

Uso di OpenAPI per recuperare le informazioni sulle policy ISE su ISE 3.3

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione su ISE](#)

[Esempi di Python](#)

[Amministratore Del Dispositivo - Elenco Di Set Di Criteri](#)

[Amministrazione dispositivi - Ottieni regole di autenticazione](#)

[Amministrazione dispositivi - Ottieni regole di autorizzazione](#)

[Accesso Alla Rete - Elenco Di Set Di Criteri](#)

[Accesso di rete - Ottieni regole di autenticazione](#)

[Accesso di rete - Ottieni regole di autorizzazione](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la procedura per l'utilizzo di OpenAPI per la gestione Cisco Identity Services Engine (ISE) Policy.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

- ISE 3.3
- Python 3.10.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

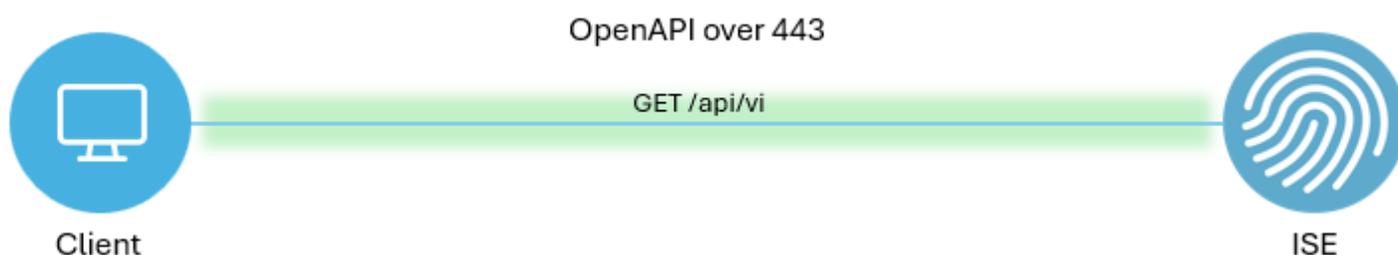
ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Da Cisco ISE 3.1 in poi, le nuove API sono disponibili in formato OpenAPI. La policy di gestione ottimizza la sicurezza e la gestione della rete migliorando l'interoperabilità, migliorando l'efficienza dell'automazione, rafforzando la sicurezza, promuovendo l'innovazione e riducendo i costi. Questa politica consente ad ISE di integrarsi facilmente con altri sistemi, ottenere una configurazione e una gestione automatizzate, fornire un controllo granulare dell'accesso, incoraggiare l'innovazione di terze parti e semplificare i processi di gestione, riducendo in tal modo i costi di manutenzione e aumentando il ritorno complessivo sull'investimento.

Configurazione

Esempio di rete

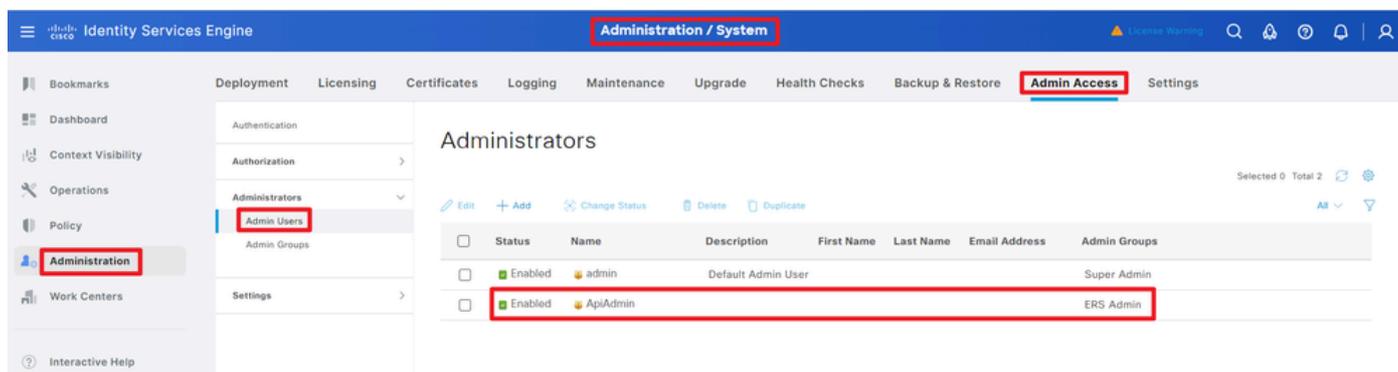


Topologia

Configurazione su ISE

Passaggio 1. Aggiungere un account amministratore OpenAPI.

