Uso di OpenAPI per ottenere informazioni sui certificati ISE su ISE 3.3

Sommario

Introduzione

In questo documento viene descritta la procedura per utilizzare openAPI per gestire il certificato Cisco Identity Services Engine (ISE).

Introduzione

Di fronte alla crescente complessità nella gestione e nella sicurezza della rete aziendale, Cisco ISE 3.1 introduce API in formato OpenAPI che semplificano la gestione del ciclo di vita dei certificati, offrendo un'interfaccia standardizzata e automatizzata per operazioni di certificazione efficienti e sicure, aiutando gli amministratori ad applicare procedure di sicurezza efficaci e a mantenere la conformità della rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

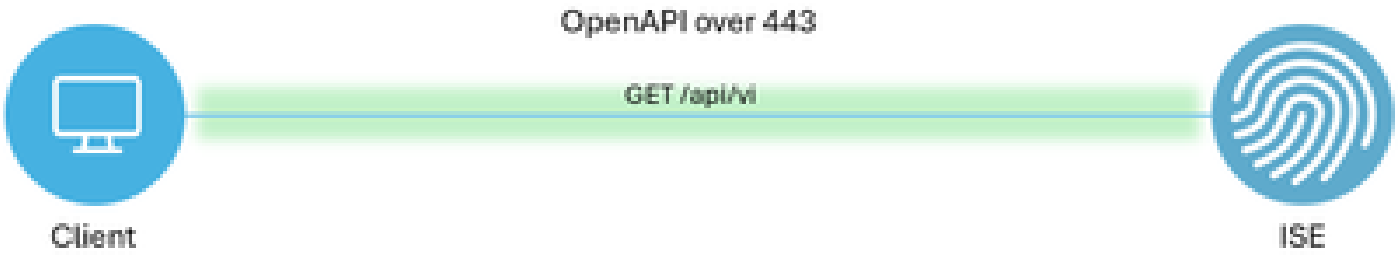
Componenti usati

- 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.

