

Use OpenAPI to Retrieve ISE Policy Information on ISE 3.3

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configuration on ISE](#)

[Python Examples](#)

[Device Admin - List Of Policy Sets](#)

[Device Admin - Get Authentication Rules](#)

[Device Admin - Get Authorization Rules](#)

[Network Access - List Of Policy Sets](#)

[Network Access - Get Authentication Rules](#)

[Network Access - Get Authorization Rules](#)

[Troubleshoot](#)

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

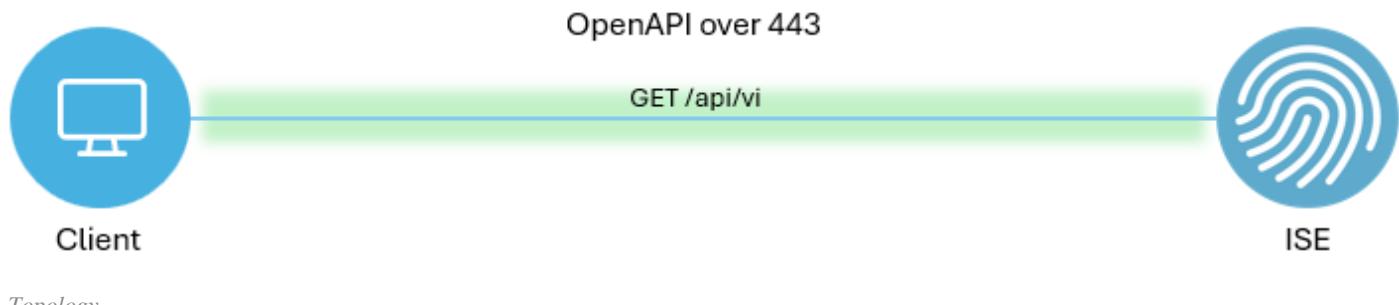
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

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 an OpenAPI admin account.

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

The screenshot shows the ISE Administration interface. The top navigation bar has 'Administration / System' highlighted. The left sidebar has 'Administration' selected. The main content area shows the 'Administrators' section with 'Admin Users' selected. A table lists two users: 'admin' (Super Admin) and 'ApiAdmin' (ERS Admin). The 'ApiAdmin' row is highlighted with a red box.

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

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**.

The screenshot shows the Cisco Identity Services Engine interface. The left sidebar has 'Administration' selected. The main content area is titled 'API Settings' under the 'API Service Settings' tab. It shows settings for the Primary Administration Node and All Other Nodes, with 'Open API' toggles highlighted by red boxes. A note at the bottom says 'Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)' with a radio button for 'Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)'. Buttons for 'Reset' and 'Save' are at the bottom right.

Enable OpenAPI

Step 3. Explore ISE OpenAPI.

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

The screenshot shows the same interface as above, but the 'ERS API' link in the 'For more information on ISE Open API, please visit:' section is highlighted with a red box.

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	<a href="https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set">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.

The screenshot shows the Cisco ISE API - Policy Swagger interface. At the top, there is a navigation bar with a 'Swagger' logo and a dropdown menu labeled 'Select a definition' with 'Policy' selected. Below the header, the title 'Cisco ISE API - Policy' is displayed along with version '1.0.0' and 'OAS3'. A sub-header indicates the URL is 'https://10.106.33.92:44240/api/v3/api-docs?group=Policy'. The main content area lists various API endpoints under 'device-admin-api-controller' and 'network-access-api-controller'. Under 'device-admin-api-controller', the 'Device Administration - Policy Sets' endpoint is highlighted with a red box. This endpoint has a 'GET /api/v1/policy/device-admin/policy-set' method listed, which is also highlighted with a red box. The method description is 'Device Admin - List of policy sets.'

