

# Utiliser OpenAPI pour récupérer les informations de stratégie ISE sur ISE 3.3

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration sur ISE](#)

[Exemples Python](#)

[Device Admin - Liste Des Jeux De Stratégies](#)

[Administrateur de périphérique - Obtenir les règles d'authentification](#)

[Administrateur de périphérique - Obtenir les règles d'autorisation](#)

[Accès Réseau - Liste Des Jeux De Stratégies](#)

[Accès réseau - Obtenir les règles d'authentification](#)

[Accès réseau - Obtenir les règles d'autorisation](#)

[Dépannage](#)

---

## Introduction

Ce document décrit la procédure d'utilisation d'OpenAPI pour gérer Cisco Identity Services Engine (ISE) Policy (politique) .

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

### Composants utilisés

- ISE 3.3
- Python 3.10.0

The information in this document was created from the devices in a specific lab environment. All of

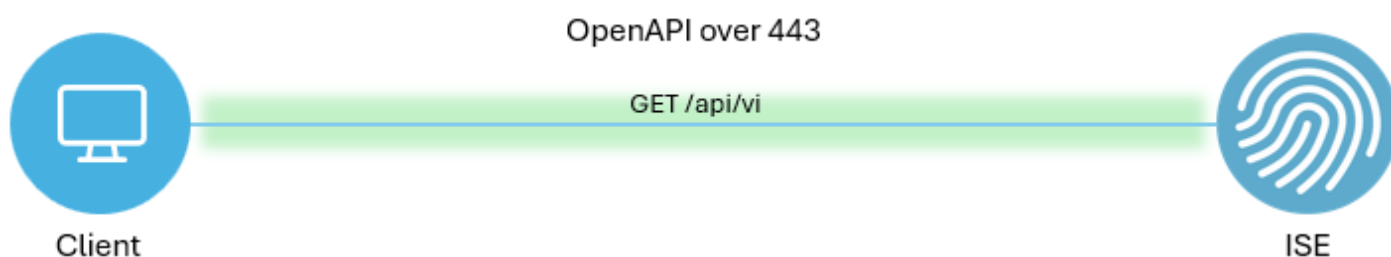
the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

À partir de Cisco ISE 3.1, de nouvelles API sont disponibles au format OpenAPI. La politique de gestion optimise la sécurité et la gestion du réseau en améliorant l'interopérabilité, l'automatisation, l'efficacité, la sécurité, l'innovation et la réduction des coûts. Cette politique permet à ISE de s'intégrer en toute transparence à d'autres systèmes, d'automatiser la configuration et la gestion, de fournir un contrôle d'accès granulaire, d'encourager l'innovation tierce et de simplifier les processus de gestion, réduisant ainsi les coûts de maintenance et augmentant le retour sur investissement global.

## Configurer

### Diagramme du réseau



Topologie

### Configuration sur ISE

Étape 1. Ajoutez un compte admin OpenAPI.

Pour ajouter un administrateur d'API, accédez à Administration > System > Admin Access > Administrators > Admin Users > Add.

