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



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.

≡							Administration / System			A 9	icense Warning	Q	۵	0 (2 A		
н	Bookmarks	Deployment Licensing	Ce	rtificates	Logging	Maintenance	Upgrade	Health	Checks	Backup & R	lestore	Admin Access	Settings				
	Dashboard	Authentication		Adam	inistrat												
명	Context Visibility	Authorization	>	Adm	inistrat	ors											
×	Operations	Administrators	Ŷ	/ Edit	+ Add	🛞 Change Status	Delete	Duplicate						26(6)	cted 0 T	All S	. ⊽
.0	Policy	Admin Users			Status	Name	Descrip	tion	First Name	Last Name	Email Ad	dress Admin Gro	NDS				
20	Administration	Admin Groups		0	Enabled	admin 😛	Default	Admin User				Super Adr	min				
di.	Work Centers	Settings	>		Enabled	a ApiAdmin						ERS Admi	n				
?	Interactive Help																

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.

∃ dentity Services Engine	Administration / System	🔺 License Warring 🔍 💩 🎯 🛱 🎗
Bookmarks Deployment Licensing C	ertificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
Dashboard Client Provisioning Id Context Visibility FIPS Mode Security Settings Alarm Bettings ID Policy General MOM / UEM Settings Id Administration Pesture Id Work Centers Protocols	API Settings Overview API Service Settings API Gateway Settings ~ API Service Settings for Primary Administration Node ERS (Read/Write) Open API (Read/Write)	
Interactive Help Endpoint Scripts > Proxy SMTP Server SMS Gateway Skytem Time API Settings > Data Connect Data Connect > DHCP & DNS Services Max Sessions Light Data Distribution	 API Service Setting for All Other Nodes ERS (Read) Open API (Read) CSRF Check (only for ERS Settings) Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients) Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3) 	Post Day
Endpoint Replication		INGRES DEVE

Activer OpenAPI

Étape 3. Explorez ISE OpenAPI.

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

≡	elinate Identity Services I	Engine		Administration / System					🔺 License Warning 🛛 🗛 🞯 🗘					
н	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
- 53	Dashboard	Client Provisionin	ng											
망	Context Visibility	FIPS Mode Security Settings		API S	API Servic	e Settings APLG	atoway Sottings							
- 2	Policy	Alarm Settings General MDM / U	JEM Settings	API Serv	ices Overvie	w	aterioy cettings							
8.	Administration	Posture		> You can m	anage Cisco ISE	nodes through two	sets of API forma	ts-External Restful Ser	vices (ERS) and OpenAPI.					
đ	Work Centers	Profiling		The ERS a Currently,	nd OpenAPI ser ERS APIs also o	vices are HTTPS-only perate over port 906	REST APIs that 0. However, port	operate over port 443. 9060 might not be sup	ported for ERS APIs in late	r:				
		Protocols		> Cisco ISE Both the A	eleases. We re PI services are	commend that you on disabled by default. E	ly use port 443 nable the API se	for ERS APIs. rvices by clicking the c	corresponding toggle buttor	15				
?	Interactive Help	Endpoint Scripts		> To use eith	service Settings er API service,	s tab. you must have the EF	S-Admin or ERS	Operator user group a	assignment.					
		Proxy SMTP Server SMS Gateway System Time		For more in https://10. For openaj ERS_V1	nformation on IS 106.33.92:442 pi documention	SE ERS API, please vis t0/ers/sdk for ERS, click below:	sit:							
	I	API Settings Data Connect		https://10.	106.33.92:442	40/api/swagger-ui/ind 183 AM	dex_html							

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</ise-pan-ip>				
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.

H Swagger,	Select a definition Policy v	
Cisco ISE API - Policy (III) (III)		
Servers https://10.106.33.92.44240 - Inferred Url v	Authorize 🔒	
device-admin-api-controller the device-admin API	*	
network-access-api-controller the network-access API	~	
Device Administration - Command Sets	~	
Device Administration - Conditions	~	
Device Administration - Dictionary Attributes List	~	
Device Administration - Identity Stores	~	
Device Administration - Network Conditions	~	
Device Administration - Policy Sets	^	
GET /api/vl/policy/device-admin/policy-set Device Admin - List of policy sets.	<u>^</u> ≜	
Device Admin - List of policy sets.		

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</id-of-policy- </ise-pan-ip>
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.

	Select a definition	Policy	~	
Cisco ISE API - Policy (100 033)				
Servers https://10.106.33.92;44240 - Inferred Uri			Authorize 🔒	
device-admin-api-controller the device-admin API			~	
network-access-api-controller the network-access API			~	
Device Administration - Command Sets			~	
Device Administration - Conditions			~	
Device Administration - Dictionary Attributes List			~	
Device Administration - Identity Stores			~	
Device Administration - Network Conditions			~	
Device Administration - Policy Sets			~	
Device Administration - Authorization Global Exception Rules			~	
Device Administration - Authentication Rules			^	
GET /api/vl/policy/device-admin/policy-set/{policyId}/authentication	ation rules.		^ ≞	
Device Admin - Get authentication rules.				

