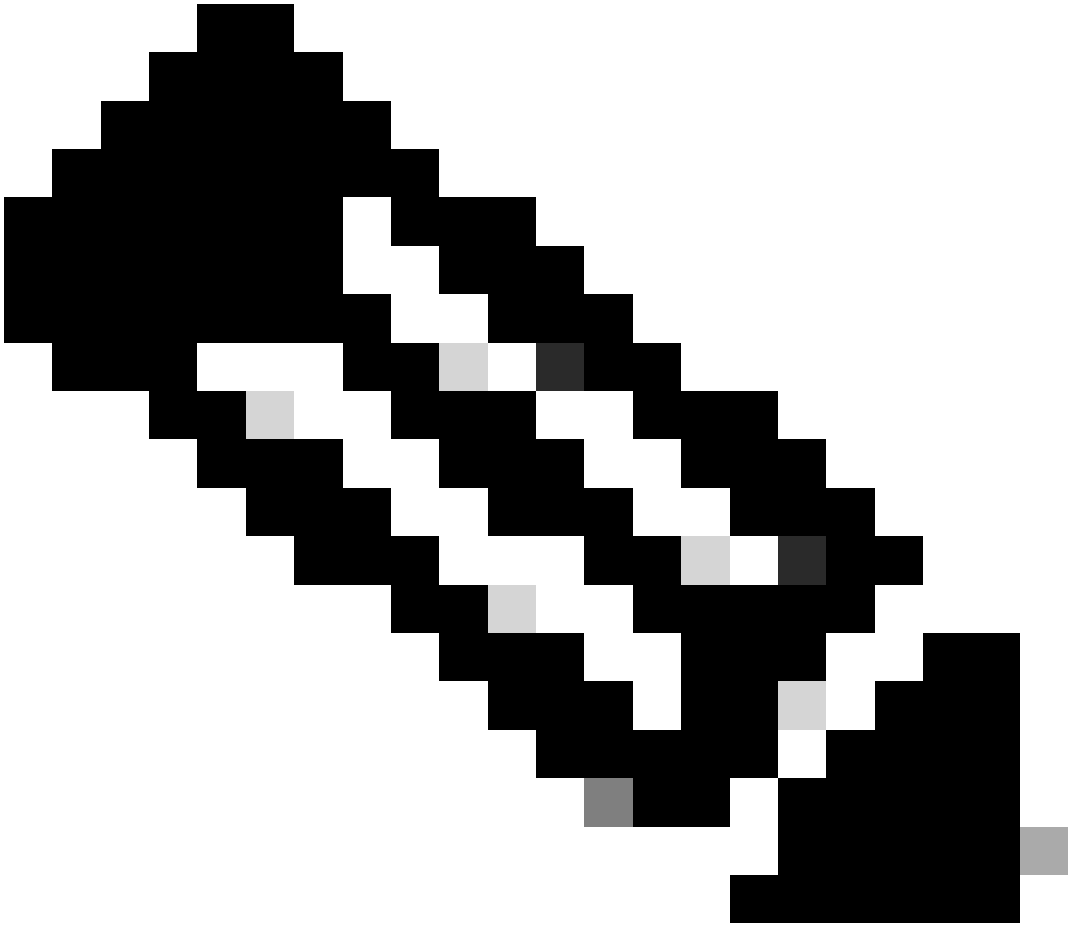
```
from requests.auth import HTTPBasicAuth
import requests

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())
```



Note: The ID is from API outputs in step 3 of Network Access - List Of Policy Sets. For example, ba71a417-4a48-4411-8bc3-d5df9b115769 is BGL_CFME02-FMC.

This is the example of expected outputs.