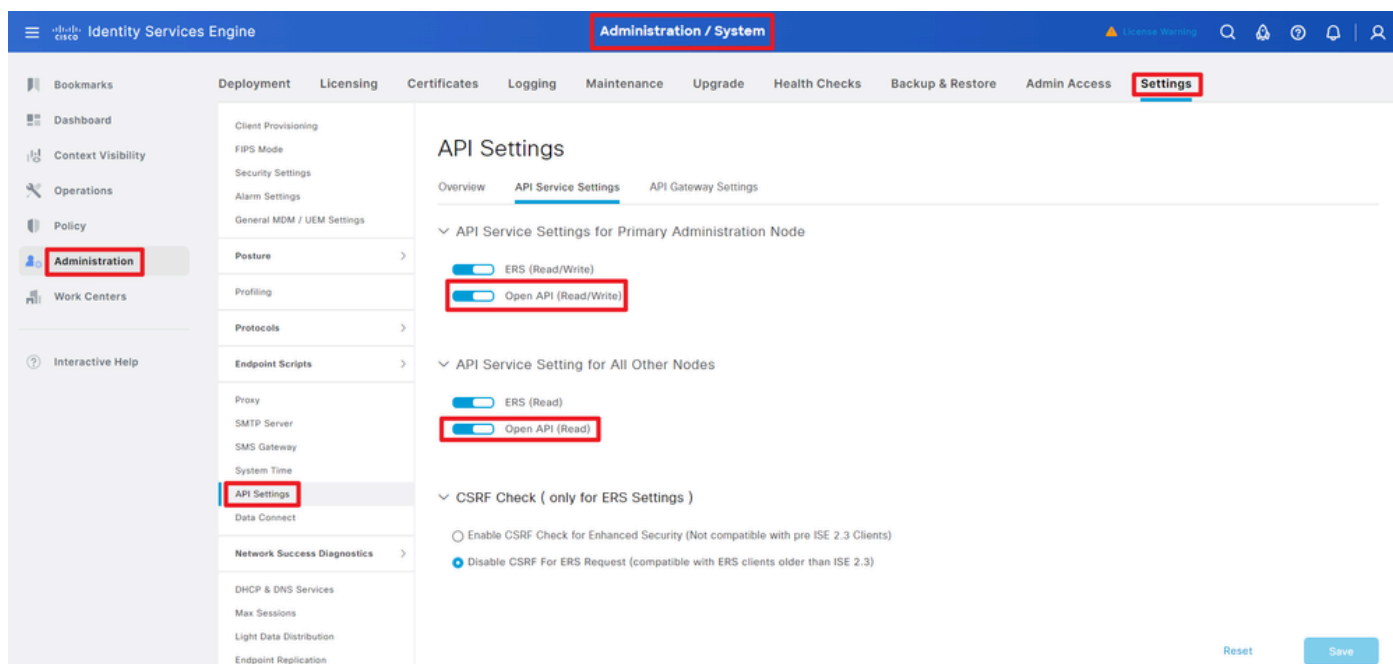
Le screenshot montre l'interface d'administration Cisco Identity Services Engine. Le menu "Administration / System" est sélectionné. Dans le sous-menu "Admin Access", "Admin Users" est sélectionné. La page "Administrators" est affichée, montrant une liste de deux administrateurs :

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

Administrateur API

Étape 2. Activez OpenAPI sur ISE.

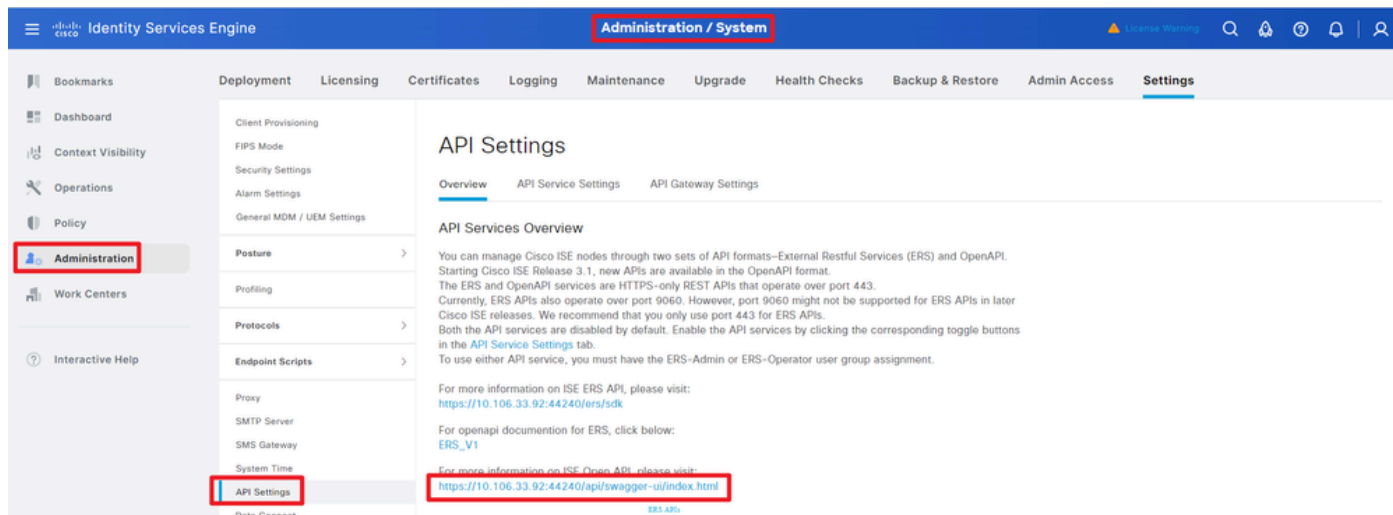
L'API ouverte est désactivée par défaut sur ISE. Pour l'activer, accédez à Administration > System > Settings > API Settings > API Service Settings. Activez les options OpenAPI. Cliquer Enregistrer.



