

OpenAPIを使用したISE 3.3でのISEポリシー情報の取得

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[ISEでの設定](#)

[Pythonの例](#)

[デバイス管理者 - ポリシーセットの一覧](#)

[デバイス管理者 - 認証ルールの取得](#)

[デバイス管理者 - 許可ルールの取得](#)

[ネットワークアクセス：ポリシーセットのリスト](#)

[ネットワークアクセス - 認証ルールの取得](#)

[ネットワークアクセス - 許可ルールの取得](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、OpenAPIを使用して Cisco Identity Services Engine (ISE) ポリシーに該当するトラフィックを区別します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

- ISE 3.3
- Python 3.10.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco ISE 3.1以降では、新しいAPIがOpenAPI形式で使用できます。管理ポリシーは、相互運用性の強化、自動化の効率化、セキュリティの強化、イノベーションの促進、コストの削減によって、ネットワークのセキュリティと管理を最適化します。このポリシーにより、ISEは他のシステムとシームレスに統合し、自動化された設定と管理を実現し、きめ細かなアクセス制御を提供し、サードパーティの革新を奨励し、管理プロセスを簡素化することができます。その結果、メンテナンスコストが削減され、全体的な投資回収率が向上します。

設定

ネットワーク図



トポロジ

ISEでの設定

ステップ 1 : anOpenAPI adminアカウントを追加します。

API管理者を追加するには、Administration > System > Admin Access > Administrators > Admin Users > Addの順に移動します。

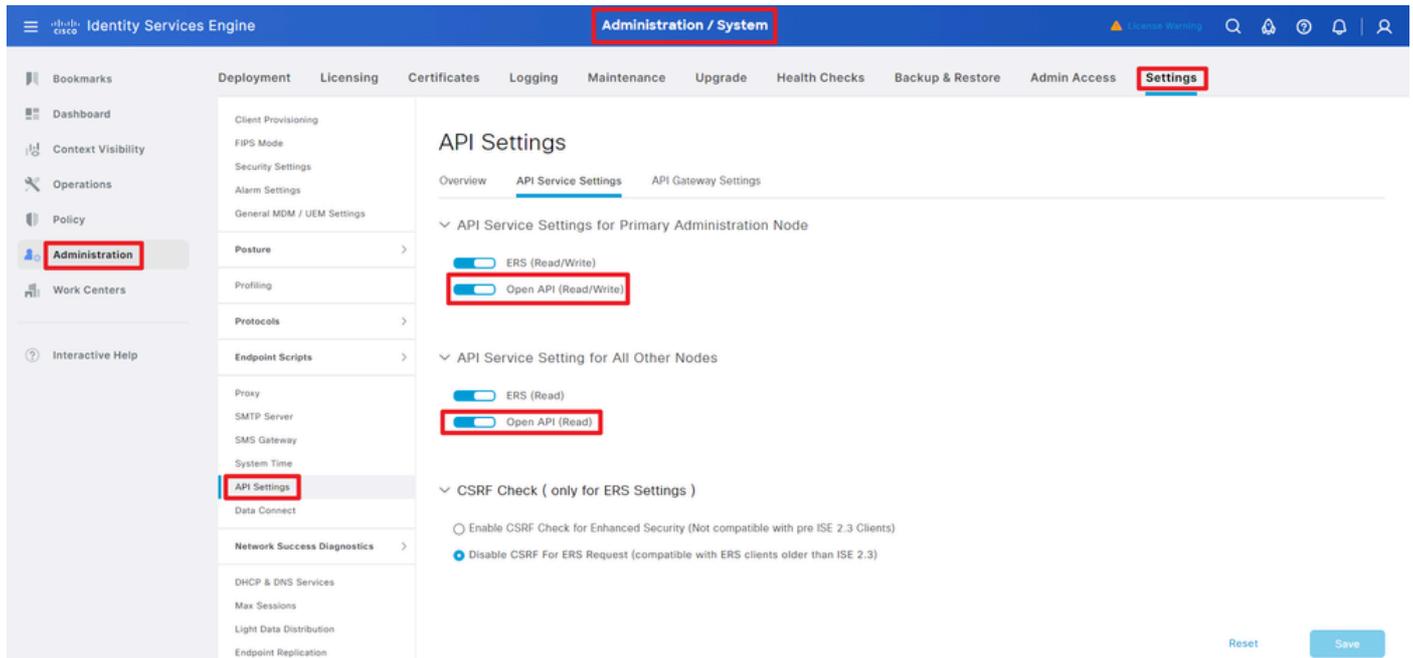
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and 'Admin Access'. The left sidebar has 'Administration' selected. The main content area is titled 'Administrators' and shows a table of administrator accounts. Two accounts are listed: 'admin' (Default Admin User) 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管理者