Configurazione

Esempio di rete

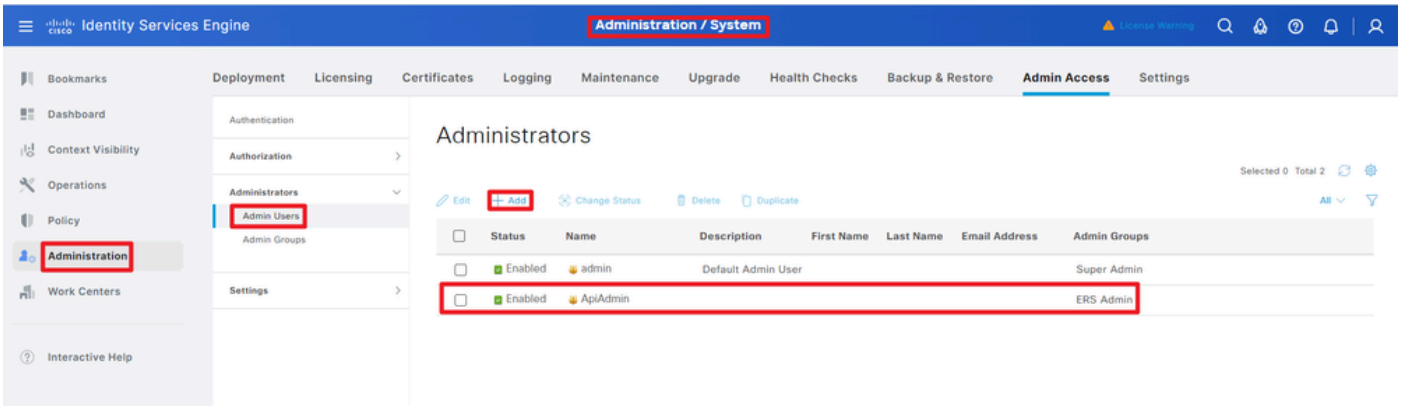


Topologia

Configurazione su ISE

Passaggio 1: Aggiungere un account amministratore Open API

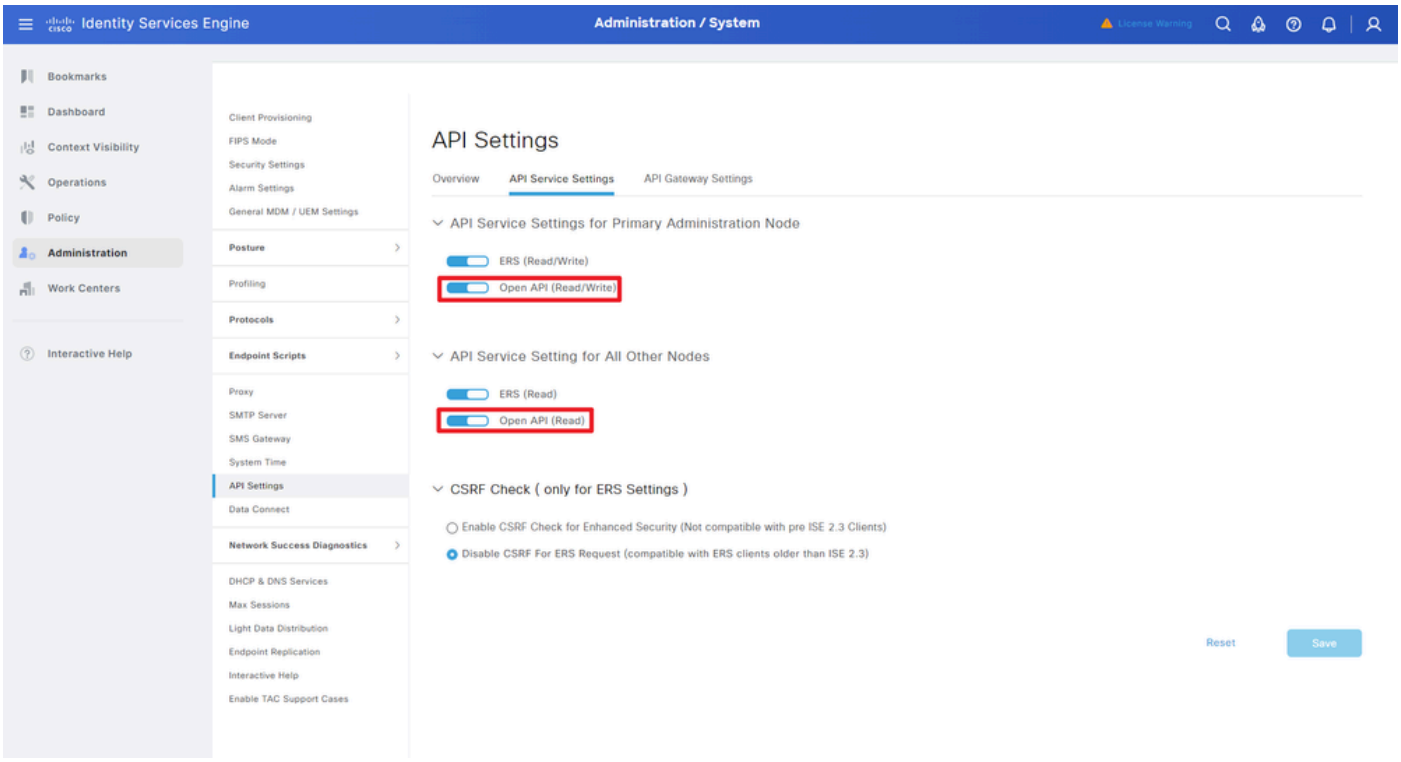
Per aggiungere un amministratore API, selezionare Amministrazione -> Sistema -> Amministrazione -> Amministratori -> Utenti amministratori -> Aggiungi.



Amministratore API

Fase 2: Abilitare Open API su ISE

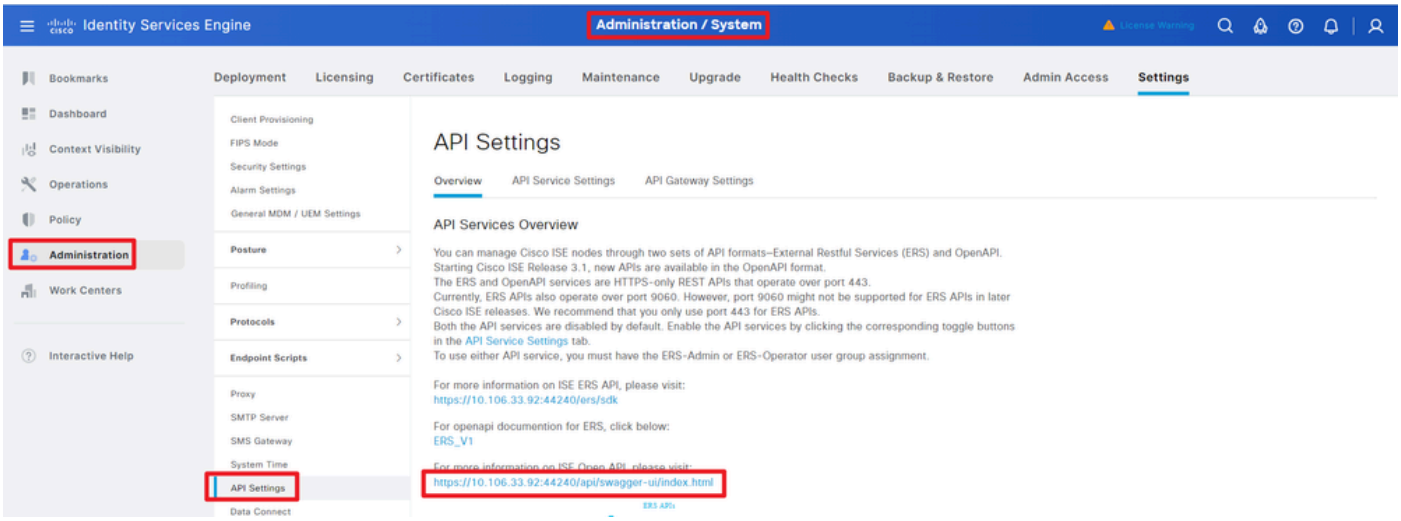
Open API è disabilitato per impostazione predefinita su ISE. Per abilitarlo, selezionare Amministrazione > Sistema > Impostazioni API > Impostazioni servizio API. Attivate o disattivate le opzioni di Open API. Fare clic su Save (Salva).



