Uso de OpenAPI para recuperar información de certificados de ISE en ISE 3.3

Contenido

Introducción

Este documento describe el procedimiento para utilizar openAPI para administrar el certificado de Cisco Identity Services Engine (ISE).

Background

Frente a la creciente complejidad en la seguridad y la gestión de redes empresariales, Cisco ISE 3.1 presenta API con formato OpenAPI que agilizan la gestión del ciclo de vida de los certificados, ofreciendo una interfaz estandarizada y automatizada para operaciones de certificados eficientes y seguras, lo que ayuda a los administradores a aplicar prácticas de seguridad sólidas y a mantener el cumplimiento de la red.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

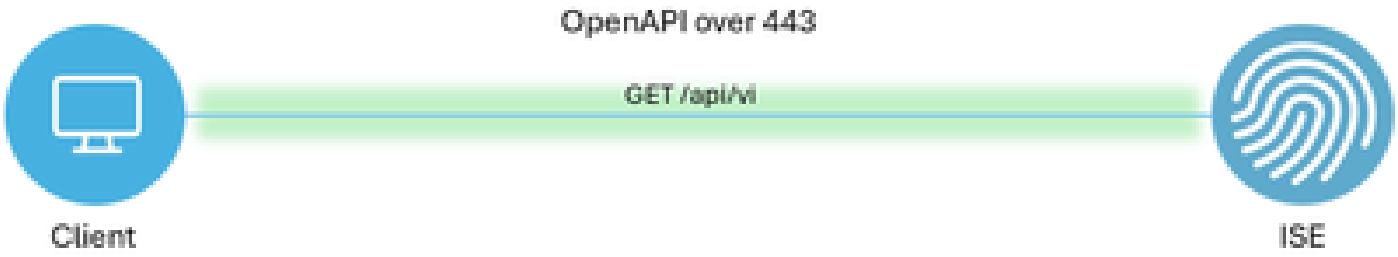
Componentes Utilizados

- ISE 3.3
- Python 3.10.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