ステップ 2 : ISEでOpenAPIを有効にします。

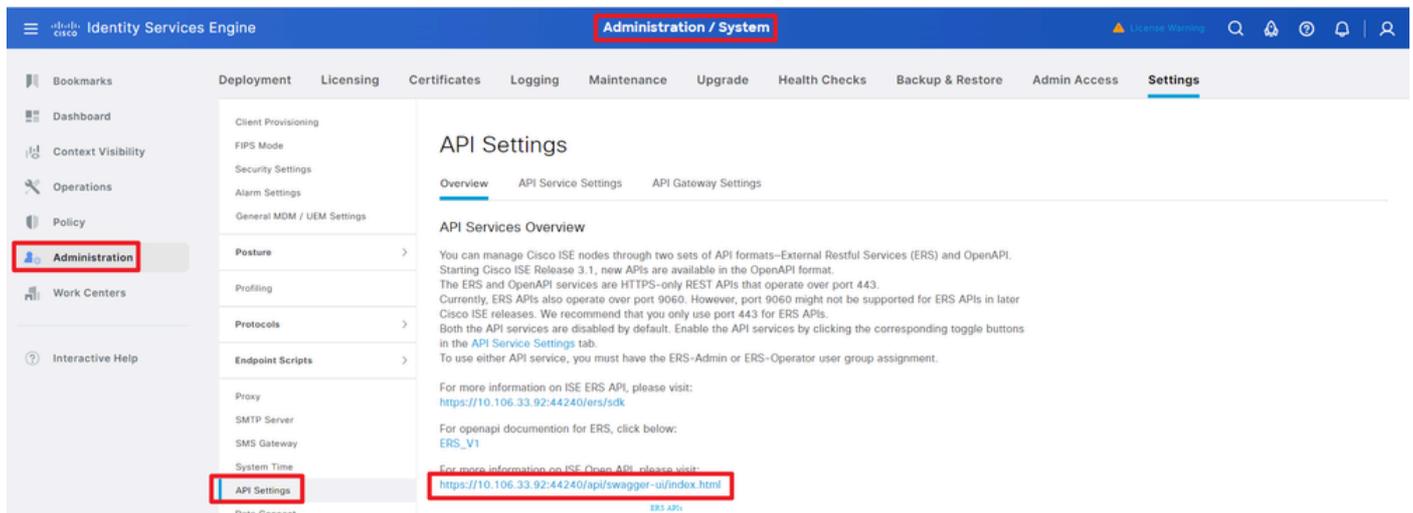
ISEでは、オープンAPIはデフォルトで無効になっています。有効にするには、に移動します。
[管理]>[システム]>[設定]>[API設定]>[APIサービス設定].OpenAPIオプションを切り替えます。クリック 保存します。 .