Abilita OpenAPI

Passaggio 3: Esplora ISE open API

passare ad Amministrazione > Sistema > Impostazioni API > Panoramica. Fare clic sul collegamento Apri API.



Visita OpenAPI

Esempi di Python

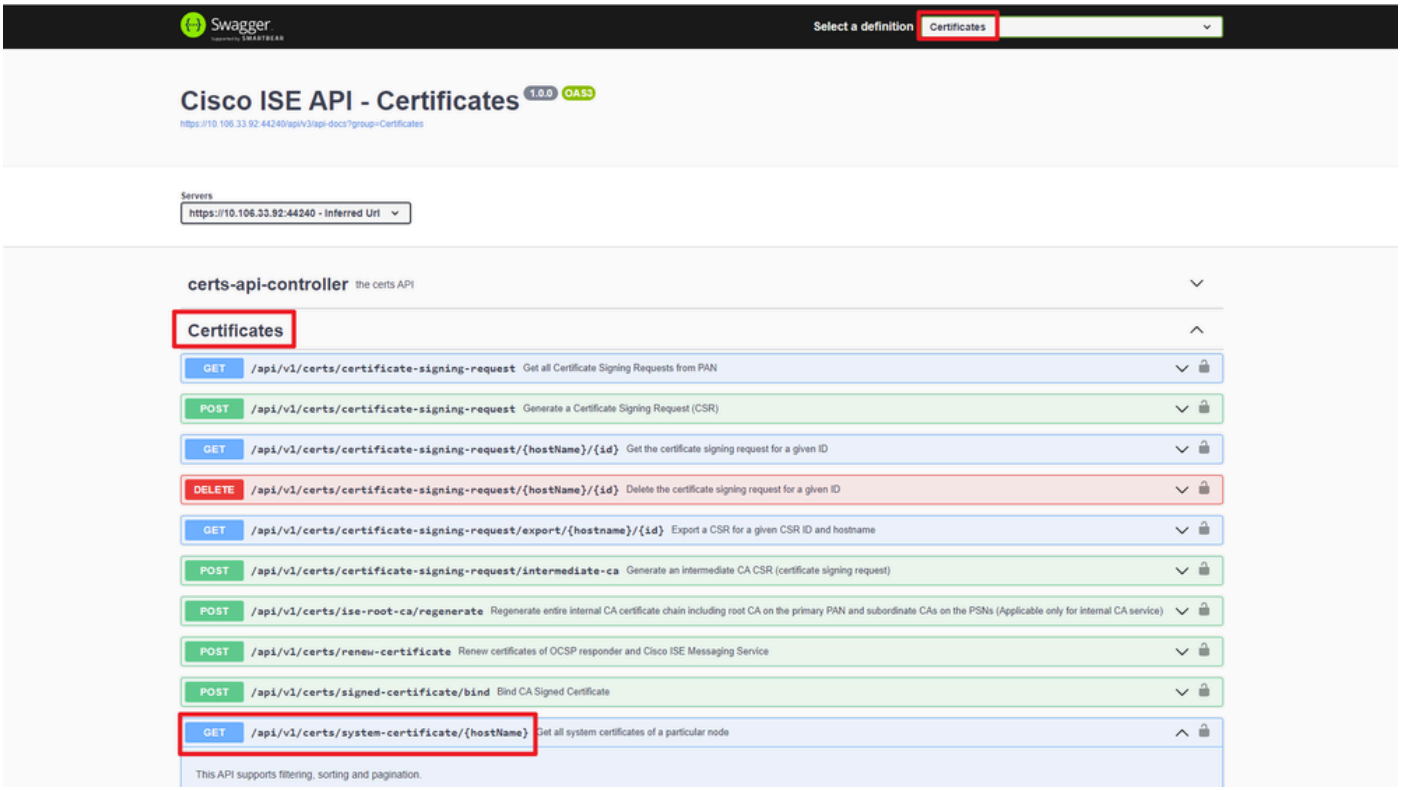
Ottieni Tutti I Certificati Di Sistema Di Un Nodo Specifico

L'API elenca tutti i certificati di un particolare nodo ISE.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare i certificati di un particolare nodo ISE.



URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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/certs/system-certificate/ISE-DLC-CFME02-PSN
"
```

```
    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())
```

Di seguito è riportato l'esempio degli output previsti.

Return Code:
200
Expected Outputs:
{'response': [{'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME0

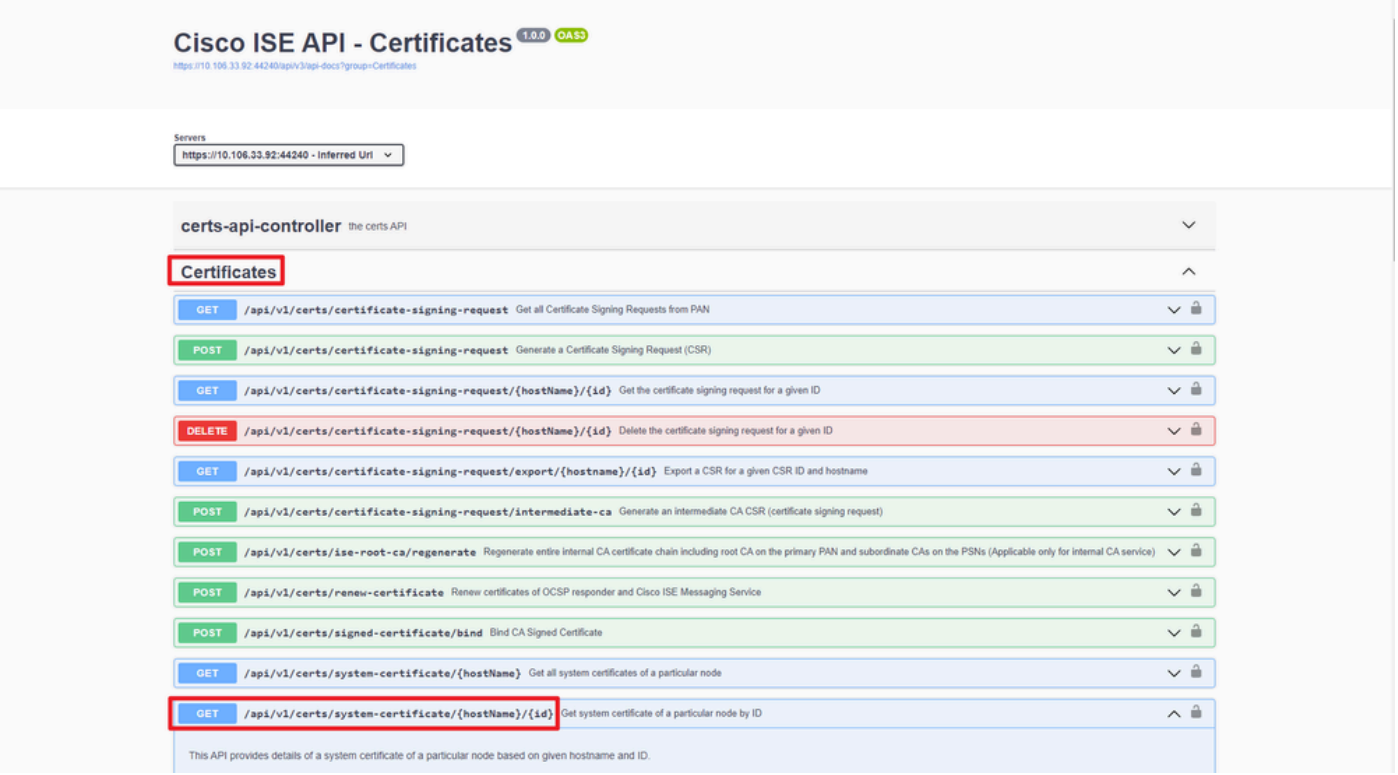
Ottieni Il Certificato Di Sistema Di Un Nodo Specifico In Base All'ID

Questa API fornisce i dettagli di un certificato di sistema di un particolare nodo in base al nome host e all'ID specificati.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-of-Certificate>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare il certificato di un particolare nodo in base al nome host e all'ID specificati.



URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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/certs/system-certificate/ISE-DLC-CFME02-PSN/5b5b28e4-2a51-495c-8413-610190e1

