OpenAPI zum Abrufen von ISE-Zertifikatinformationen auf ISE 3.3 verwenden

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Verwendung von openAPI zur Verwaltung von Cisco Identity Services Engine (ISE)-Zertifikaten beschrieben.

Hintergrund

Angesichts der zunehmenden Komplexität der Sicherheit und Verwaltung von Unternehmensnetzwerken führt die Cisco ISE 3.1 APIs im OpenAPI-Format ein, die das Lebenszyklus-Management von Zertifikaten optimieren. Sie bieten eine standardisierte und automatisierte Schnittstelle für effiziente und sichere Zertifikatabläufe, die Administratoren dabei unterstützt, strenge Sicherheitsvorkehrungen durchzusetzen und die Netzwerk-Compliance aufrechtzuerhalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

- Python

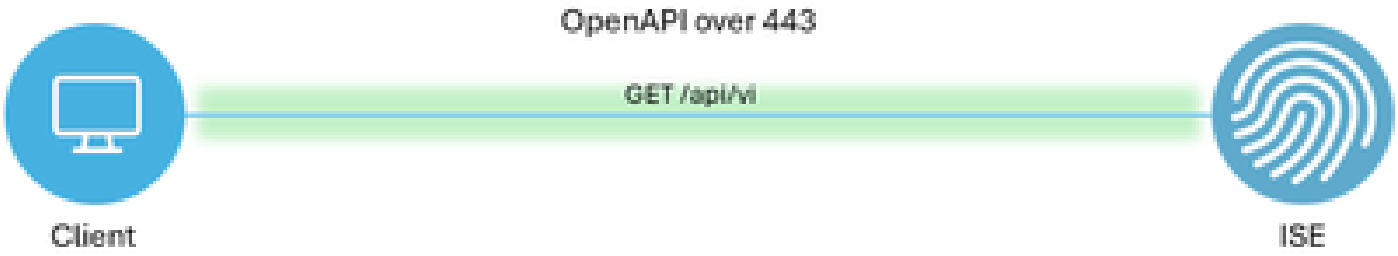
Verwendete Komponenten

- ISE 3.3
- Python 3.10.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm

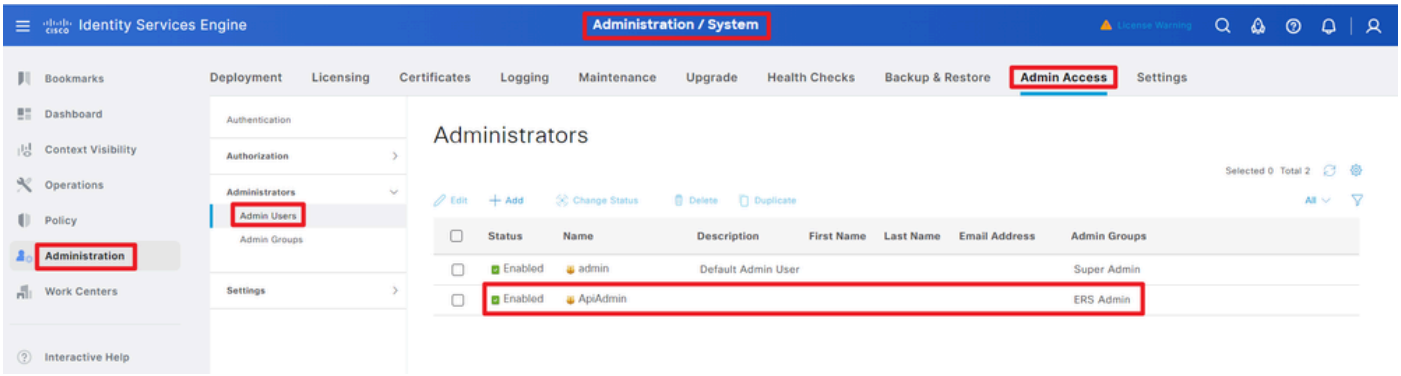


Topologie

Konfiguration auf der ISE

Schritt 1: Hinzufügen eines offenen API-Administrationskontos

Um einen API-Administrator hinzuzufügen, navigieren Sie zu Administration > System > Admin Access > Administrators > Admin Users > Add.