OpenAPIの有効化

ステップ 3 : ISE OpenAPIを確認します。

移動先 : [管理]>[システム]>[設定]>[API設定]>[概要].OpenAPIをクリックしてリンクにアクセスします。



OpenAPIにアクセス

Pythonの例

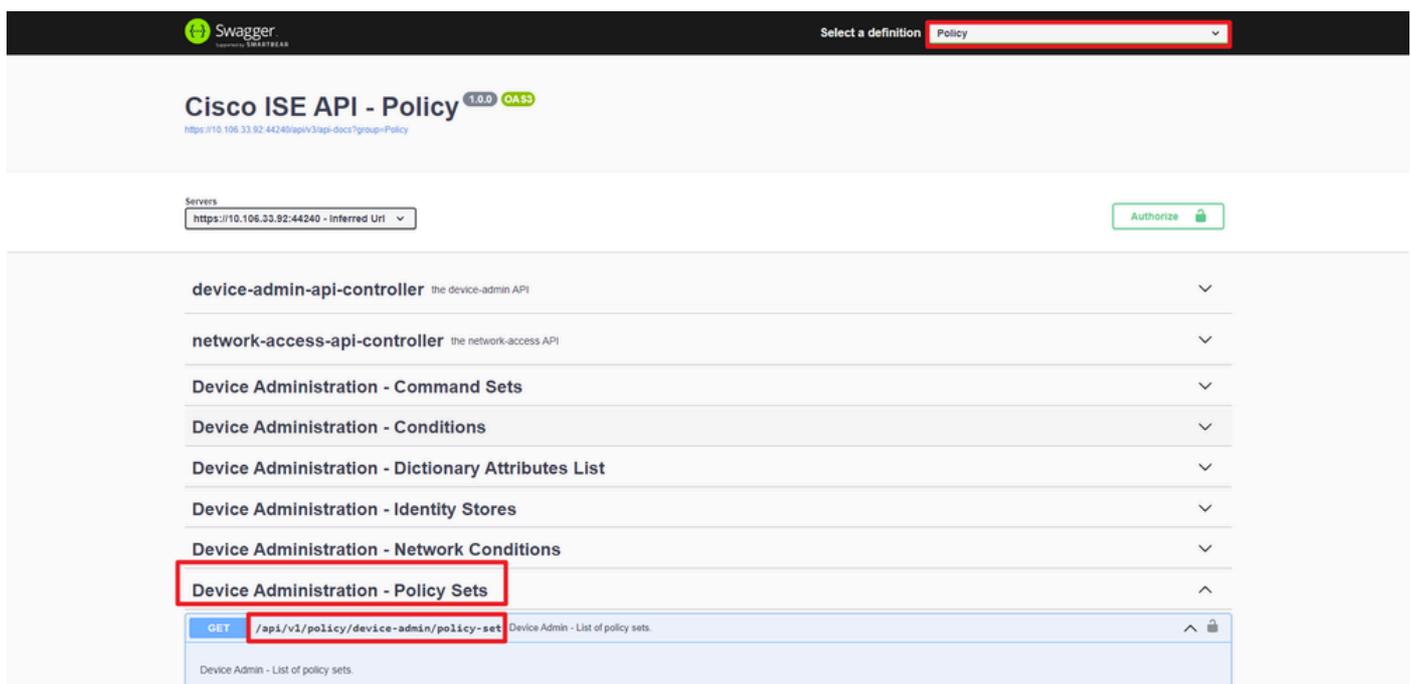
デバイス管理者 – ポリシーセットの一覧

このAPIは、デバイス管理ポリシーセット情報を取得します。

ステップ 1 : APIコールに必要な情報。

メソッド	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ 2 : デバイスマネージャポリシーセット情報の取得に使用されるURLを見つけます。



API URI(API URI)

ステップ 3 : これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

```
<#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())

```

次に、予想される出力例を示します。

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

Dデバイス管理者 – 認証ルールの取得

このAPIは、特定のポリシーセットの認証ルールを取得します。

ステップ 1 : APIコールに必要な情報。

メソッド	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authentication
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ 2 : 認証ルール情報の取得に使用するURLを探します。

The screenshot shows the Swagger UI for the Cisco ISE API - Policy. The 'Servers' dropdown is set to 'https://10.106.33.92:44240 - Inferred Uri'. A list of API endpoints is displayed, with 'Device Administration - Authentication Rules' highlighted in red. Below this, the endpoint details are shown, including the method 'GET' and the full API URI: '/api/v1/policy/device-admin/policy-set/{policyId}/authentication'.