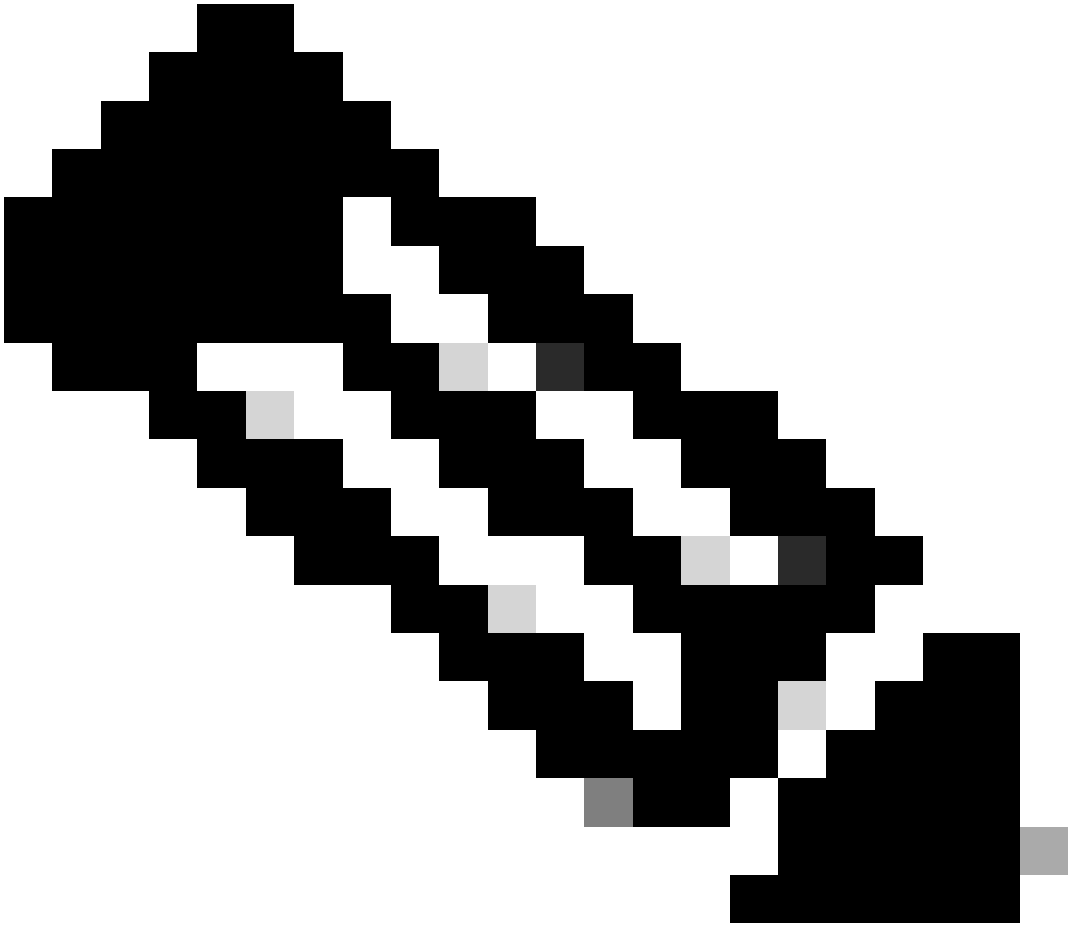
" headers = {

"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 "Get All System Certificates Of A Particular Node", ad esempio, 5b5b28e4-2a51-495c-8413-610190e1070b è "Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com".

Di seguito è riportato l'esempio degli output previsti.

Return Code:
200
Expected Outputs:
{'response': {'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02

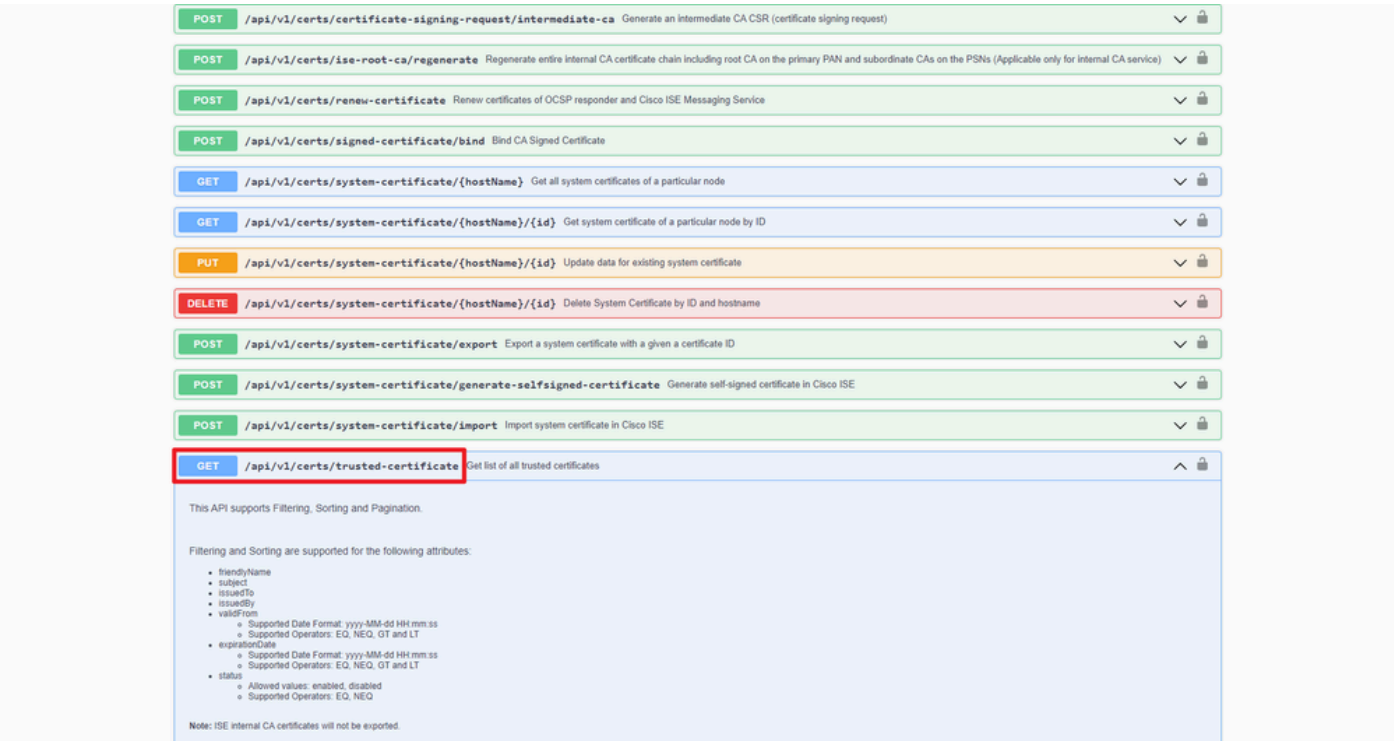
Ottieni Elenco Di Tutti I Certificati Attendibili

L'API elenca tutti i certificati attendibili del cluster ISE.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: individuare l'URL utilizzato per recuperare i certificati attendibili.



URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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/certs/trusted-certificate

" 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:")
```