Per aggiungere un amministratore API, selezionare Amministrazione > Sistema > Accesso amministratore > Amministratori > Utenti amministratori > Aggiungi.



Amministratore API

Passaggio 2. Abilitare OpenAPI su ISE.

Open API è disabilitato per impostazione predefinita su ISE. Per attivarlo, passare a Amministrazione > Sistema > Impostazioni > Impostazioni API > Impostazioni servizio API. Attivate o disattivate le opzioni di OpenAPI. Fare clic su Salva.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and 'Settings'. The left sidebar has 'Administration' highlighted. The main content area shows the 'API Settings' page with the following sections:

- API Service Settings for Primary Administration Node**
 - ERS (Read/Write)
 - Open API (Read/Write)
- 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)

Buttons for 'Reset' and 'Save' are visible at the bottom right.

Abilita OpenAPI

Passaggio 3. Scopri ISE OpenAPI.

Passa a Amministrazione > Sistema > Impostazioni > Impostazioni API > Panoramica. Fare clic su OpenAPI per visitare il collegamento.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and 'Settings'. The left sidebar has 'Administration' highlighted. The main content area shows the 'API Settings' page with the following sections:

- API Services Overview**

You can manage Cisco ISE nodes through two sets of API formats—External Restful Services (ERS) and OpenAPI. Starting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format. The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443. Currently, ERS APIs also operate over port 9060. However, port 9060 might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 443 for ERS APIs.

Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the **API Service Settings** tab.

To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.

For more information on ISE ERS API, please visit:
<https://10.106.33.92:44240/ers/sdk>

For openapi documentation for ERS, click below:
ERS_V1

For more information on ISE Open API, please visit:
<https://10.106.33.92:44240/api/swagger-ui/index.html>

The 'API Settings' menu item in the left sidebar is highlighted.

Visita OpenAPI

Esempi di Python

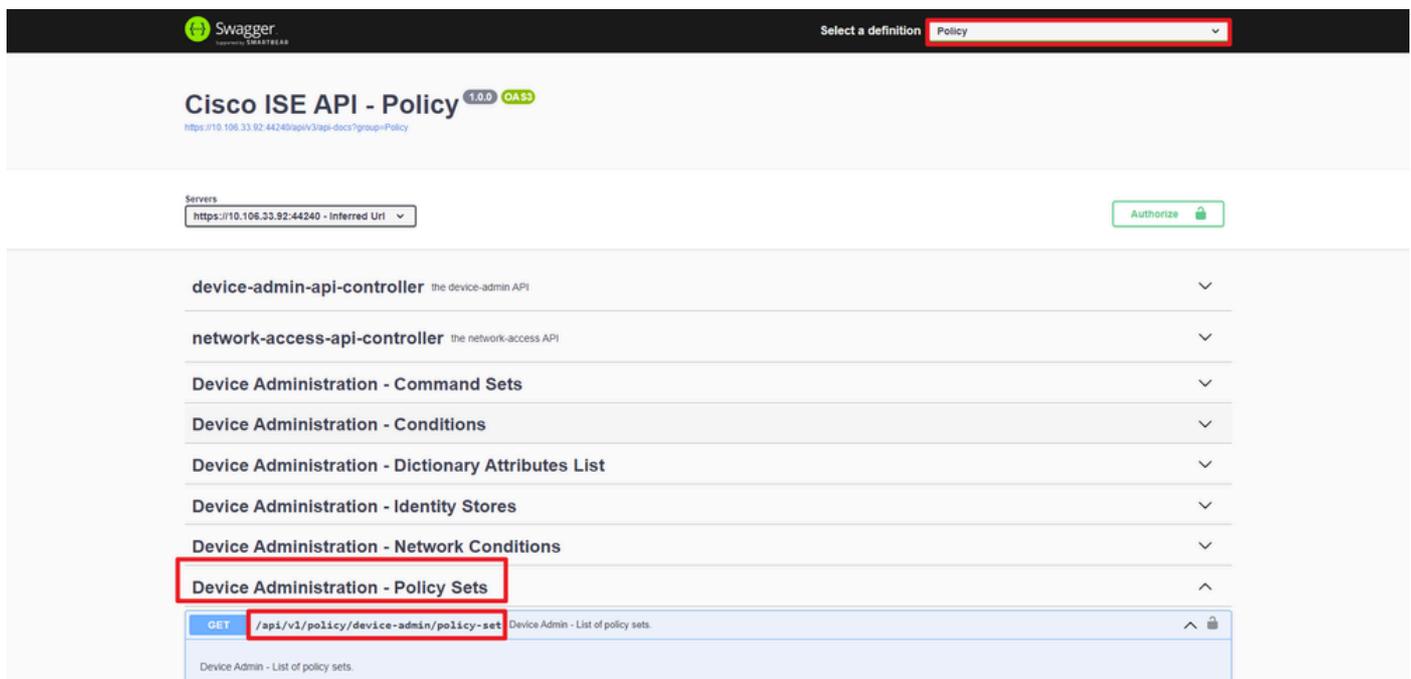
Amministratore Del Dispositivo - Elenco Di Set Di Criteri