API URI(API URI)

ステップ 3 : これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスとの接続が良好であることを確認します。

<#root>

```

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

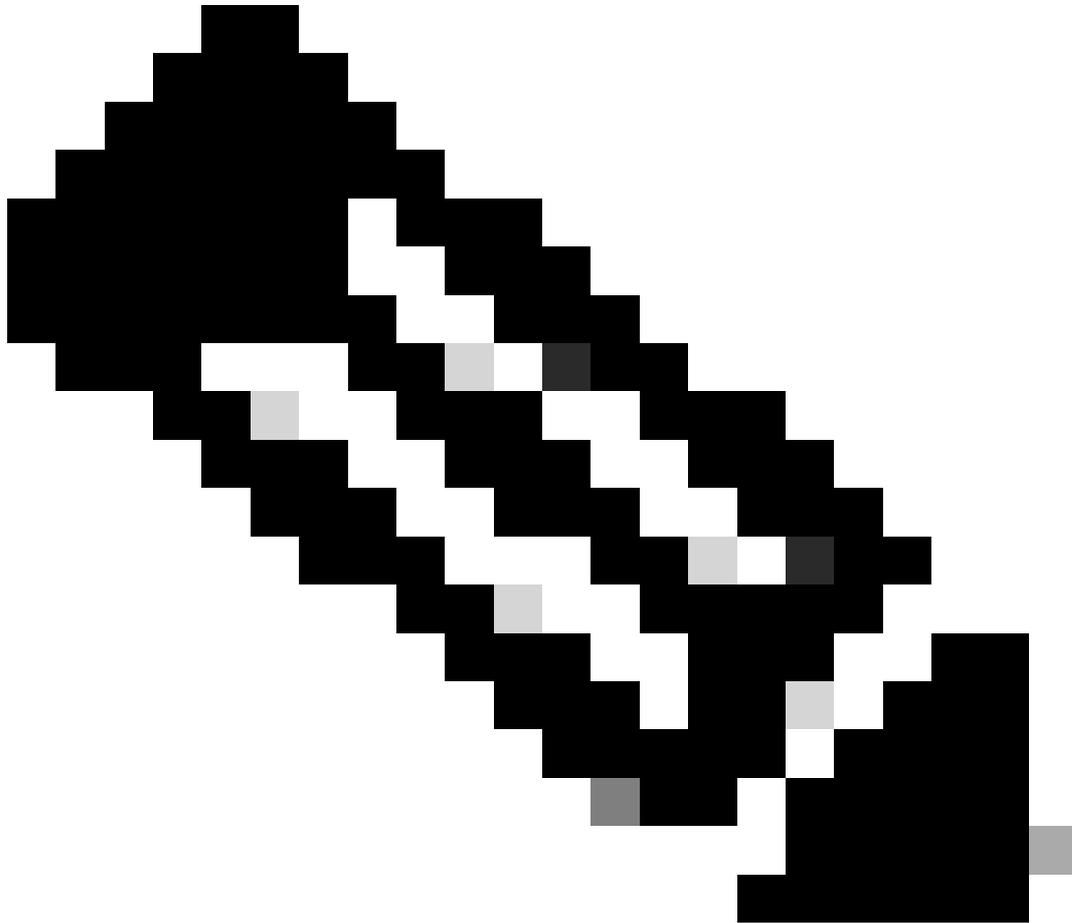
if __name__ == "__main__":

    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())
```



注:IDは、「デバイス管理者 – ポリシーセットのリスト」のステップ3のAPI出力からのものです。たとえば、41ed8579-429b-42a8-879e-61861cb82bbfはTACACSのデフォルトポリシーセットです。