Di seguito è riportato l'esempio degli output previsti.(Omesso)

```
Return Code:
200
Expected Outputs:
{'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=Ver
```

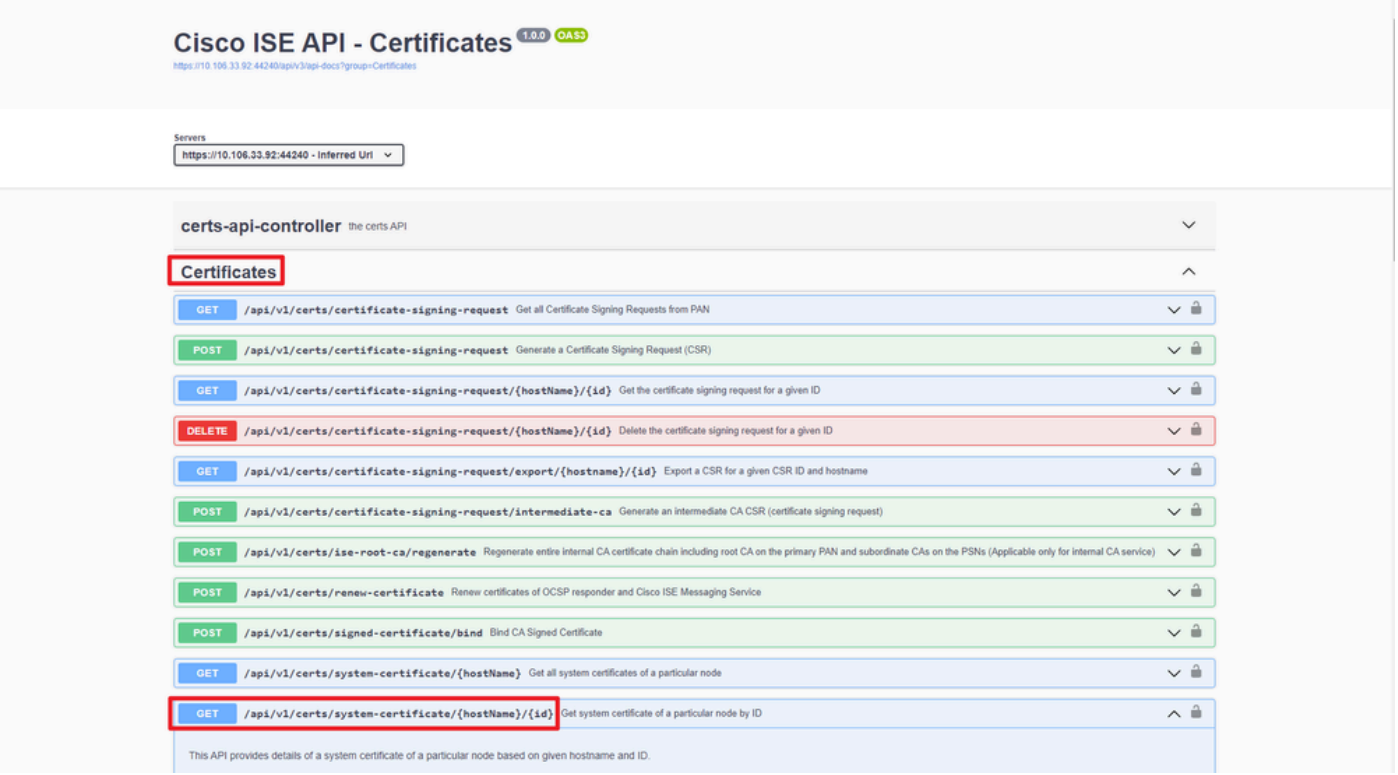
Ottieni certificato di attendibilità per ID