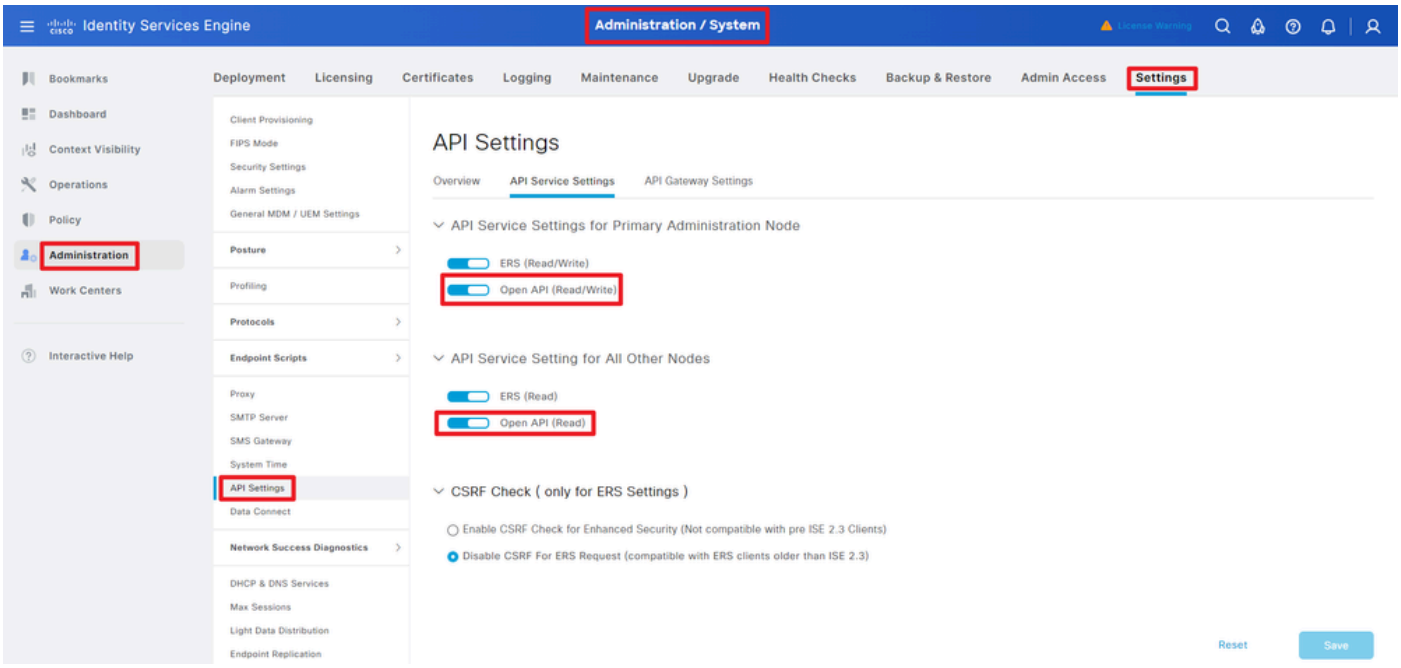


API-Administrator

Schritt 2: Aktivieren der offenen API auf der ISE

Die offene API ist auf der ISE standardmäßig deaktiviert. Um sie zu aktivieren, navigieren Sie zu Administration > System > Settings > API Settings > API Service Settings. Schalten Sie die Open

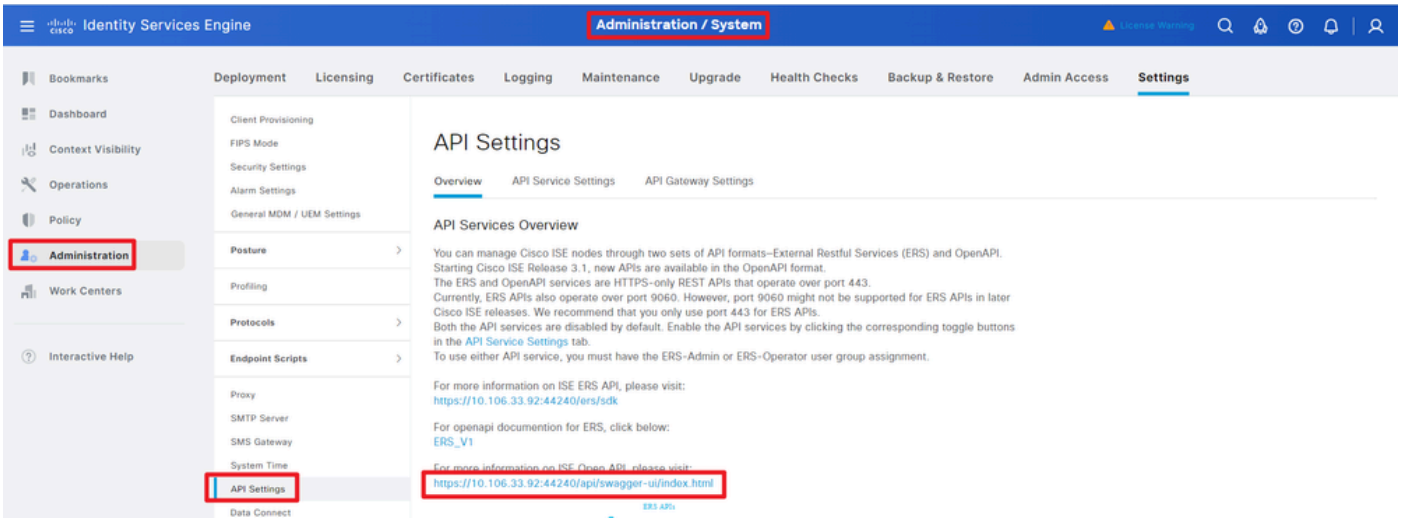
API-Optionen um. Klicken Sie auf Speichern.