Activer OpenAPI

### Étape 3. Explorez ISE OpenAPI.

Naviguez jusqu'à Administration > System > Settings > API Settings > Overview. Cliquez sur OpenAPI pour visiter le lien.



Visitez OpenAPI

## Exemples Python

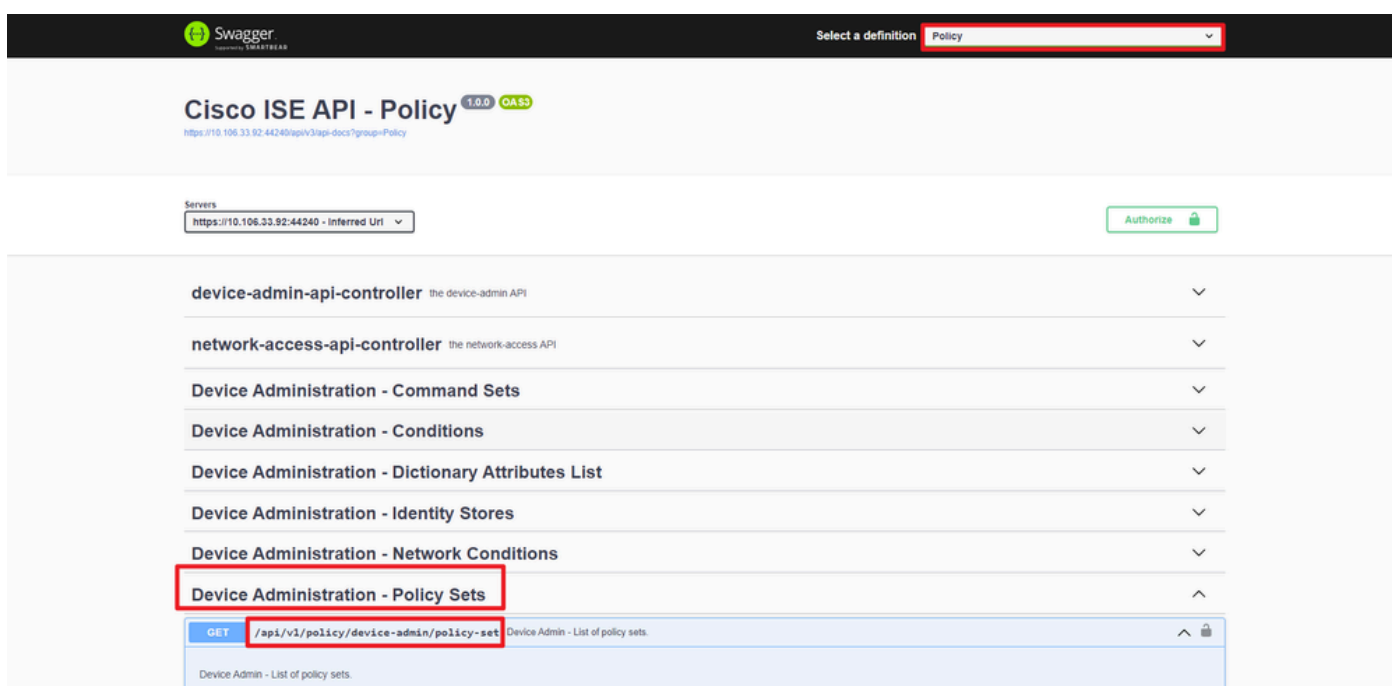
### Device Admin - Liste Des Jeux De Stratégies

Cette API récupère les informations des ensembles de stratégies d'administration de périphériques.