Questa API consente di visualizzare i dettagli di un certificato di attendibilità in base a un determinato ID.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-of-Certificate>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare le informazioni sulla distribuzione.



URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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/certs/trusted-certificate/147d97cc-6ce9-43d7-9928-8cd0fa83e140

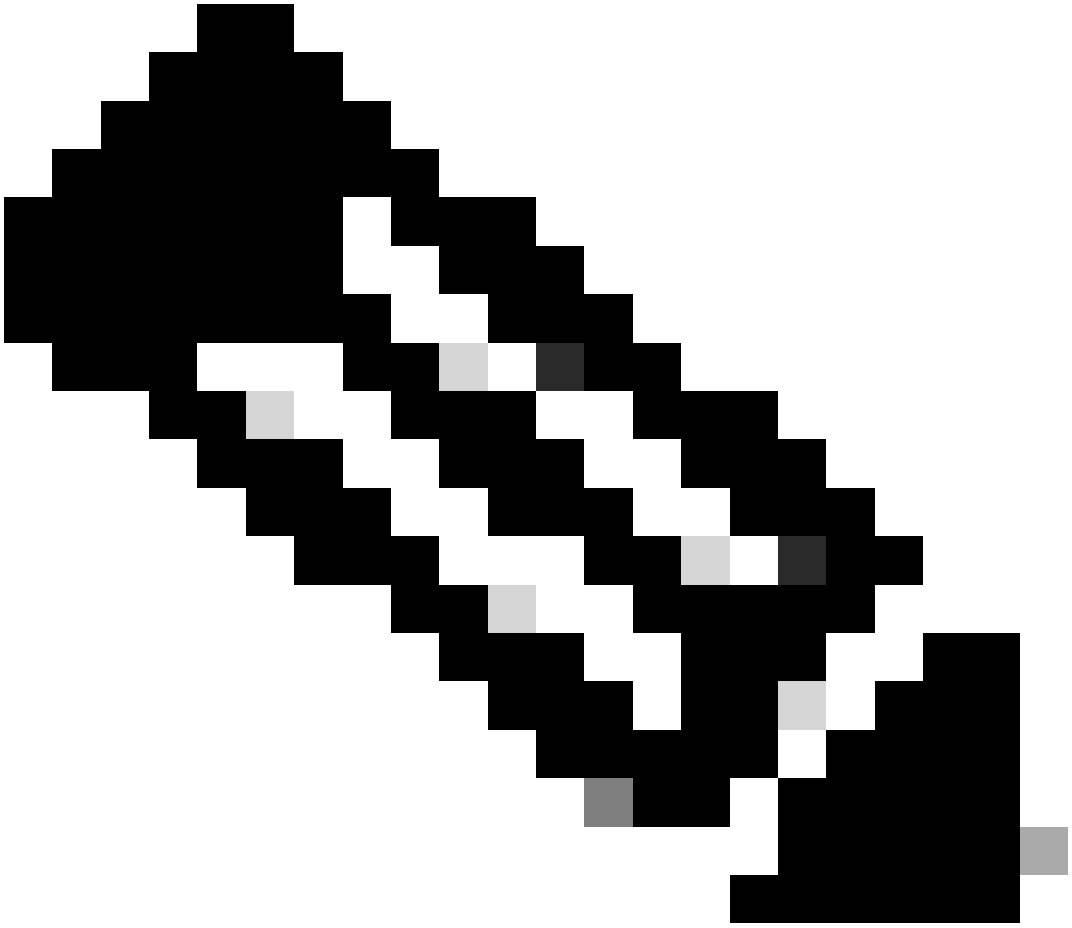
" headers = {

"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 "Get List Of All Trusted Certificates", ad esempio, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 è "VeriSign Class 3 Public Primary Certification Authority".