OpenAPI aktivieren

Schritt 3: Erkunden der offenen ISE-API

Navigieren Sie zu Administration > System > Settings > API Settings > Overview. Klicken Sie auf API-Besuchslink öffnen.



OpenAPI aufrufen

Python-Beispiele

Abrufen aller Systemzertifikate eines bestimmten Knotens

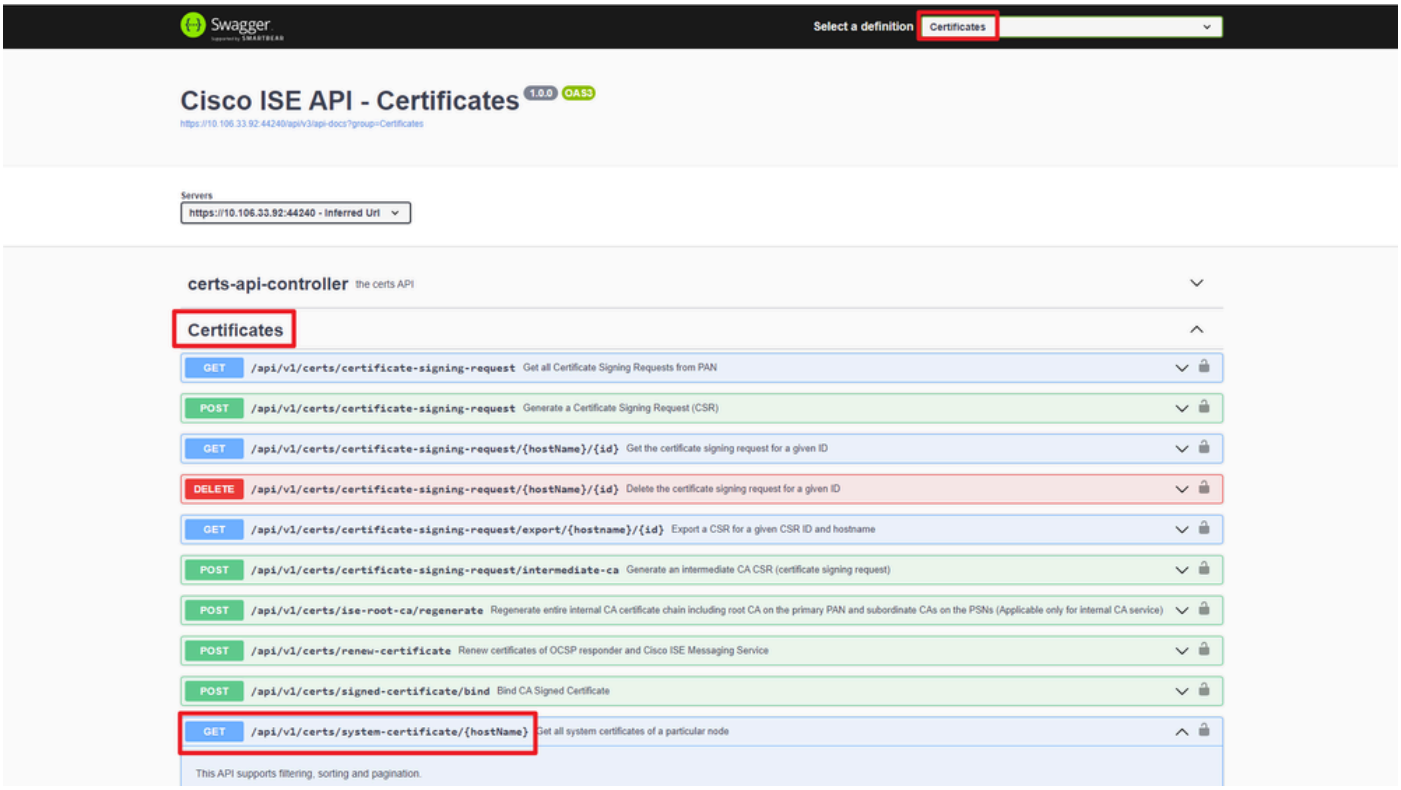
Die API listet alle Zertifikate eines bestimmten ISE-Knotens auf.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN

URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von Zertifikaten eines bestimmten ISE-Knotens verwendet wird.



API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, auf dem das Python-Codebeispiel ausgeführt wird.