## Étape 1. Informations requises pour un appel API.

Méthode	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set
Identifiants	Utilisez les informations d'identification du compte OpenAPI.
Header (En-tête)	Accept (accepter) : application/json Content-Type (Type de contenu) : application/json

## Étape 2. Localisez l'URL utilisée pour récupérer les informations des ensembles de stratégies d'administration de périphériques.



The screenshot shows the Swagger UI for the Cisco ISE API. The 'Policy' definition is selected. The 'Device Administration - Policy Sets' endpoint is highlighted with a red box, showing the URL '/api/v1/policy/device-admin/policy-set'.

URI API

## Étape 3. Ceci est un exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer en tant que fichier python à exécuter.

Assurez-vous d'une bonne connectivité entre ISE et le périphérique exécutant l'exemple de code 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())

```

Voici l'exemple des résultats attendus.

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

## DAdministrateur de périphérique - Obtenir les règles d'authentification

Cette API récupère les règles d'authentification d'un ensemble de stratégies particulier.

Étape 1. Informations requises pour un appel API.

Méthode	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authentication
Identifiants	Utilisez les informations d'identification du compte OpenAPI.
Header (En-tête)	Accept (accepter) : application/json Content-Type (Type de contenu) : application/json

Étape 2. Localisez l'URL utilisée pour récupérer les informations de règle d'authentification.

URI API

Étape 3. Ceci est un exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer en tant que fichier python à exécuter.

Assurez-vous d'une bonne connectivité entre ISE et le périphérique exécutant l'exemple de code python.

<#root>

```

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

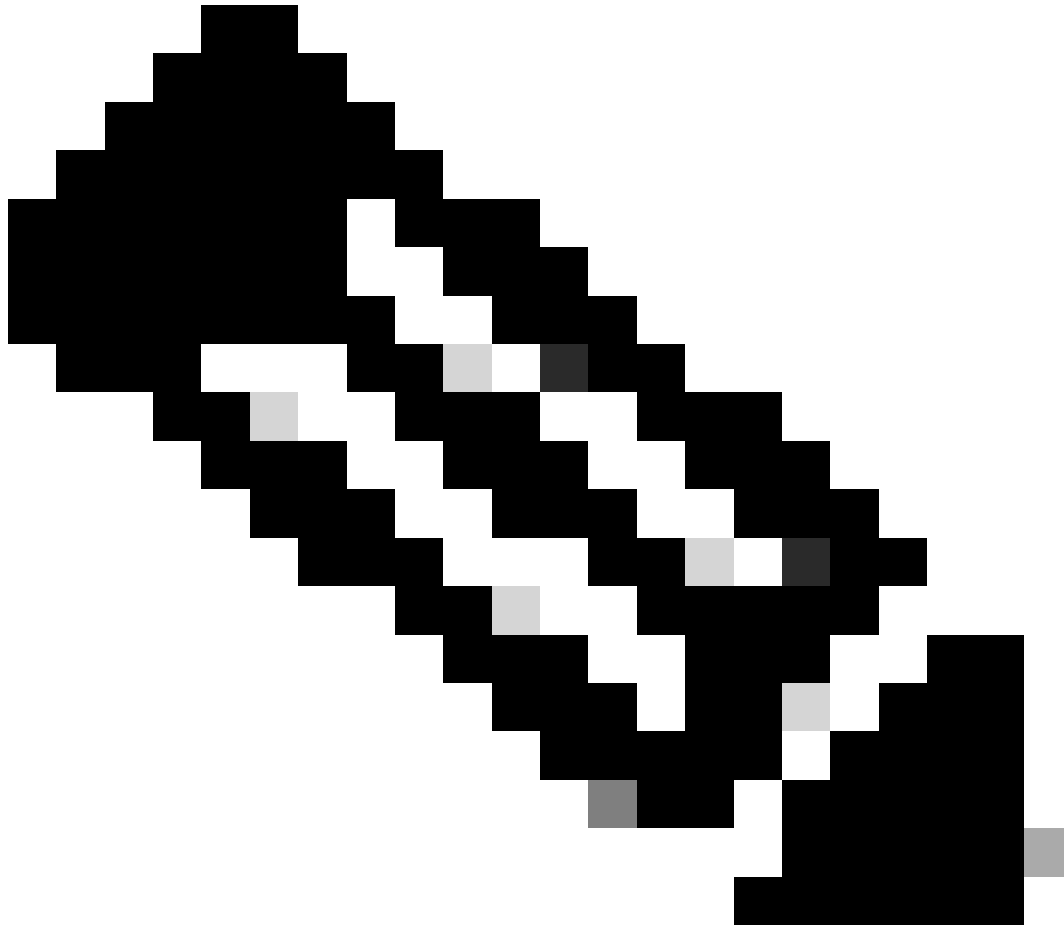
    url = "
https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authentication
"
    headers = {
"Accept": "application/json", "Content-Type": "application/json"
}
    basicAuth = HTTPBasicAuth(
"ApiAdmin", "Admin123"
)