Questa API recupera le informazioni sui set di criteri di amministrazione del dispositivo.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sui set di criteri di amministrazione del dispositivo.



URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

Verificare che la connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python sia buona.

<#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())

```

Questo è l'esempio degli output previsti.

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

DDevice Admin - Ottieni regole di autenticazione

Questa API recupera le regole di autenticazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authentication
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulle regole di autenticazione.

URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

Verificare che la connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python sia buona.

<#root>

```

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

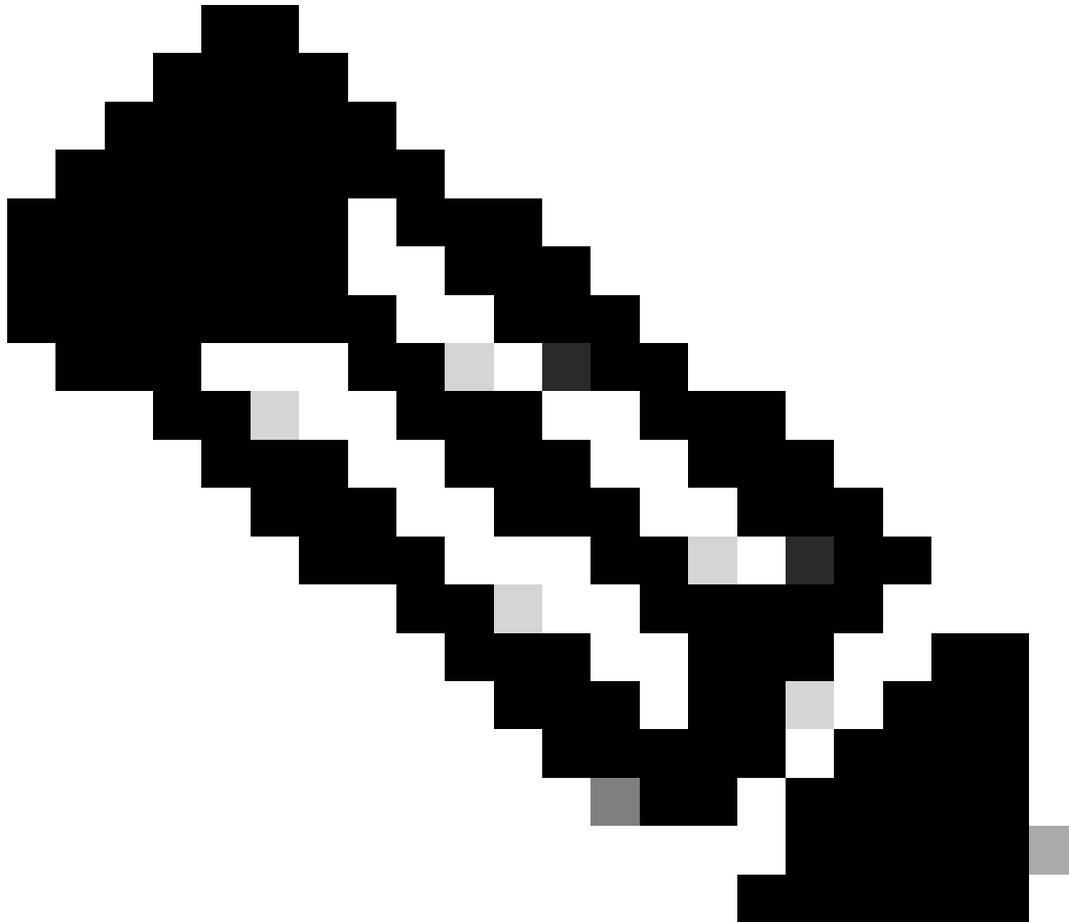
if __name__ == "__main__":