次に、予想される出力例を示します。

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

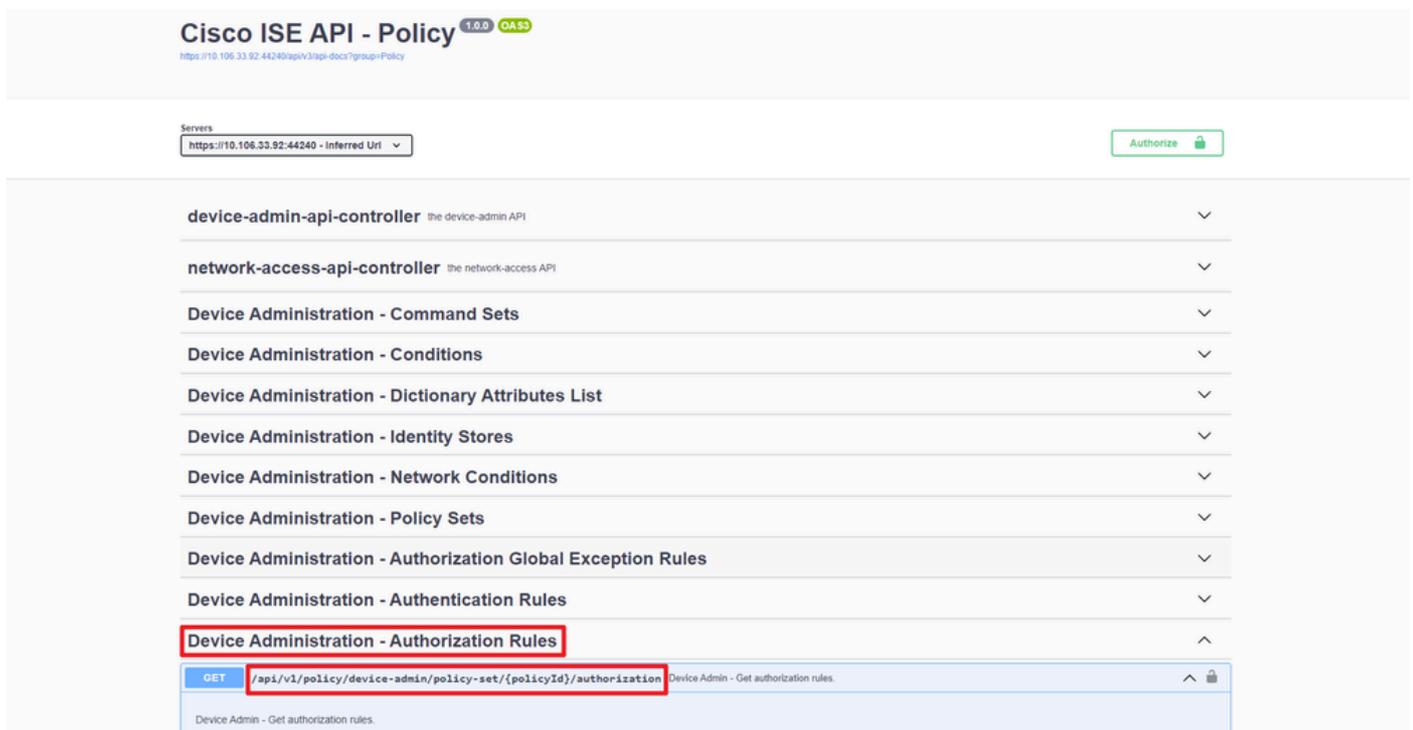
デバイス管理者 – 許可ルールの取得

このAPIは、特定のポリシーセットの認可ルールを取得します。

ステップ 1 : APIコールに必要な情報。

メソッド	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authorization
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ 2 : 許可ルール情報の取得に使用されるURLを探します。



API URI(API URI)