    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
    print("Return Code:")
    print(response.status_code)

```

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

---



Remarque : l'ID provient des résultats de l'API à l'étape 3 de Device Admin - List Of Policy Sets. Par exemple, 41ed8579-429b-42a8-879e-61861cb82bbf est un jeu de stratégies TACACS par défaut.

---

Voici l'exemple des résultats attendus.

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

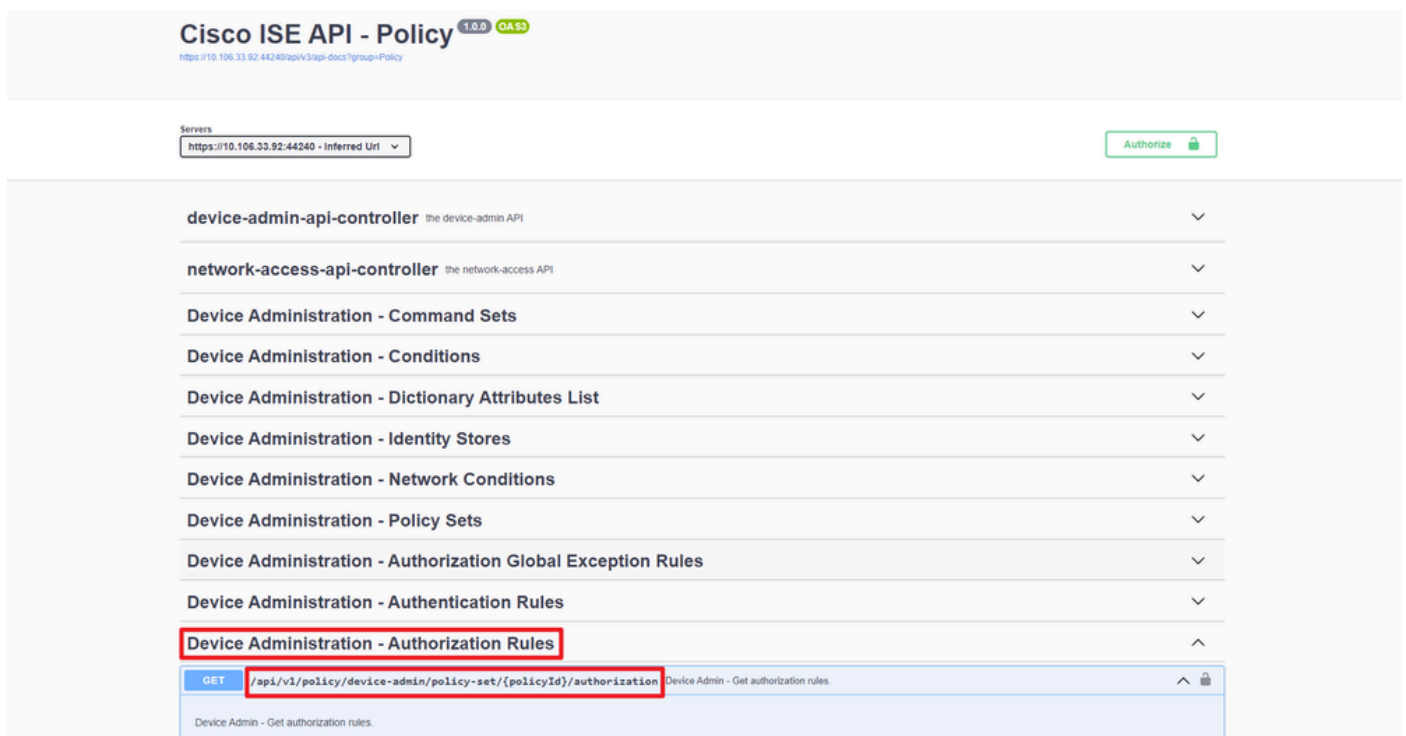
Administrateur de périphérique - Obtenir les règles d'autorisation

Cette API récupère les règles d'autorisation d'un ensemble de stratégies particulier.