<#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())
```

Hier sehen Sie das Beispiel der erwarteten Ergebnisse.

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

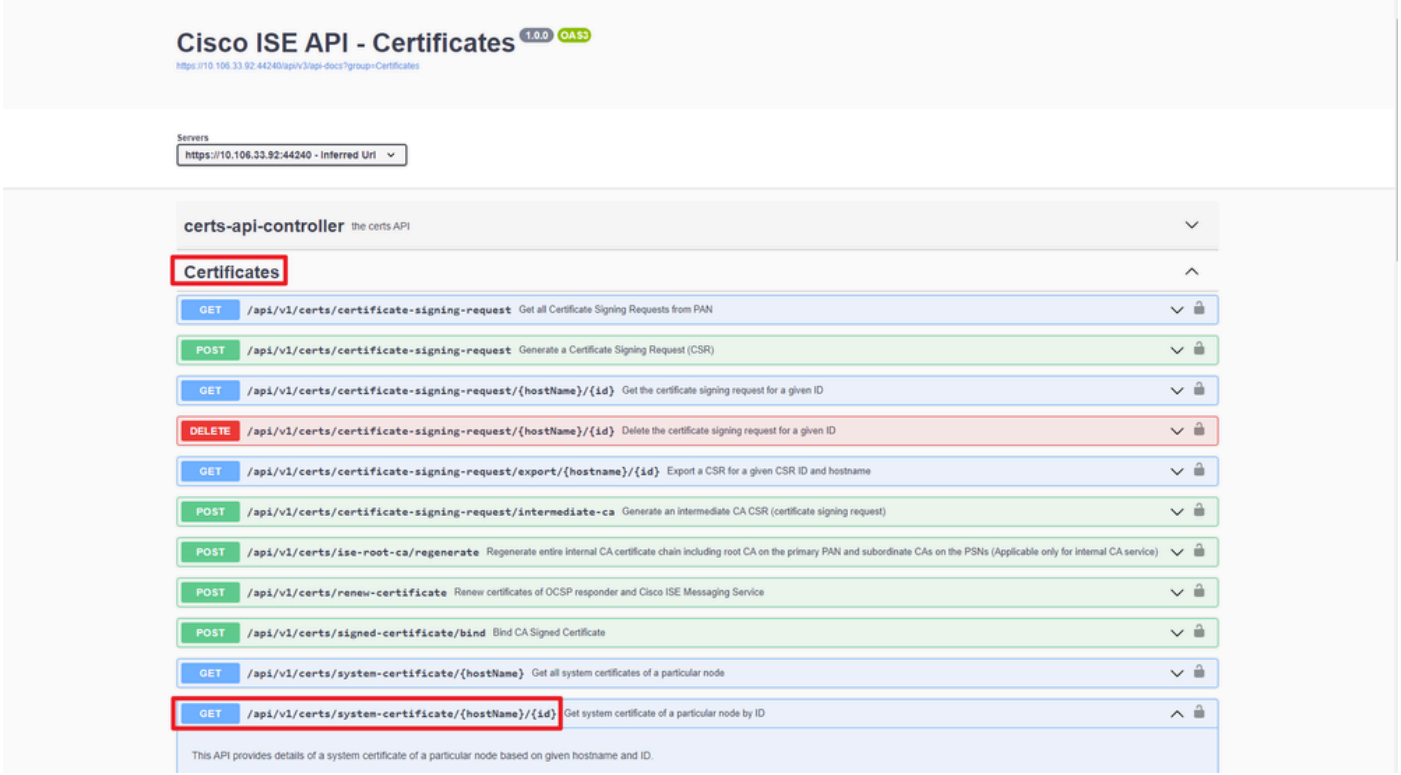
Systemzertifikat eines bestimmten Knotens nach ID abrufen

Diese API stellt Details eines Systemzertifikats eines bestimmten Knotens basierend auf dem angegebenen Hostnamen und der angegebenen ID bereit.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-Of-Certificate>
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen des Zertifikats eines bestimmten Knotens basierend auf dem angegebenen Hostnamen und der angegebenen ID verwendet wird.



API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, auf dem das Python-Codebeispiel ausgeführt wird.

<#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

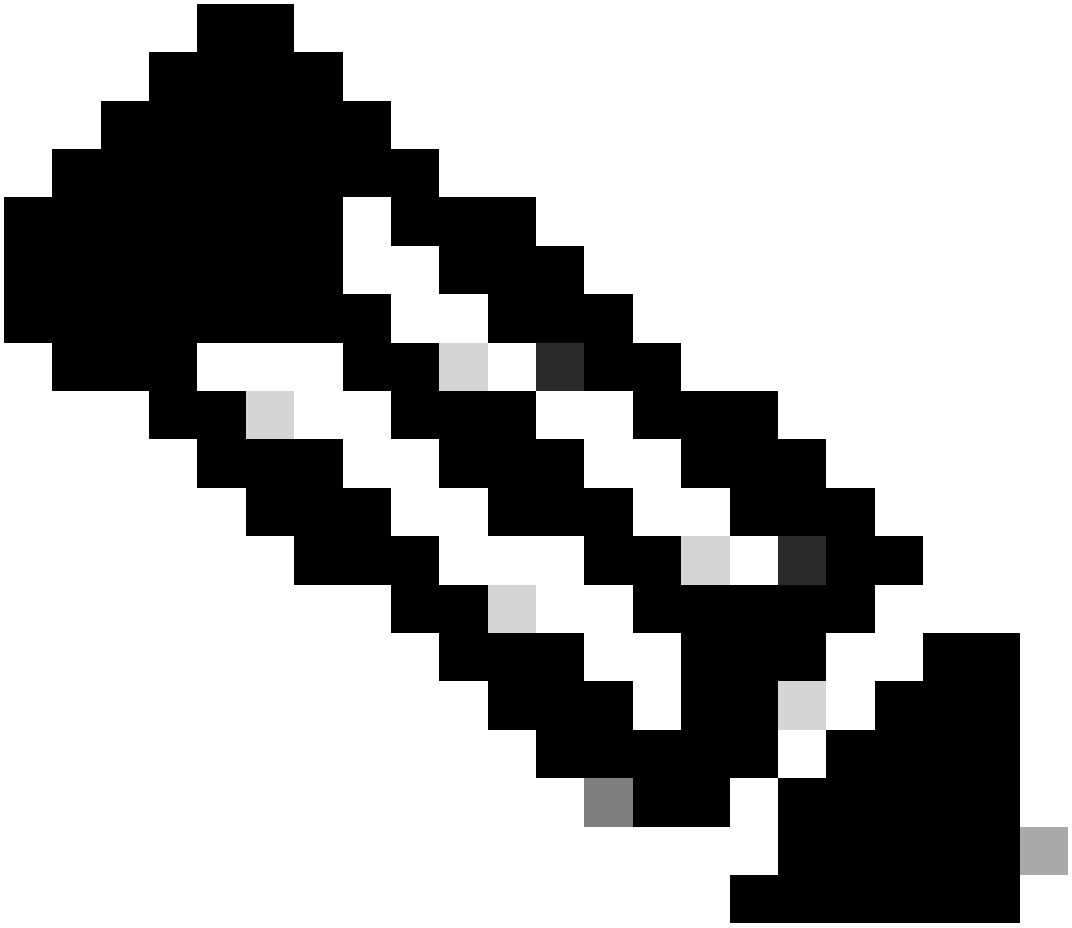