ステップ 3 : これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

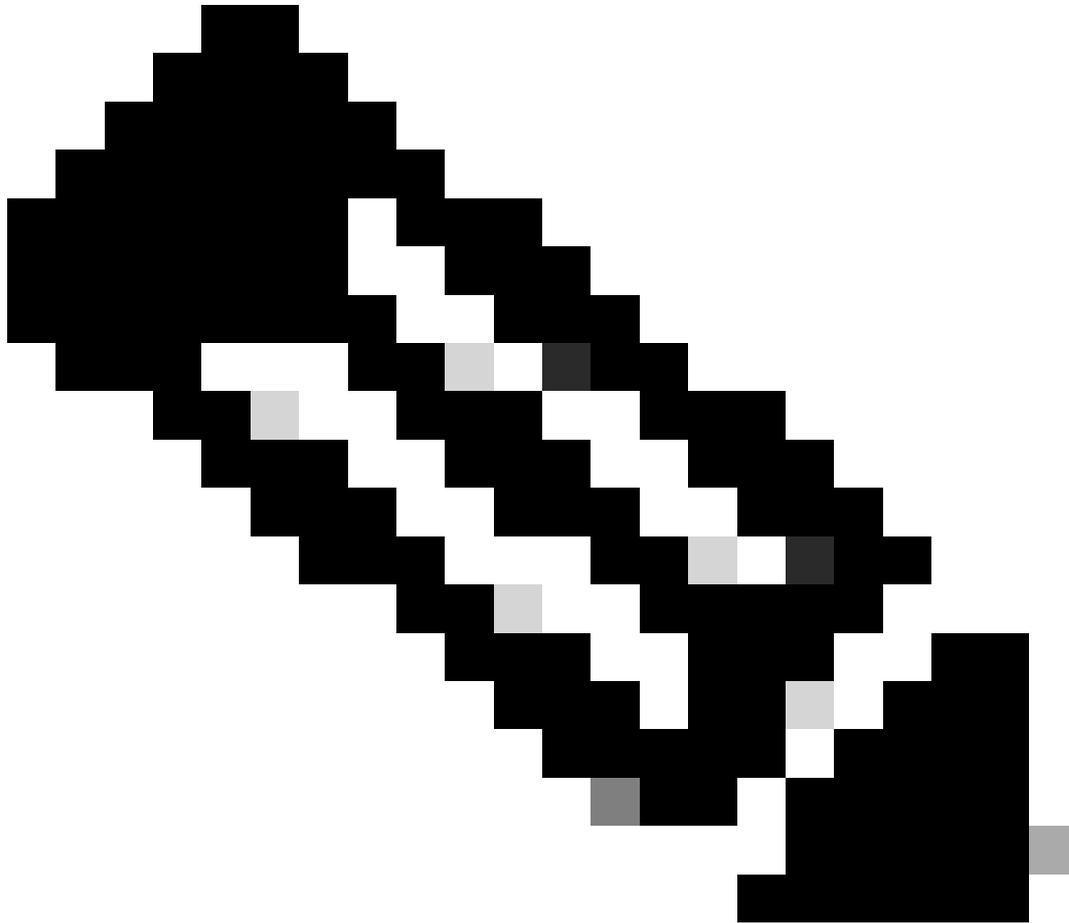
ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#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/authorization" 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:")
```



注:IDは、「デバイス管理者 – ポリシーセットのリスト」のステップ3のAPI出力からのものです。たとえば、41ed8579-429b-42a8-879e-61861cb82bbfはTACACSのデフォルトポリシーセットです。

次に、予想される出力例を示します。

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'}}
```

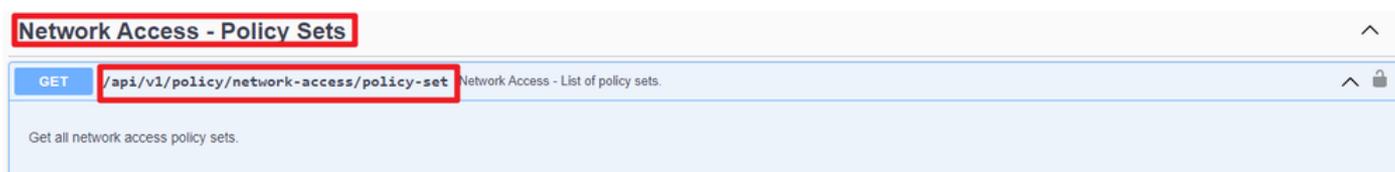
ネットワークアクセス：ポリシーセットのリスト

このAPIは、ISE導入のネットワークアクセスポリシーセットを取得します。

ステップ 1：APIコールに必要な情報。

メソッド	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ 2：特定のISEノード情報を取得するために使用されるURLを見つけます。