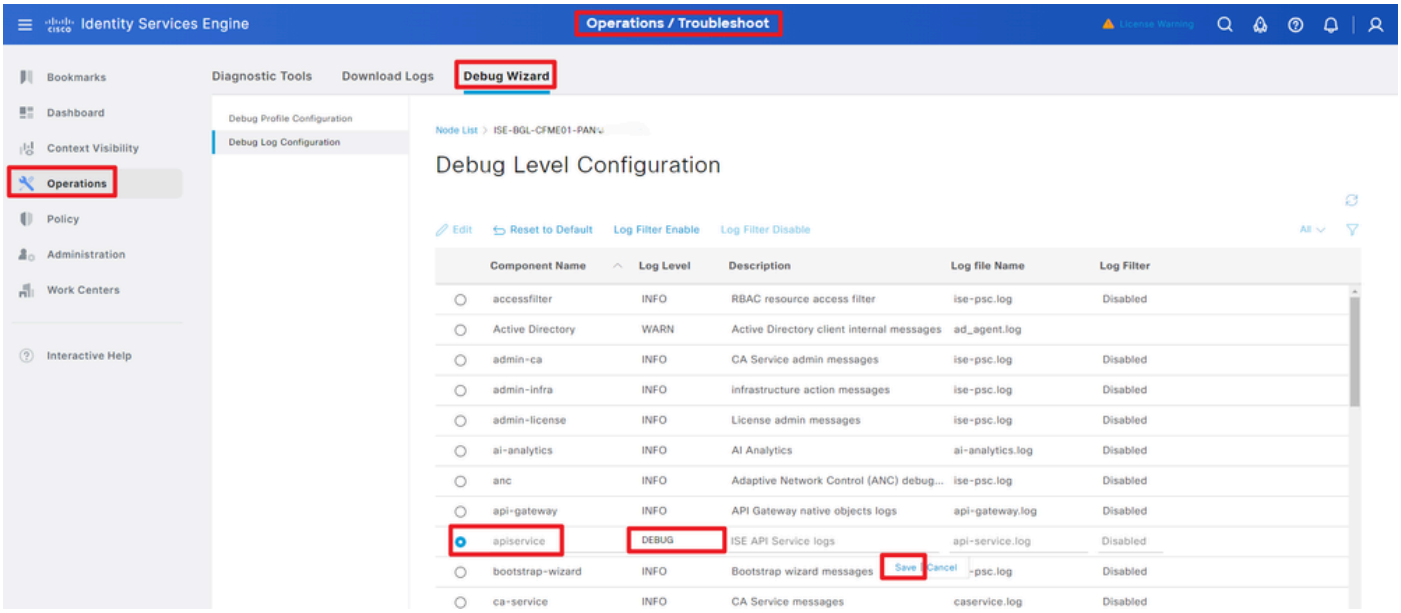
Return Code:
200
Expected Outputs:
{'version': '1.0.0', 'response': [{'rule': {'default': False, 'id': 'bc67a4e5-9000-4645-9d75-7c2403ca22ac', 'name': 'FMC Admin', 'hitCounts': 0, 'rank': 0, 'state':

Troubleshoot

To troubleshoot issues that are related to the OpenAPIs, set the**Log Level** for the**apiservice**component to**DEBUG**in the**Debug Log Configuration**window.

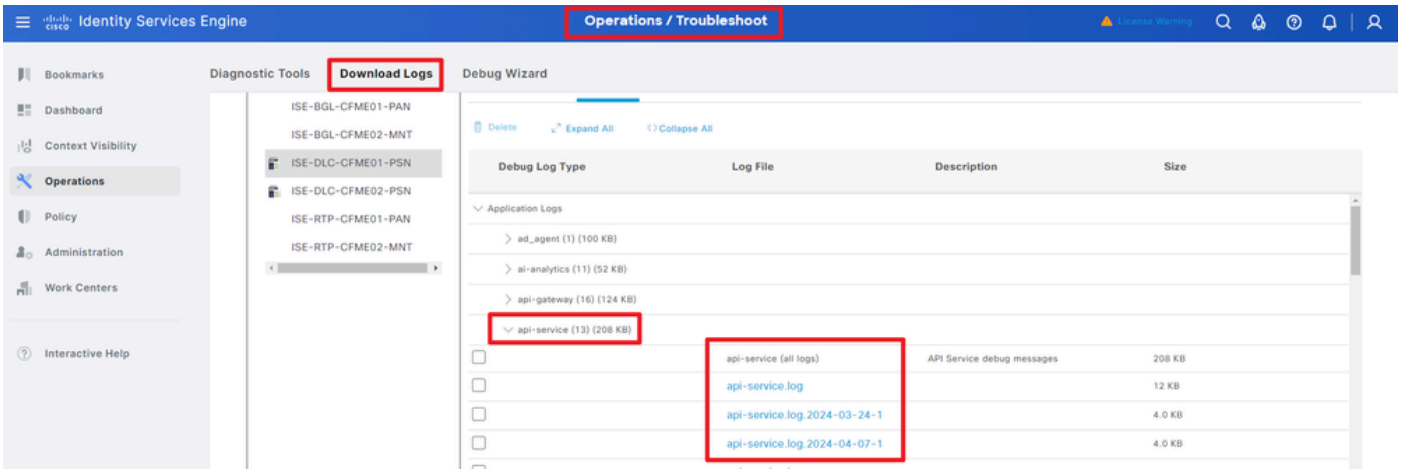
To enable debug, navigate to**Operations > Troubleshoot > Debug Wizard > Debug Log Configuration >**

ISE Node > apiservice.



API Service Debug

To download debug log file, navigate to **Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs**.



Download Debug Logs