" headers = {

"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:")



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von "Get All System Certificates Of A Particular Node", z. B. 5b5b28e4-2a51-495c-8413-610190e1070b ist "Default self-signed saml server certificate - CN=SAML_ISE -DLC-CFME02-PSN.cisco.com".

Hier sehen Sie das Beispiel der erwarteten Ergebnisse.

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

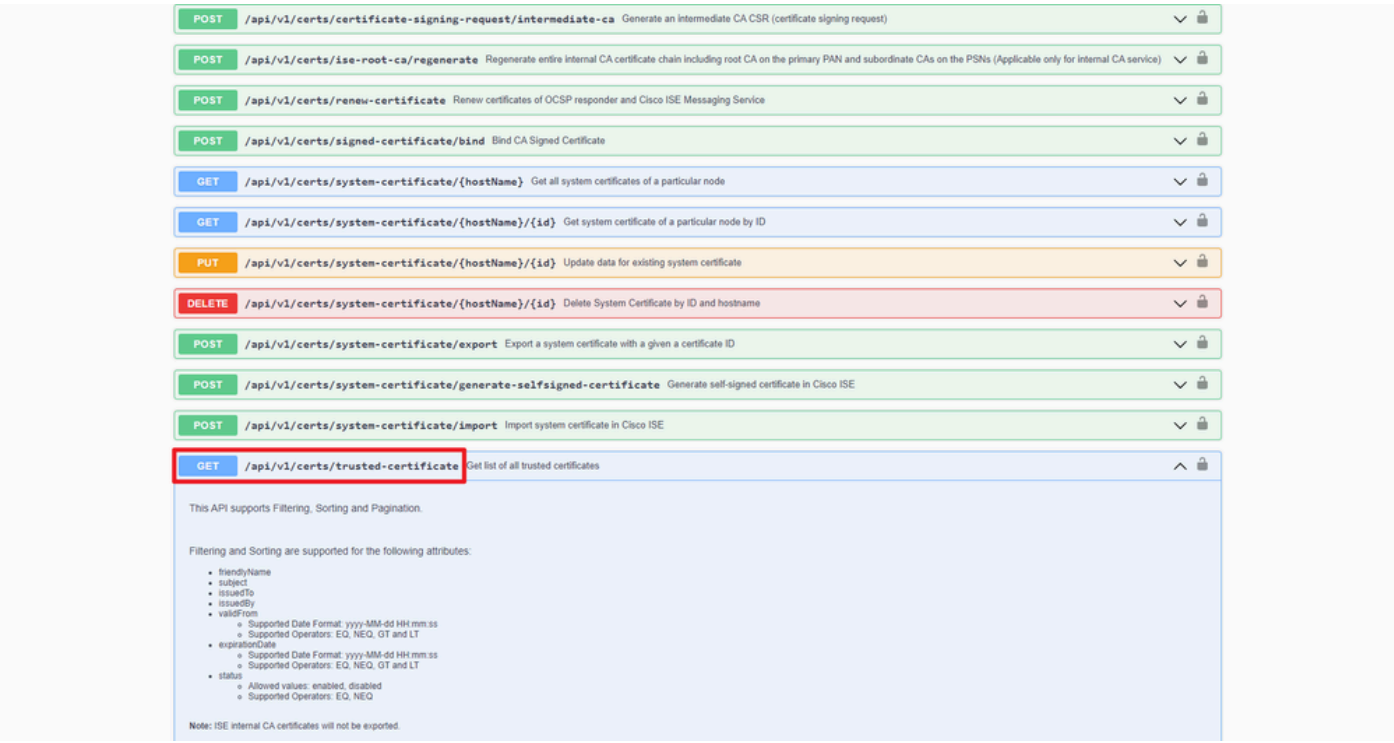
Liste aller vertrauenswürdigen Zertifikate abrufen

Die API listet alle vertrauenswürdigen Zertifikate des ISE-Clusters auf.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von vertrauenswürdigen Zertifikaten verwendet wird.



API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, auf dem das Python-Codebeispiel ausgeführt wird.

<#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:")
```