Étape 1. Informations requises pour un appel API.

Méthode	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authorization
Identifiants	Utilisez les informations d'identification du compte OpenAPI.
Header (En-tête)	Accept (accepter) : application/json Content-Type (Type de contenu) : application/json

Étape 2. Localisez l'URL utilisée pour récupérer les informations de règle d'autorisation.



URI API

Étape 3. Ceci est un exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer en tant que fichier python à exécuter.

Assurez-vous d'une bonne connectivité entre ISE et le périphérique exécutant l'exemple de code python.

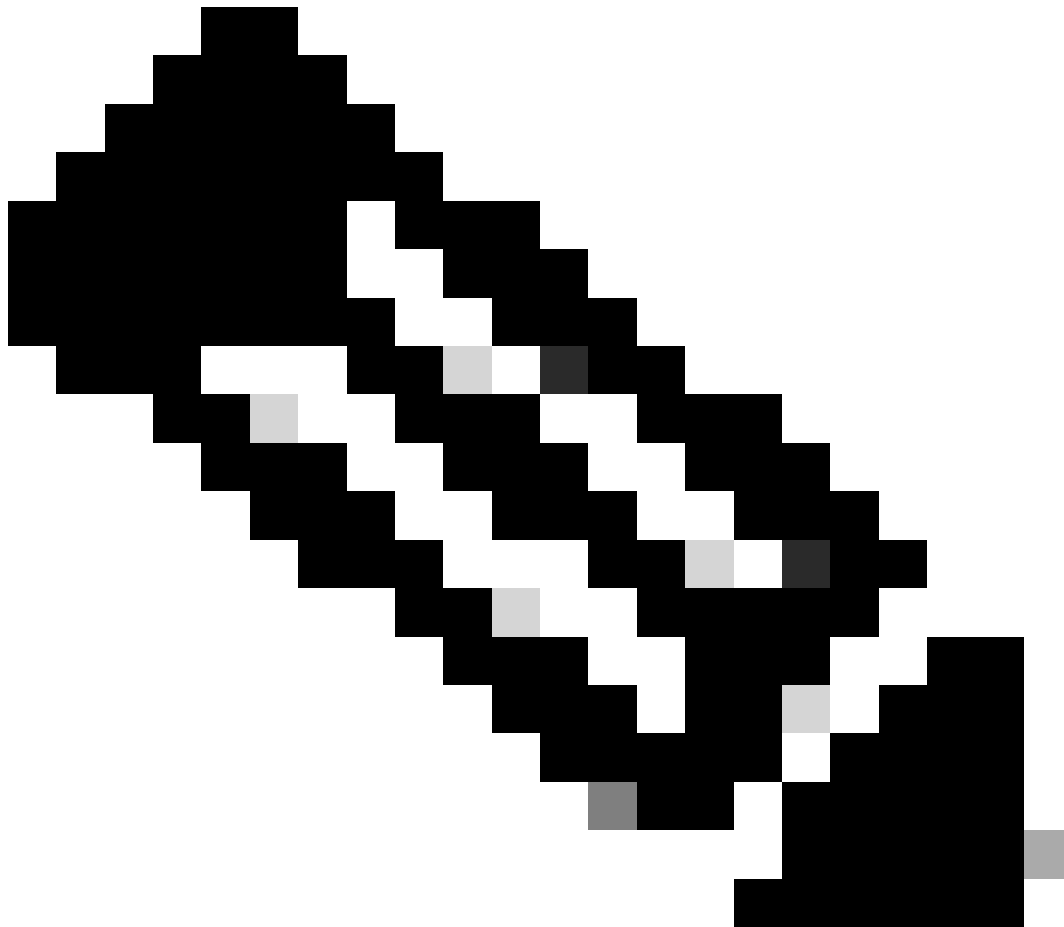
<#root>