API URI(API URI)

ステップ 3：これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユーザー名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#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())

```

次に、予想される出力例を示します。

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

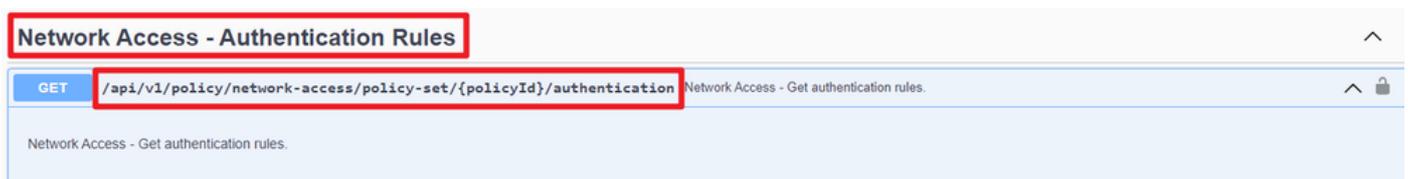
ネットワークアクセス – 認証ルールの取得

このAPIは、特定のポリシーセットの認証ルールを取得します。

ステップ 1：APIコールに必要な情報。

メソッド	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authentication
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ 2：認証ルール情報の取得に使用するURLを探します。



API URI(API URI)

ステップ 3：これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユーザー名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#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())
```



注：このIDは、「ネットワークアクセス：ポリシーセットのリスト」の手順3のAPI出力から取得されます。たとえば、ba71a417-4a48-4411-8bc3-d5df9b115769はBGL_CFME02-FMCです。

次に、予想される出力例を示します。

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

ネットワークアクセス – 許可ルールの取得

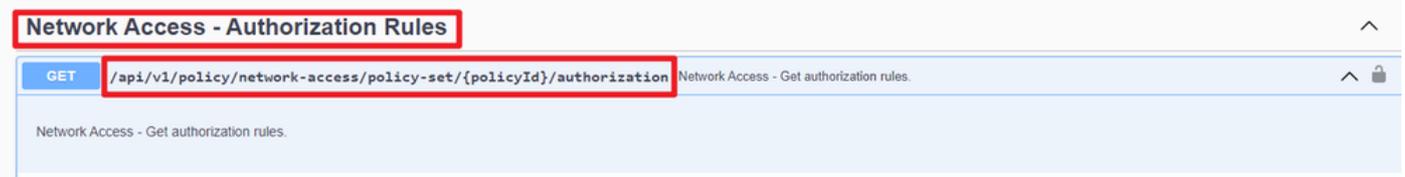
このAPIは、特定のポリシーセットの認可ルールを取得します。

ステップ 1：APIコールに必要な情報。

メソッド	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/network-

	access/policy-set/<ID-Of-Policy-Set>/authorization (許可)
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ 2 : 許可ルール情報の取得に使用されるURLを探します。



API URI(API URI)