Hier ist das Beispiel der erwarteten Ausgaben. (weggelassen)

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

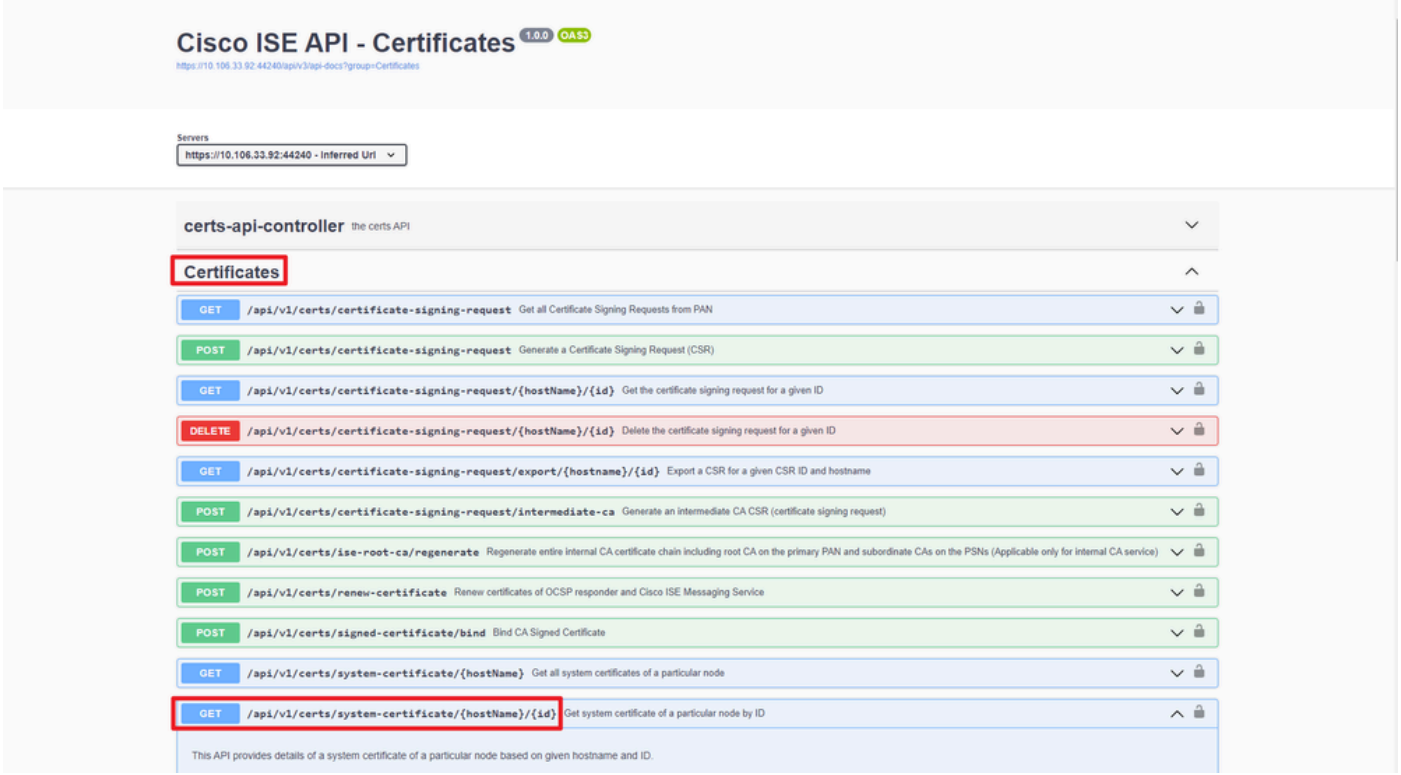
Vertrauenswürdiges Zertifikat nach ID abrufen

Diese API kann Details eines Vertrauensstellungszertifikats basierend auf einer angegebenen ID anzeigen.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-Of-Certificate>
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von Bereitstellungsinformationen verwendet wird.