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

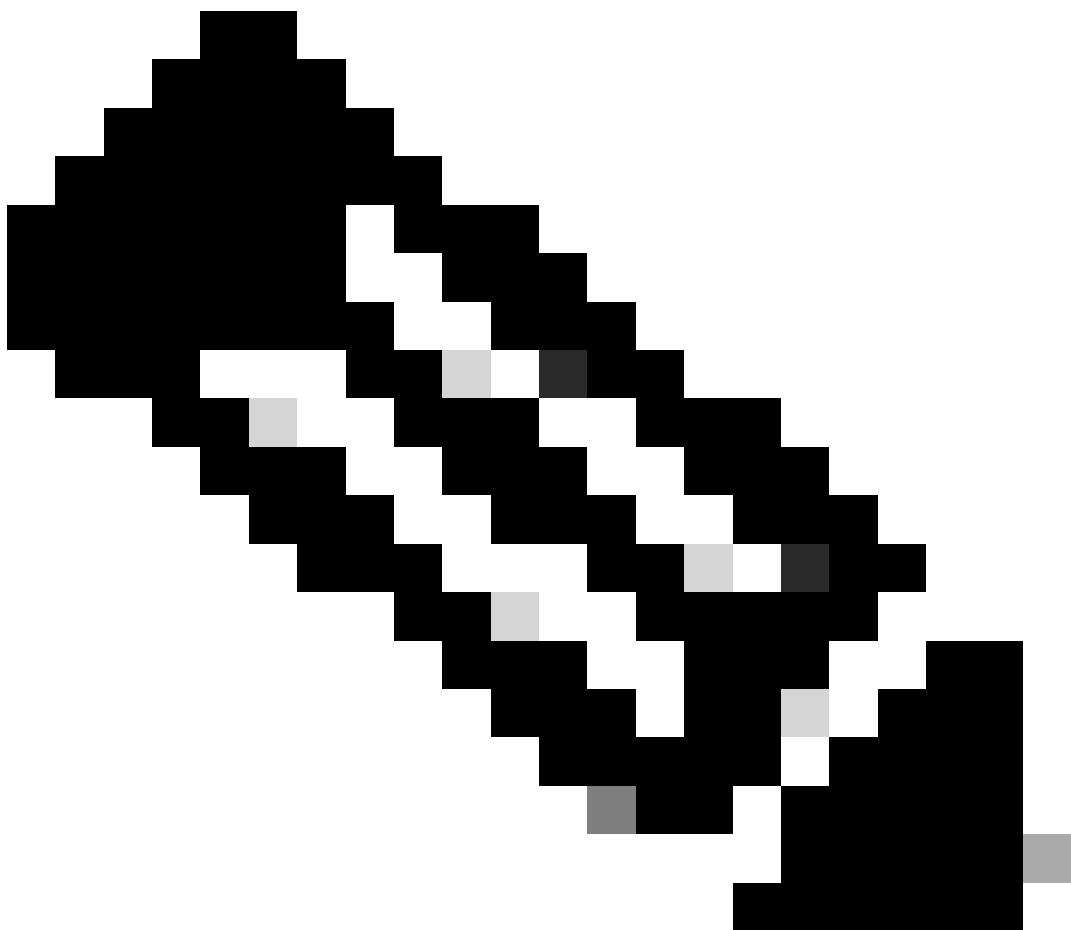
requests.packages.urllib3.disable_warnings()

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

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



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	<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
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.

The screenshot shows the Cisco ISE API - Policy OpenAPI Specification (OAS) interface. At the top, it displays the title "Cisco ISE API - Policy 0.0 OAS" and the URL "https://10.106.33.92:44240/api/v3/api-docs?group=Policy". Below this, there is a "Servers" dropdown set to "https://10.106.33.92:44240 - Inferred Url" and an "Authorize" button. The main content area lists various API endpoints under "Device Administration". One endpoint, "Device Administration - Authorization Rules", is highlighted with a red box around its URL field. The URL field contains "GET /api/v1/policy/device-admin/policy-set/{policyId}/authorization". A tooltip for this URL reads "Device Admin - Get authorization rules." Below the URL, the description "Device Admin - Get authorization rules." is visible.