ステップ 3 : これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

<#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"
```

```
)
```

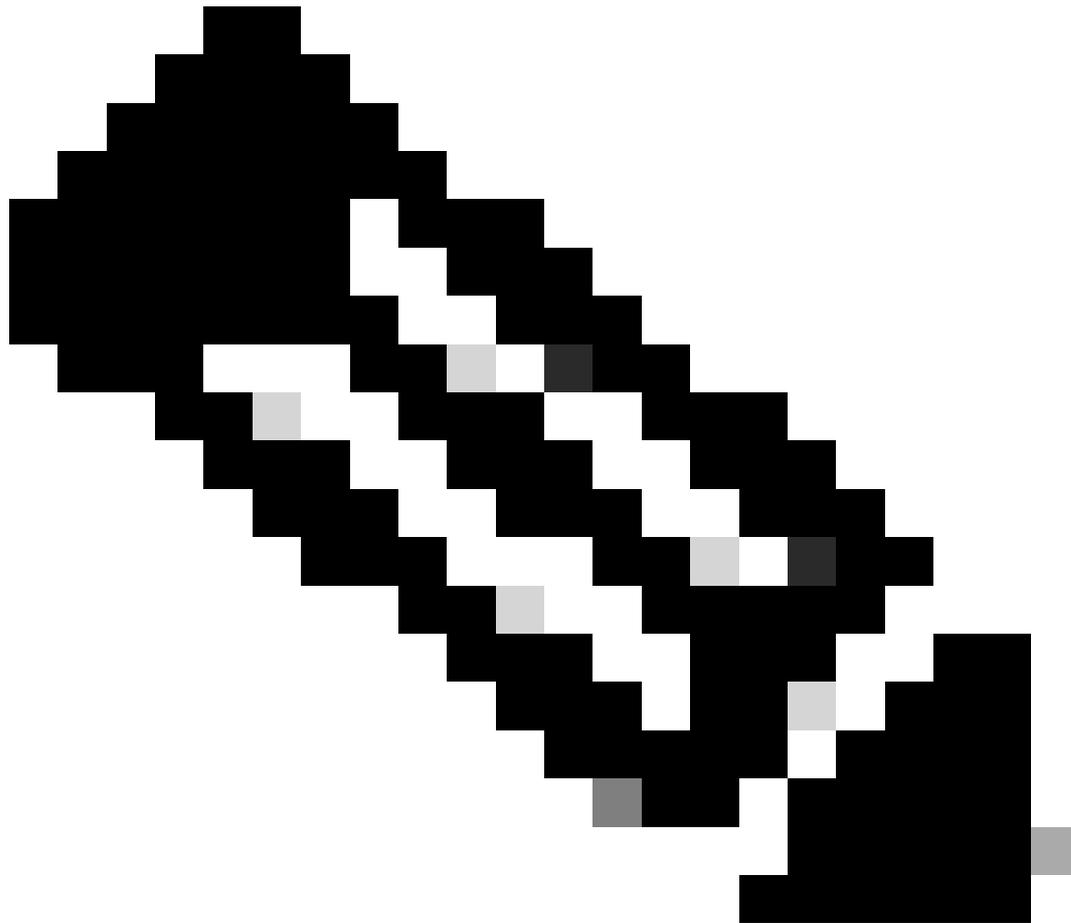
```
    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
```

```
    print("Return Code:")
```

```
    print(response.status_code)
```

```
    print("Expected Outputs:")
```

```
    print(response.json())
```



注:IDは、「ネットワークアクセス：ポリシーセットのリスト」の手順3のAPI出力からのものです。たとえば、ba71a417-4a48-4411-8bc3-d5df9b115769はBGL_CFME02-FMCです。

次に、予想される出力例を示します。

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

トラブルシュート

OpenAPIに関連する問題をトラブルシューティングするには、デバッグログ設定ウィンドウで theapiservicecomponent のログレベルを DEBUG に設定します。

デバッグを有効にするには、Operations > Troubleshoot > Debug Wizard > Debug Log

Configuration > ISE Node > apiserviceの順に移動します。

The screenshot shows the Cisco Identity Services Engine (ISE) 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 Wizard" and shows the "Debug Level Configuration" for the "ISE-BGL-CFME01-PAN" node. A table lists various components and their log levels. The "apiservice" component is selected, and its log level is set to "DEBUG".

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サービスのデバッグ

デバッグログファイルをダウンロードするには、Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logsの順に移動します。

The screenshot shows the Cisco Identity Services Engine (ISE) 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 shows a list of nodes. The "ISE-DLC-CFME01-PSN" node is selected. The "Debug Wizard" section shows a table of debug log types. The "api-service" log type is selected, and its log files are listed.

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

デバッグログのダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。