```
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:")
```

---



Remarque : l'ID provient des résultats de l'API à l'étape 3 de Device Admin - List Of Policy Sets. Par exemple, 41ed8579-429b-42a8-879e-61861cb82bbf est un jeu de stratégies TACACS par défaut.

---

Voici l'exemple des résultats attendus.

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'}
```

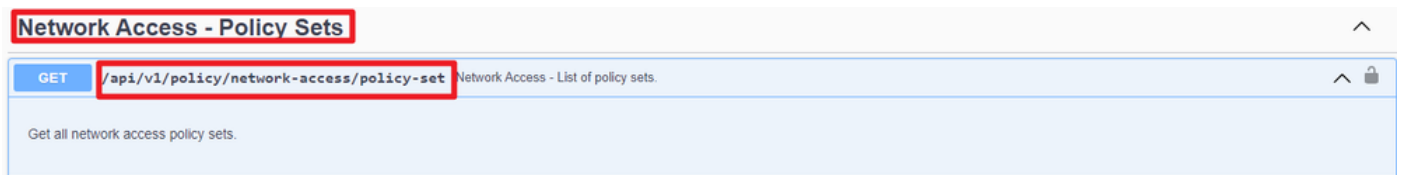
## Accès Réseau - Liste Des Jeux De Stratégies

Cette API récupère les ensembles de politiques d'accès réseau des déploiements ISE.

Étape 1. Informations requises pour un appel API.

Méthode	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set
Identifiants	Utilisez les informations d'identification du compte OpenAPI.
Header (En-tête)	Accept (accepter) : application/json Content-Type (Type de contenu) : application/json

Étape 2. Localisez l'URL utilisée pour récupérer les informations de noeud ISE spécifiques.



URI API

Étape 3. Ceci est un exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer en tant que fichier python à exécuter.

Assurez-vous d'une bonne connectivité entre ISE et le périphérique exécutant l'exemple de code 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())

```

Voici l'exemple des résultats attendus.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': False, 'id': 'ba71a417-4a48-4411-8bc3-d5df9b115769', 'name': 'BGL\_CFME0

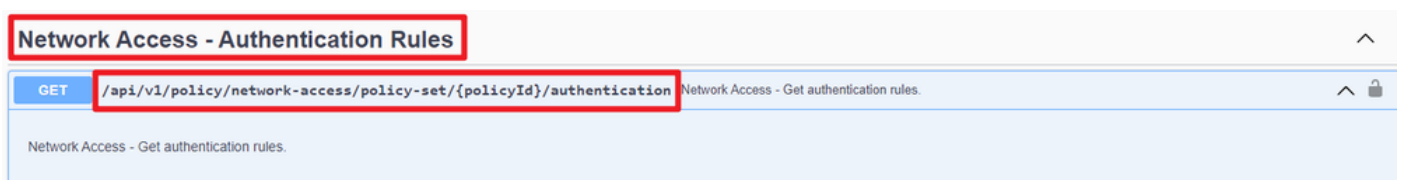
## Accès réseau - Obtenir les règles d'authentification

Cette API récupère les règles d'authentification d'un ensemble de stratégies particulier.

Étape 1. Informations requises pour un appel API.

Méthode	GET
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authentication
Identifiants	Utilisez les informations d'identification du compte OpenAPI.
Header (En-tête)	Accept (accepter) : application/json Content-Type (Type de contenu) : application/json

Étape 2. Localisez l'URL utilisée pour récupérer les informations de la règle d'authentification.



URI API

Étape 3. Ceci est un exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer en tant que fichier python à exécuter.

Assurez-vous d'une bonne connectivité entre ISE et le périphérique exécutant l'exemple de code

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())
```

---

Remarque : l'ID provient des résultats de l'API à l'étape 3 de Accès réseau - Liste des ensembles de politiques. Par exemple, `ba71a417-4a48-4411-8bc3-d5df9b115769` est `BGL_CFME02-FMC`.