    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())
```



Nota: l'ID deriva dagli output API al passaggio 3 di Device Admin - List Of Policy Sets. Ad esempio, 41ed8579-429b-42a8-879e-61861cb82bbf è impostato come criterio predefinito di TACACS.

Questo è l'esempio degli output previsti.

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

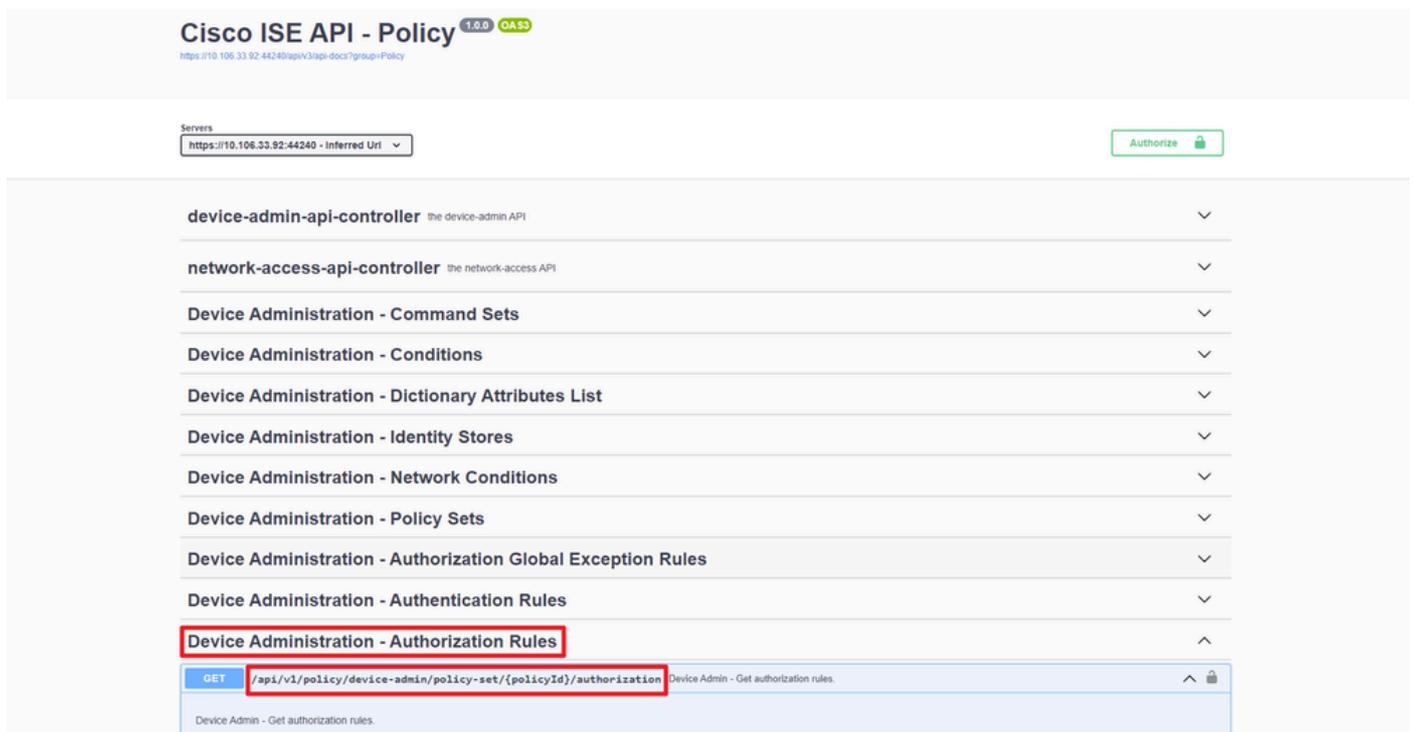
Amministrazione dispositivi - Ottieni regole di autorizzazione