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 = ""

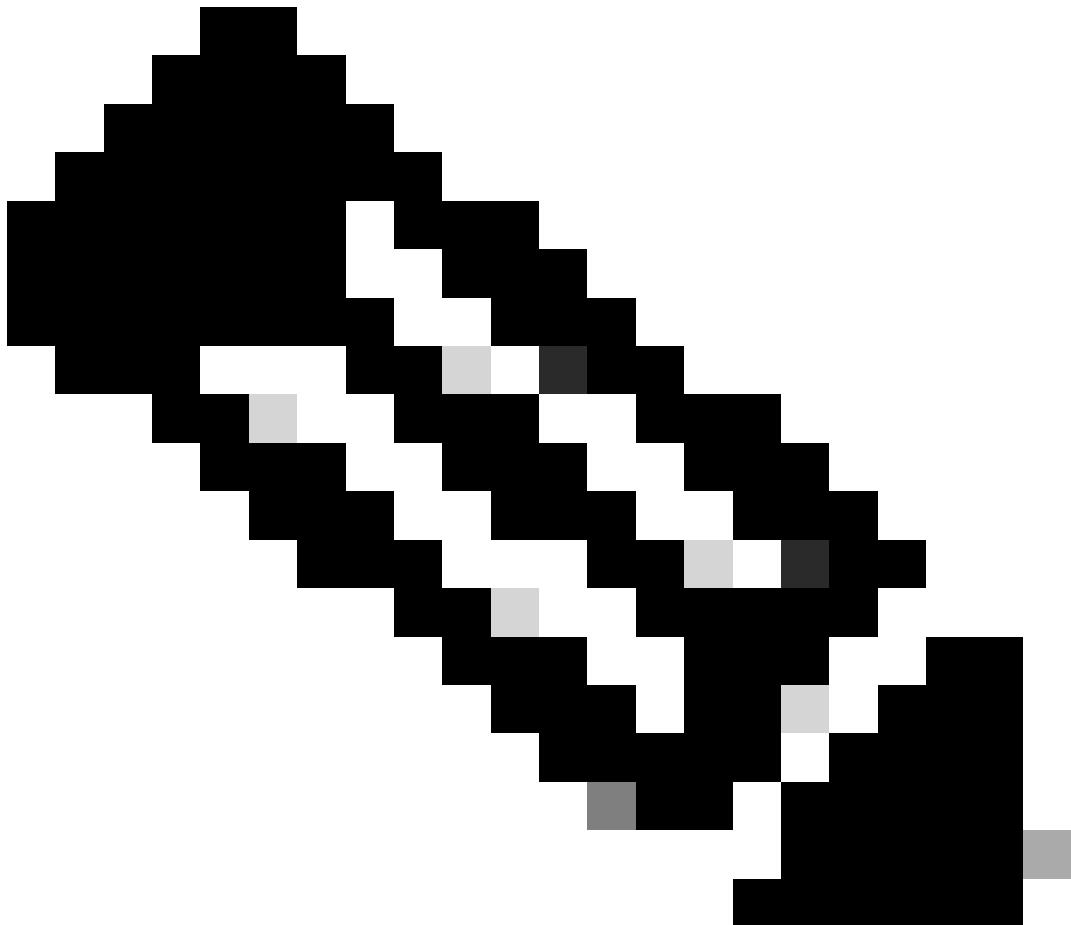
    https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authoriz
    "
    headers = {
        "Accept": "application/json", "Content-Type": "application/json"
    }
    auth = HTTPBasicAuth(username, password)
    response = requests.get(url, headers=headers, auth=auth, verify=False)
    print(response.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'}}]}
```

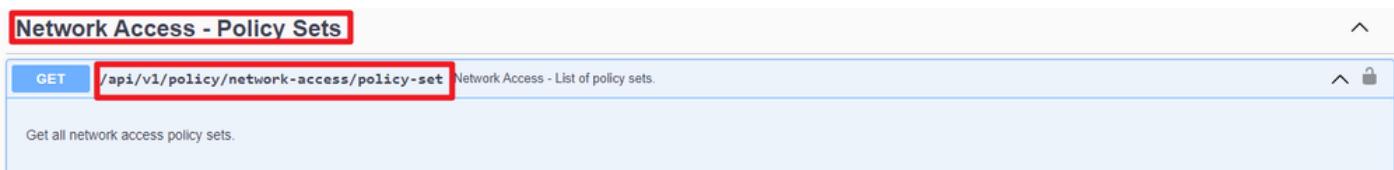
Network Access - List Of Policy Sets

This API retrieves network access policy sets of ISE deployments.

Step 1. Required information for an API call.

Method	GET
URL	<a href="https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set">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.



The screenshot shows a browser interface for an API documentation page. At the top, there's a header bar with a search icon and a user profile icon. Below it, a navigation bar has 'Network Access - Policy Sets' selected. The main content area shows a table with one row. The first column is 'GET' and the second column is the URL '/api/v1/policy/network-access/policy-set'. A red box highlights the URL. Below the table, a note says 'Get all network access policy sets.' To the left, a sidebar lists 'API URI'.

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_CFM02-FMC', 'description': None, 'hitCount': 0}}]}
```

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	<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
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.