API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, auf dem das Python-Codebeispiel ausgeführt wird.

<#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

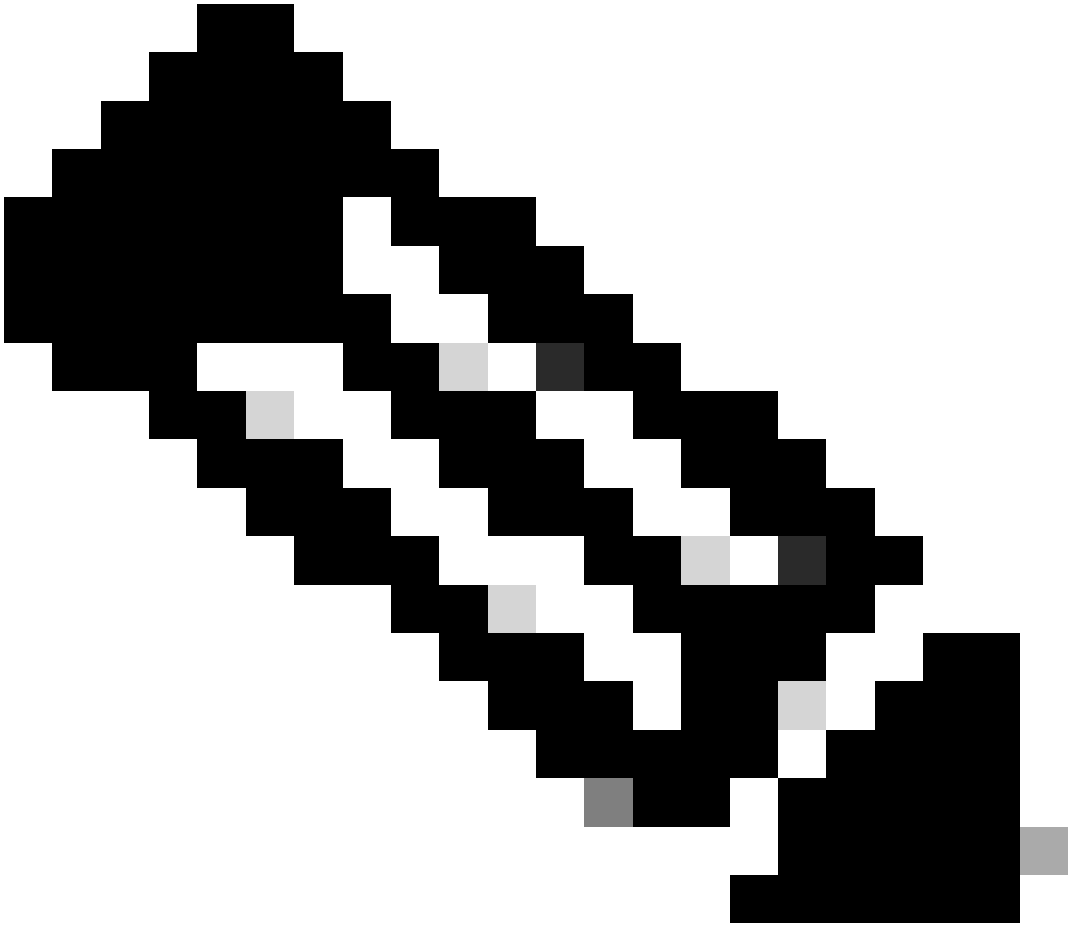
" headers = {

"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:")



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von "Get List Of All Trusted Certificates" (Liste aller vertrauenswürdigen Zertifikate abrufen), z. B. 147d97cc-6ce9-43d7-9928-8cd0fa83e140 ist "VeriSign Class 3 Public Primary Certification Authority".