Questa API recupera le regole di autorizzazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authorization
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulla regola di autorizzazione.



URI API

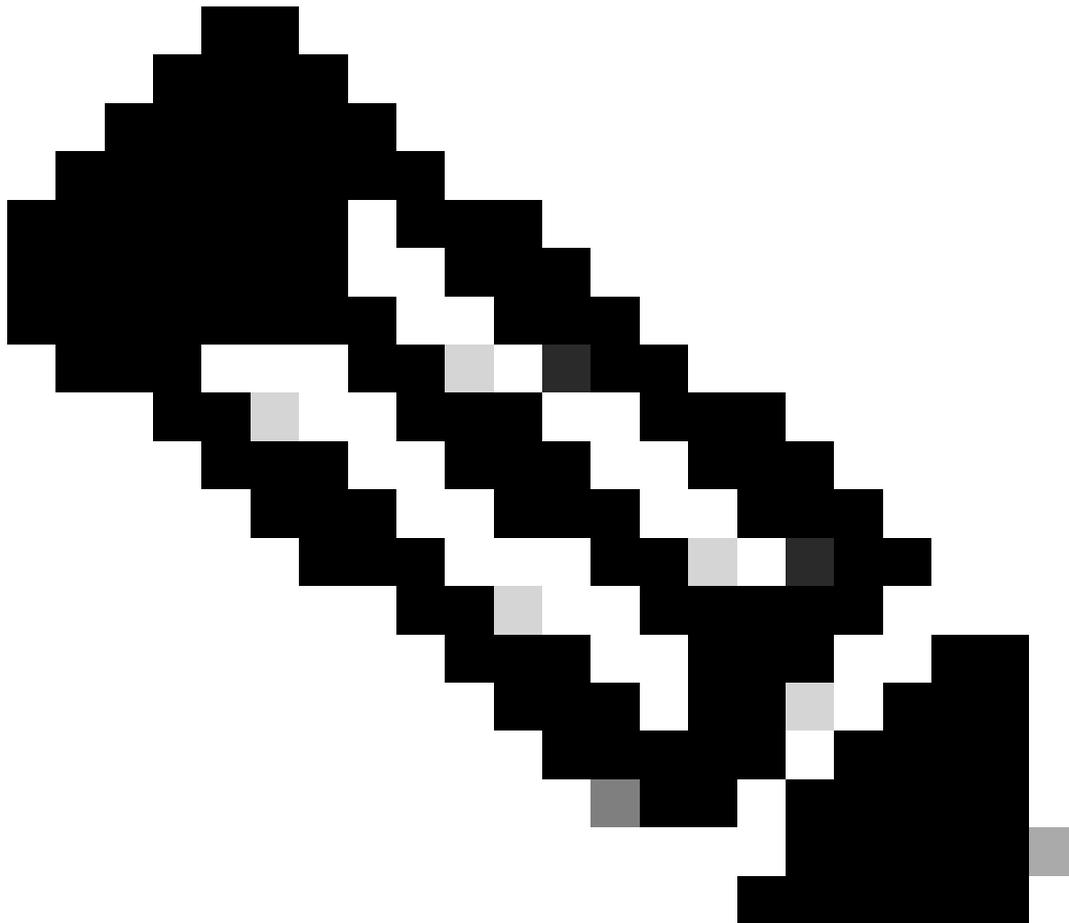
Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

Verificare che la connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python sia buona.

<#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:")
```