The screenshot shows a browser window with the title "Network Access - Authentication Rules". Below the title, there is a blue button labeled "GET" and a red box highlights the URL field containing the path "/api/v1/policy/network-access/policy-set/{policyId}/authentication". To the right of the URL field, there is a note: "Network Access - Get authentication rules." Below the URL field, there is another note: "Network Access - Get authentication rules."

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>

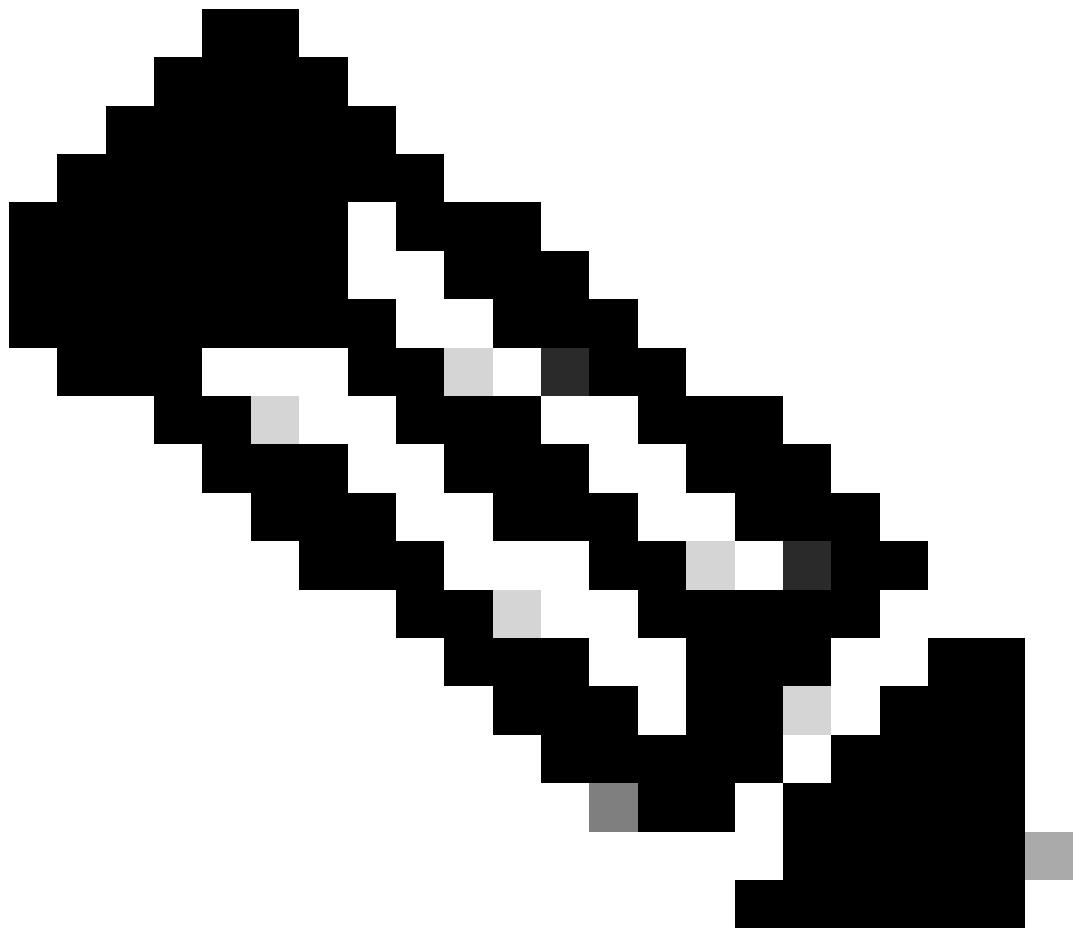
from requests.auth import HTTPBasicAuth
import requests

```

```
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/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())
```



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': 'enab}}
```

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	<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
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.