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/authent:
...
    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': 'True, 'Name': 'Default': 'True, 'Name': 'Default': 'True, 'Name': 'True, '

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</id-of-policy- </ise-pan-ip>
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.

Cisco ISE API - Policy (100) (100) https://10.105.33.82-44240hepv3/agi-dece?prougi-Policy		
Servers https://10.106.33.92:44240 - Inferred Url v	Authorize 🔒	
device-admin-api-controller the device-admin API	~	
network-access-api-controller the network-access API	~	
Device Administration - Command Sets	~	
Device Administration - Conditions	~	
Device Administration - Dictionary Attributes List	~	
Device Administration - Identity Stores	~	
Device Administration - Network Conditions	~	
Device Administration - Policy Sets	~	
Device Administration - Authorization Global Exception Rules	~	
Device Administration - Authentication Rules	~	
Device Administration - Authorization Rules	^	
GET /api/vl/policy/device-admin/policy-set/{policyId}/authorization Device Admin - Get authorization rules.	∧ ≙	
Device Admin - Get authorization rules.		

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 = "

 $\tt https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed 8579-429b-42a 8-879e-61861cb 82bbf/authorized and the set of the$

```
" 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

{'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '39d9f546-e58c-4f79-9856-c0a244b8a2ae', 'name': 'Default', 'hitCounts': 0, 'rank': 0, 'state': 'enable': 'enable': 'locale': 'loc

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</ise-pan-ip>
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.

Network Access - Policy Sets						
GET /api/v1/policy/network-access/policy-set Network Access - List of policy sets.	^ ≜					
Get all network access policy sets.						

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</id-of-policy- </ise-pan-ip>
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.

Network Access - Authentication Rules								
GET	/api/v1/policy/network-access/policy-set/{policyId}/authentication Network Access - Get authentication rules.	^ ≜						
Network Ar	ccess - Get authentication rules.							

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/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())
```



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': '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	https:// <ise-pan-ip>/api/v1/policy/network-</ise-pan-ip>

	access/policy-set/ <id-of-policy-< th=""></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.

Network Access - Authorization Rules	^
GET /api/v1/policy/network-access/policy-set/{policyId}/authorization Network Access - Get authorization rules.	^ ≜
Network Access - Get authorization rules.	

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.

≡	dentity Services	Engine	Operations / Troubleshoot					🔺 License Warning	Q	۵	0	٥	A
н	Bookmarks	Diagnostic Tools Download Le	ogs Det	oug Wizard									
ा हा २	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List Debu	ISE-BOL-CFMEDI-PAN	onfiguration							4	3
0	Policy		0 Edit	Seset to Default	Log Filter Enable	Log Filter Disable					All		7
20	Administration			Component Name	∧ Log Level	Description	Log file Name	Log Filter					
-fil	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled					
			0	Active Directory	WARN	Active Directory client internal messages	ad_agent.log						
?	Interactive Help		0	admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled					
			0	admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled					
			0	admin-license	INFO	License admin messages	ise-psc.log	Disabled					
			0	ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled					
			0	anc	INFO	Adaptive Network Control (ANC) debug	ise-psc.log	Disabled					
			0	api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled					
			0	apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled					
			0	bootstrap-wizard	INFO	Bootstrap wizard messages Save I Can	cel -psc.log	Disabled					
			0	ca-service	INFO	CA Service messages	caservice.log	Disabled					

Débogage du service API

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

≡	dentity Services	Engine	Ð		Operations / Troubleshoot				🔺 License Warning	Q	۵	0	$\varphi \mid \varphi$
Щ	Bookmarks	Diagn	nostic Tools	Download Logs	Debug Wiza	ard							
10	Dashboard		ISE-B	GL-CFME01-PAN									
명	Context Visibility		ISE-B	IGL-CFME02-MNT	Delete	2 [®] Expand All S≩Collapse A		Berry Andrea	0 1				
*	Operations		E ISE-D	C-CEME02-PSN	Debug	g Log Type	Log File	Description	Size				
0	Policy		ISE-R	TP-CFME01-PAN	✓ Applicatio	on Logs							
8.	Administration		ISE-R	TP-CFME02-MNT	> ad,	_agent (1) (100 KB)							_
ril.	Work Centers		×	,	> ai-	analytics (11) (52 KB) i-gateway (16) (124 KB)							
					\lor api	i-service (13) (208 KB)							
?	Interactive Help						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				

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.