Nota: l'ID deriva dagli output API al passaggio 3 di Device Admin - List Of Policy Sets. Ad esempio, 41ed8579-429b-42a8-879e-61861cb82bbf è impostato come criterio predefinito di TACACS.

Questo è l'esempio degli output previsti.

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'}
```

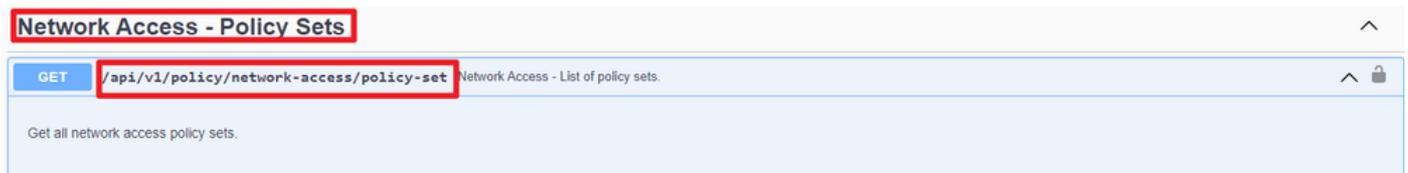
Accesso Alla Rete - Elenco Di Set Di Criteri

Questa API recupera i set di criteri di accesso alla rete delle distribuzioni ISE.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni specifiche del nodo ISE.



URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

Verificare che la connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python sia buona.

<#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())

```

Questo è l'esempio degli output previsti.

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

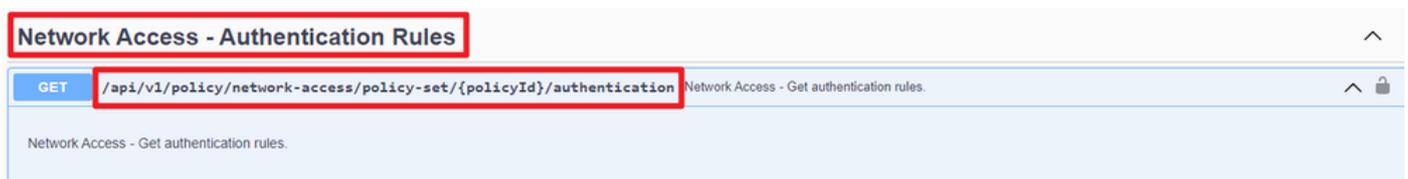
Accesso di rete - Ottieni regole di autenticazione

Questa API recupera le regole di autenticazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authentication
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulla regola di autenticazione.



URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

Verificare che la connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python sia buona.

<#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())
```

Nota: l'ID deriva dagli output API al passaggio 3 di Accesso alla rete - Elenco di set di criteri. Ad esempio, ba71a417-4a48-4411-8bc3-d5df9b115769 è BGL_CFME02-FMC.

Questo è l'esempio degli output previsti.

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

Accesso di rete - Ottieni regole di autorizzazione

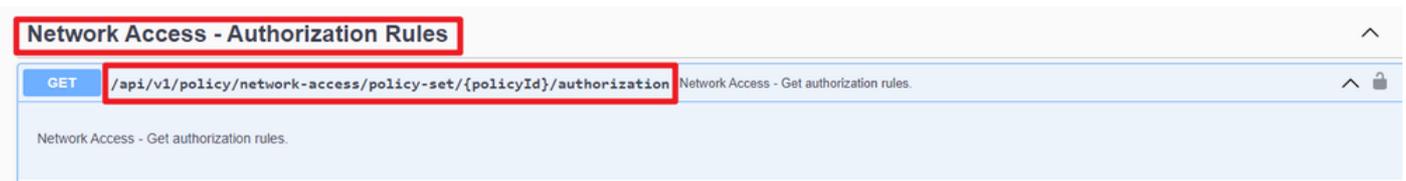
Questa API recupera le regole di autorizzazione di un set di criteri specifico.

Passaggio 1. Informazioni necessarie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/policy/network-

	access/policy-set/<ID-Of-Policy-Set>/authorization
Credenziali	Utilizzare le credenziali dell'account OpenAPI.
Intestazioni	Accetta : application/json Content-Type : application/json

Passaggio 2. Individuare l'URL utilizzato per recuperare le informazioni sulla regola di autorizzazione.



URI API

Passaggio 3. Questo è un esempio di codice Python. Copiare e incollare il contenuto. Sostituire l'ISE IP, il nome utente e la password. Salvare come file Python da eseguire.

Verificare che la connettività tra ISE e il dispositivo su cui è in esecuzione il codice Python sia buona.

<#root>