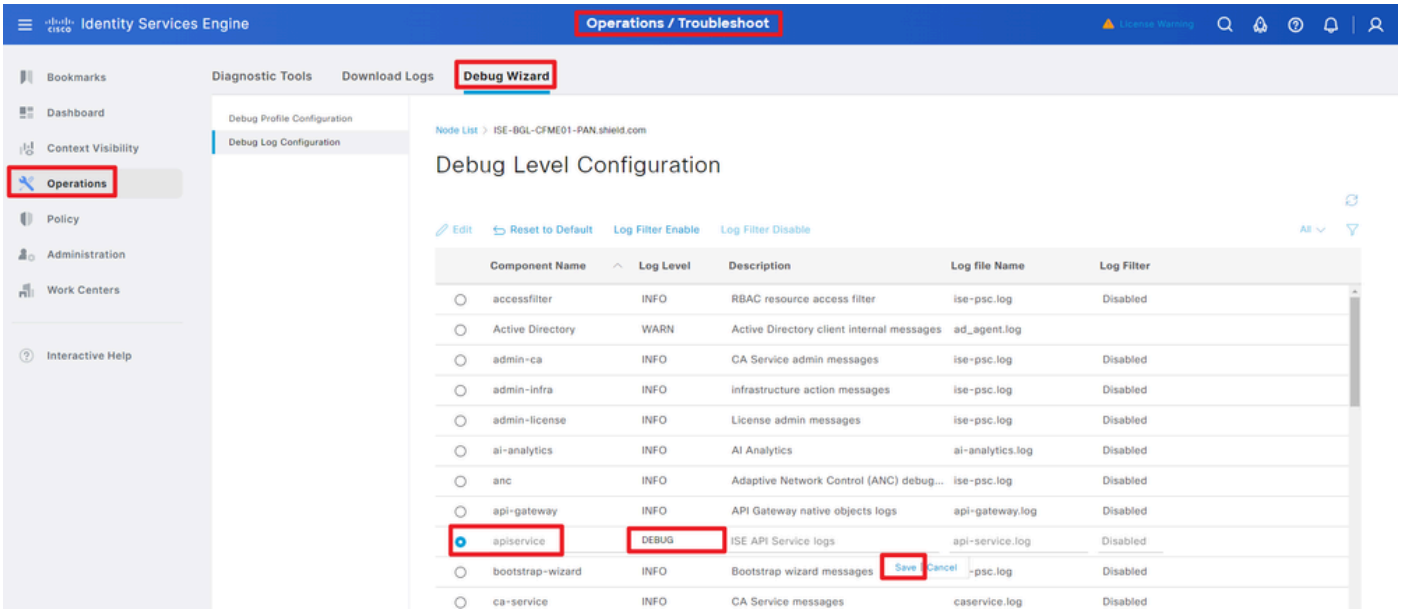
Hier sehen Sie das Beispiel der erwarteten Ergebnisse.

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

Fehlerbehebung

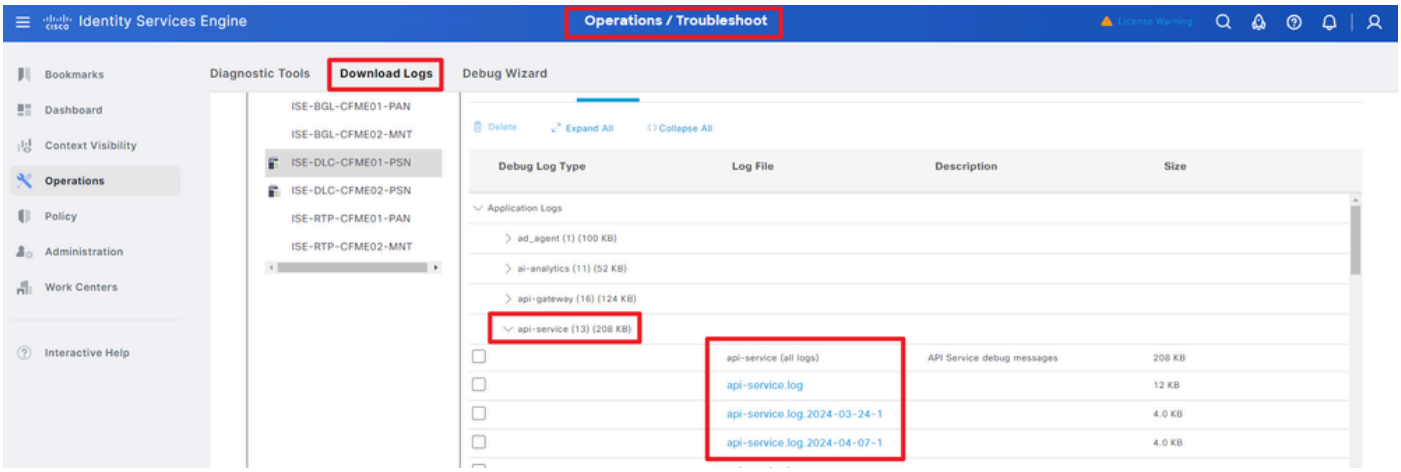
Um Probleme im Zusammenhang mit den Open APIs zu beheben, legen Sie **dieLog**-Ebene für die apiservicecomponent im Konfigurationsfenster**Debug Log** auf DEBUG fest.

Um das Debugging zu aktivieren, navigieren Sie zu **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > apiservice.**



Debuggen von API-Diensten

Um Debug-Protokolle herunterzuladen, navigieren Sie zu **Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs.**



Debug-Protokolle herunterladen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.