The screenshot shows a web-based API documentation interface. At the top, there's a header "Network Access - Authorization Rules". Below it, a navigation bar has a "GET" button and a highlighted URL: "/api/v1/policy/network-access/policy-set/{policyId}/authorization". A tooltip for this URL says "Network Access - Get authorization rules." To the right of the URL, there are icons for copy and lock. The main content area below the navigation bar contains the text "Network Access - Get authorization rules.".

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/authorizat
```

```
"
```

```
    headers = {
```

```
        "Accept": "application/json", "Content-Type": "application/json"
```

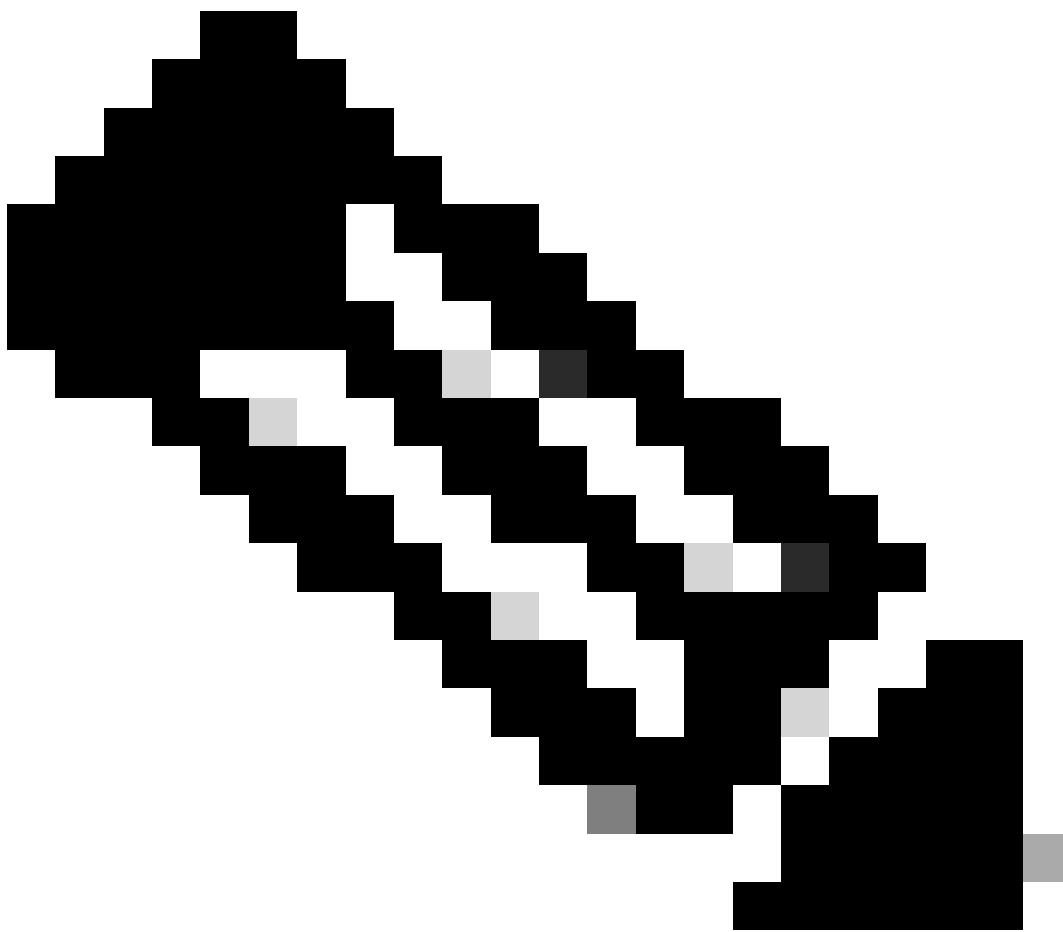
```
}
```

```
    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())
```



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_CFM02-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": "Active"}, ...]}
```

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.

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

API Service Debug

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

Log File	Description	Size
api-service (all logs)	API Service debug messages	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

Download Debug Logs