```

from requests.auth import HTTPBasicAuth
import requests

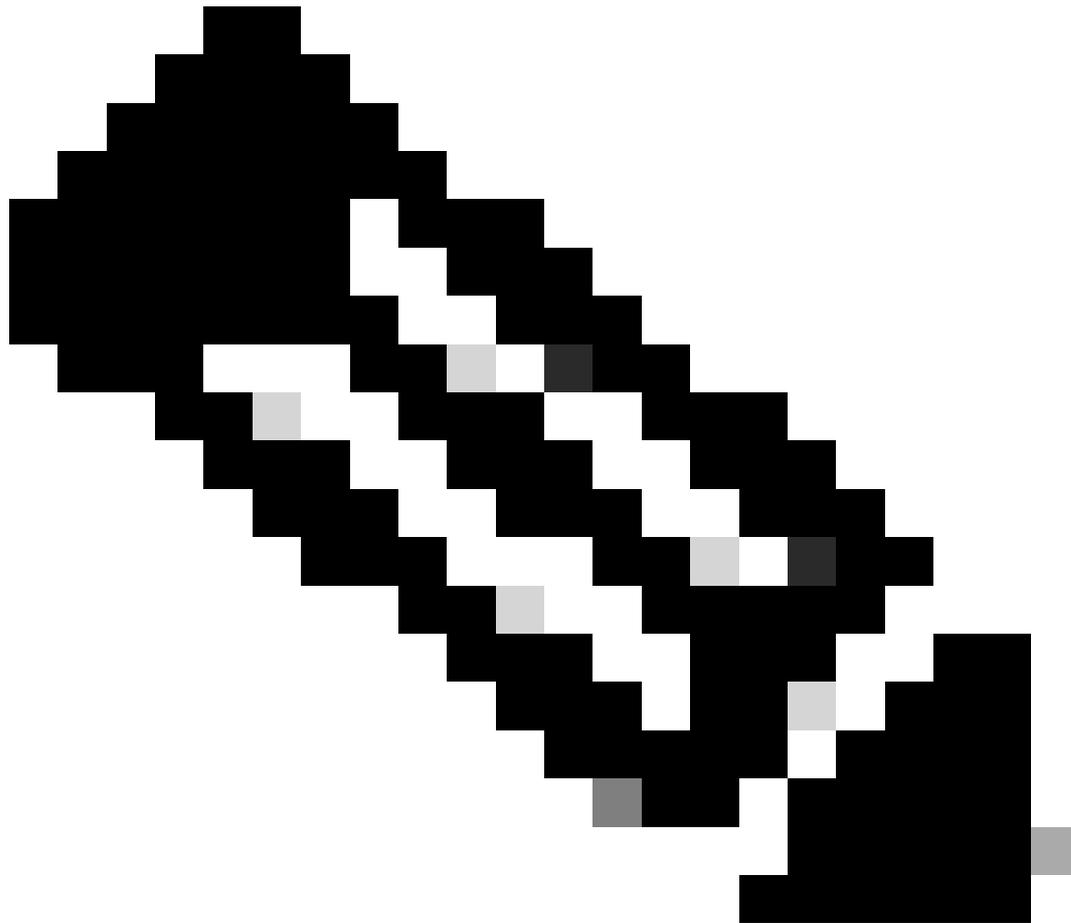
requests.packages.urllib3.disable_warnings()

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())

```



Nota: l'ID deriva dagli output API al passaggio 3 di Accesso alla rete - Elenco di set di criteri. Ad esempio, ba71a417-4a48-4411-8bc3-d5df9b115769 è BGL_CFME02-FMC.

Questo è l'esempio degli output previsti.

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

Risoluzione dei problemi

Per risolvere i problemi relativi alle OpenAPI, impostare il livello di log per apiservicecomponent su DEBUG nella finestra di configurazione del log di debug.

Per abilitare il debug, selezionare Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > apiservice.

Identity Services Engine **Operations / Troubleshoot** License Warning

Bookmarks Dashboard Context Visibility **Operations** Policy Administration Work Centers Interactive Help

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"/> apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	ise-psc.log	Disabled
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log	Disabled

Debug del servizio API

Per scaricare il file di log di debug, selezionare Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs (Operazioni > Risoluzione dei problemi > Log di download > Nodo PAN ISE > Log di debug).

Identity Services Engine **Operations / Troubleshoot** License Warning

Bookmarks Dashboard Context Visibility **Operations** Policy Administration Work Centers Interactive Help

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

Deletes 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

Scarica log di debug

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).