---

Voici l'exemple des résultats attendus.

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

### Accès réseau - Obtenir les règles d'autorisation

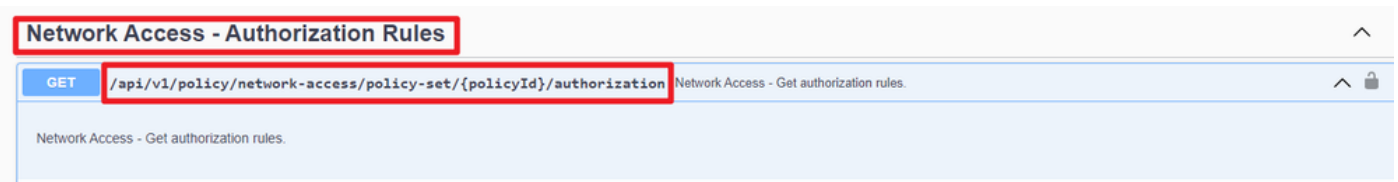
Cette API récupère les règles d'autorisation d'un ensemble de stratégies particulier.

Étape 1. Informations requises pour un appel API.

Méthode	GET
URL	<code>https://&lt;ISE-PAN-IP&gt;/api/v1/policy/network-</code>

	access/policy-set/<ID-Of-Policy-Set>/authorization
Identifiants	Utilisez les informations d'identification du compte OpenAPI.
Header (En-tête)	Accept (accepter) : application/json Content-Type (Type de contenu) : application/json

Étape 2. Localisez l'URL utilisée pour récupérer les informations de règle d'autorisation.



URI API

Étape 3. Ceci est un exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer en tant que fichier python à exécuter.

Assurez-vous d'une bonne connectivité entre ISE et le périphérique exécutant l'exemple de code 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())

```



Remarque : l'ID provient des résultats de l'API à l'étape 3 de Accès réseau - Liste des ensembles de politiques. Par exemple, ba71a417-4a48-4411-8bc3-d5df9b115769 est BGL\_CFME02-FMC.

---

Voici l'exemple des résultats attendus.

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

## Dépannage

Pour résoudre les problèmes liés aux API ouvertes, définissez le niveau de consignation pour le composant apiservicecomponent sur DEBUG dans la fenêtre Configuration du journal de débogage.

Pour activer le débogage, accédez à Opérations > Dépannage > Assistant de débogage > Configuration du journal de débogage > Noeud ISE > apiservice.

Identity Services Engine Operations / Troubleshoot

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration  
Debug Log Configuration

Node List > ISE-BGL-CFME01-PAN

### Debug Level Configuration

Edit Reset to Default Log Filter Enable Log Filter Disable

Component Name	Log Level	Description	Log file Name	Log Filter
<input type="radio"/> accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled
<input type="radio"/> Active Directory	WARN	Active Directory client internal messages	ad_agent.log	
<input type="radio"/> admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled
<input type="radio"/> admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled
<input type="radio"/> admin-license	INFO	License admin messages	ise-psc.log	Disabled
<input type="radio"/> ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled
<input type="radio"/> anc	INFO	Adaptive Network Control (ANC) debug...	ise-psc.log	Disabled
<input type="radio"/> api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled
<input checked="" type="radio"/> <b>apiservice</b>	<b>DEBUG</b>	ISE API Service logs	api-service.log	Disabled
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	...psc.log	Disabled
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log	Disabled

Save Cancel

Débogage du service API

Pour télécharger le fichier journal de débogage, accédez à Opérations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs.

Identity Services Engine Operations / Troubleshoot

Diagnostic Tools **Download Logs** Debug Wizard

ISE-BGL-CFME01-PAN  
ISE-BGL-CFME02-MNT  
ISE-DLC-CFME01-PSN  
ISE-DLC-CFME02-PSN  
ISE-RTP-CFME01-PAN  
ISE-RTP-CFME02-MNT

Delete Expand All Collapse All

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

Télécharger les journaux de débogage



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.