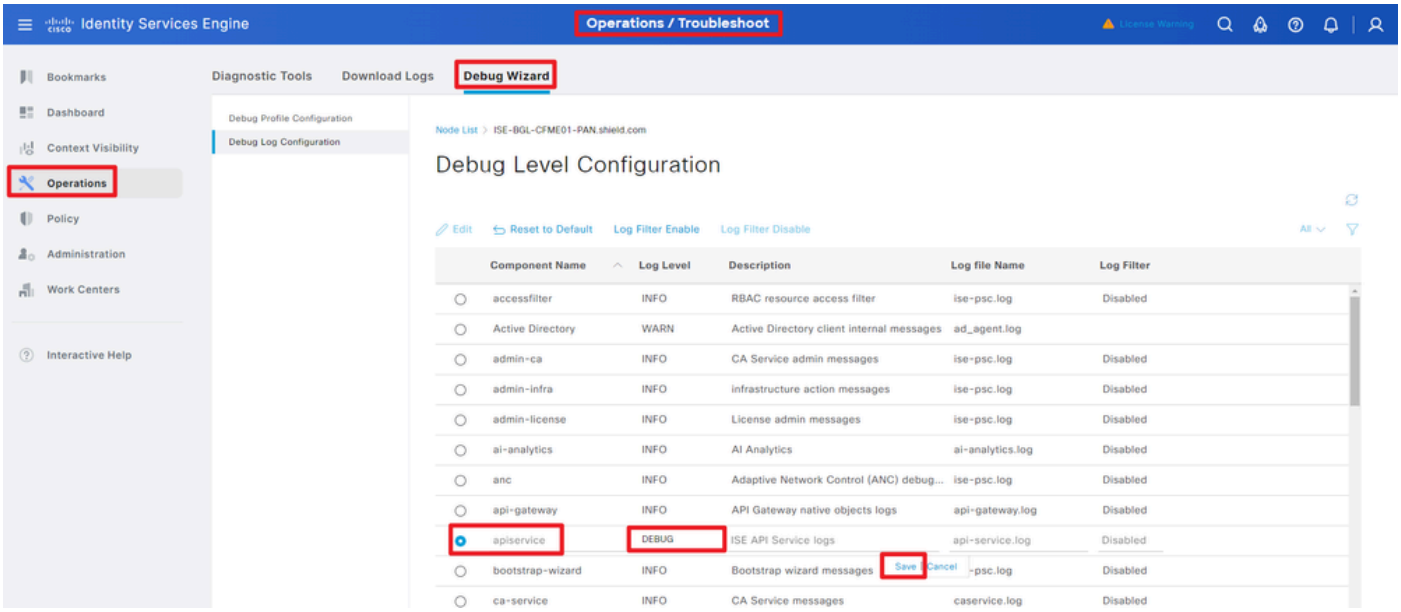
Di seguito è riportato l'esempio degli output previsti.

Return Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certifi

Risoluzione dei problemi

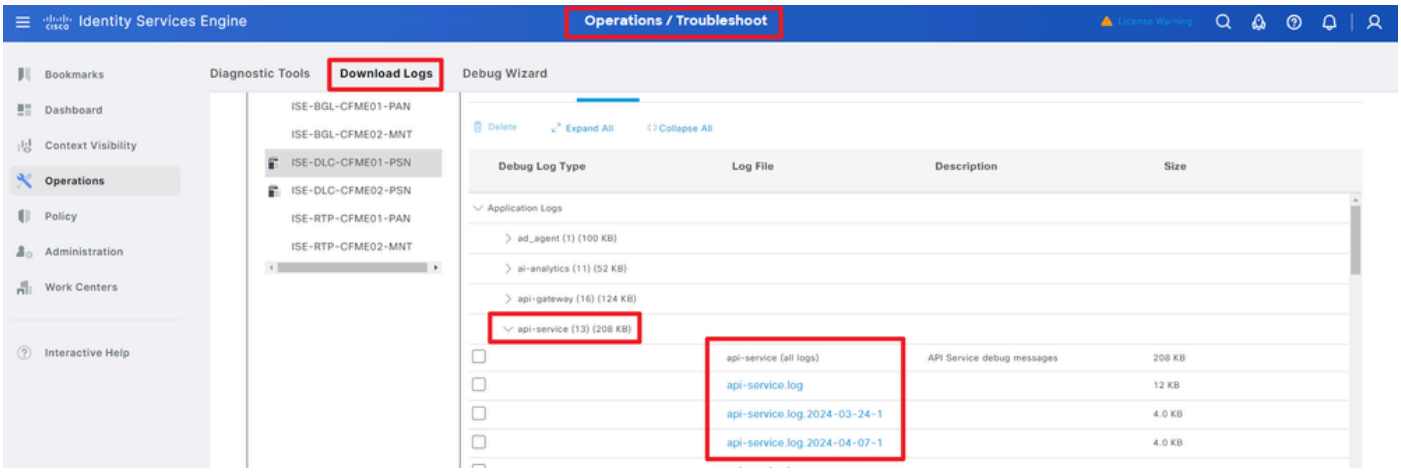
Per risolvere i problemi relativi alle API aperte, impostare **il** livello di **log** per apiservicecomponent su DEBUGnella finestra di configurazione **del log di debug**.

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



Debug del servizio API

Per scaricare i 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).**



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).