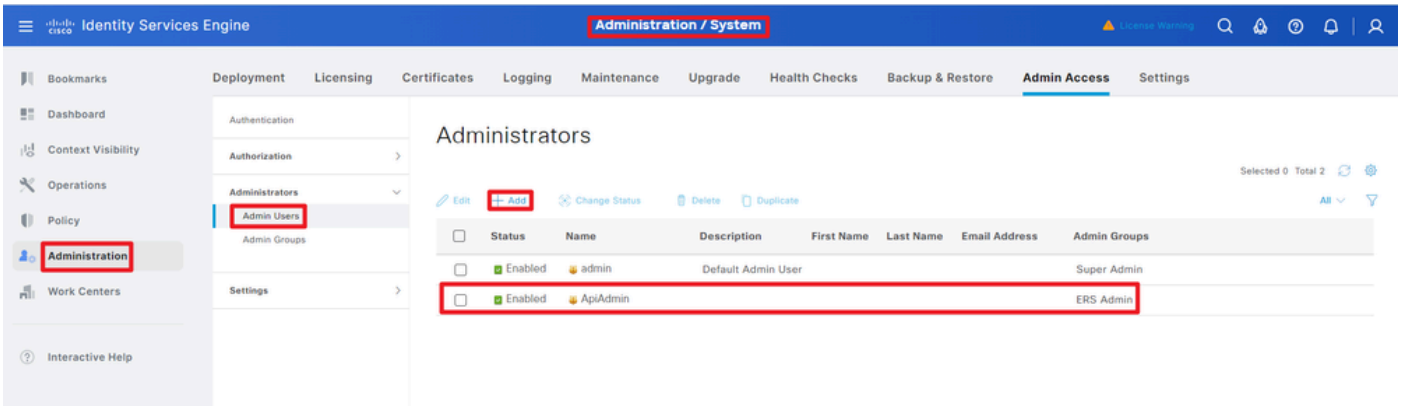


Topología

Configuración en ISE

Paso 1: Agregar una cuenta de administrador de API abierta

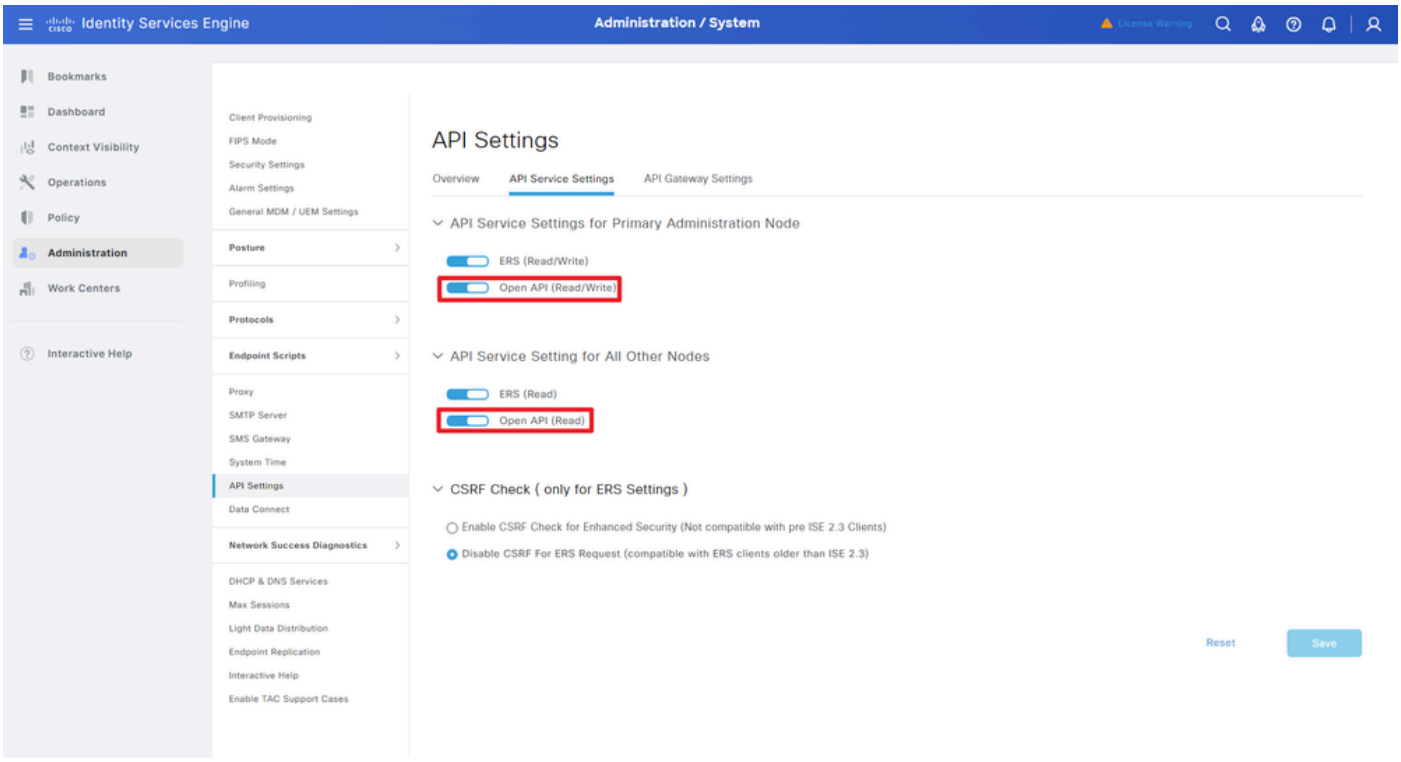
Para agregar un administrador de API, vaya aAdministración -> Sistema -> Administración -> Administradores -> Usuarios administrativos -> Agregar.



Administrador de API

Paso 2: Habilitar API abierta en ISE

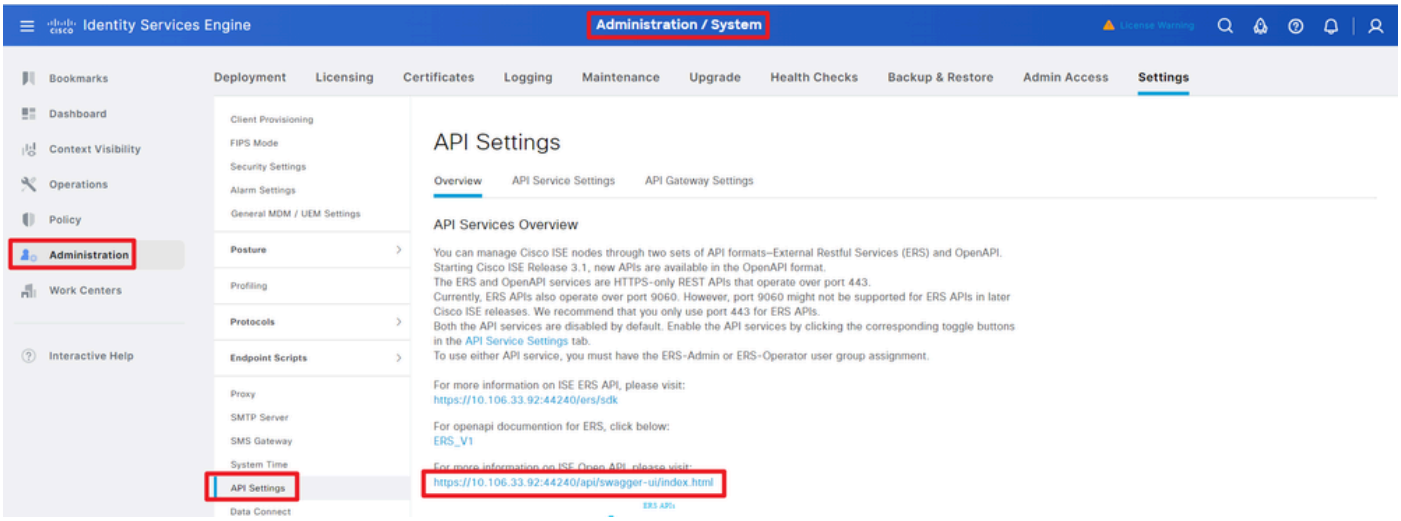
API abierta está desactivada de forma predeterminada en ISE. Para habilitarlo, navegue hasta Administration > System > API Settings > API Service Settings. Active o desactive las opciones de API abierta. Click Save.



Habilitar OpenAPI

Paso 3: Explore la API abierta de ISE

Vaya a Administration > System > API Settings > Overview. Haga clic en el enlace de visita API abierta.



Visite OpenAPI

Ejemplos de Python

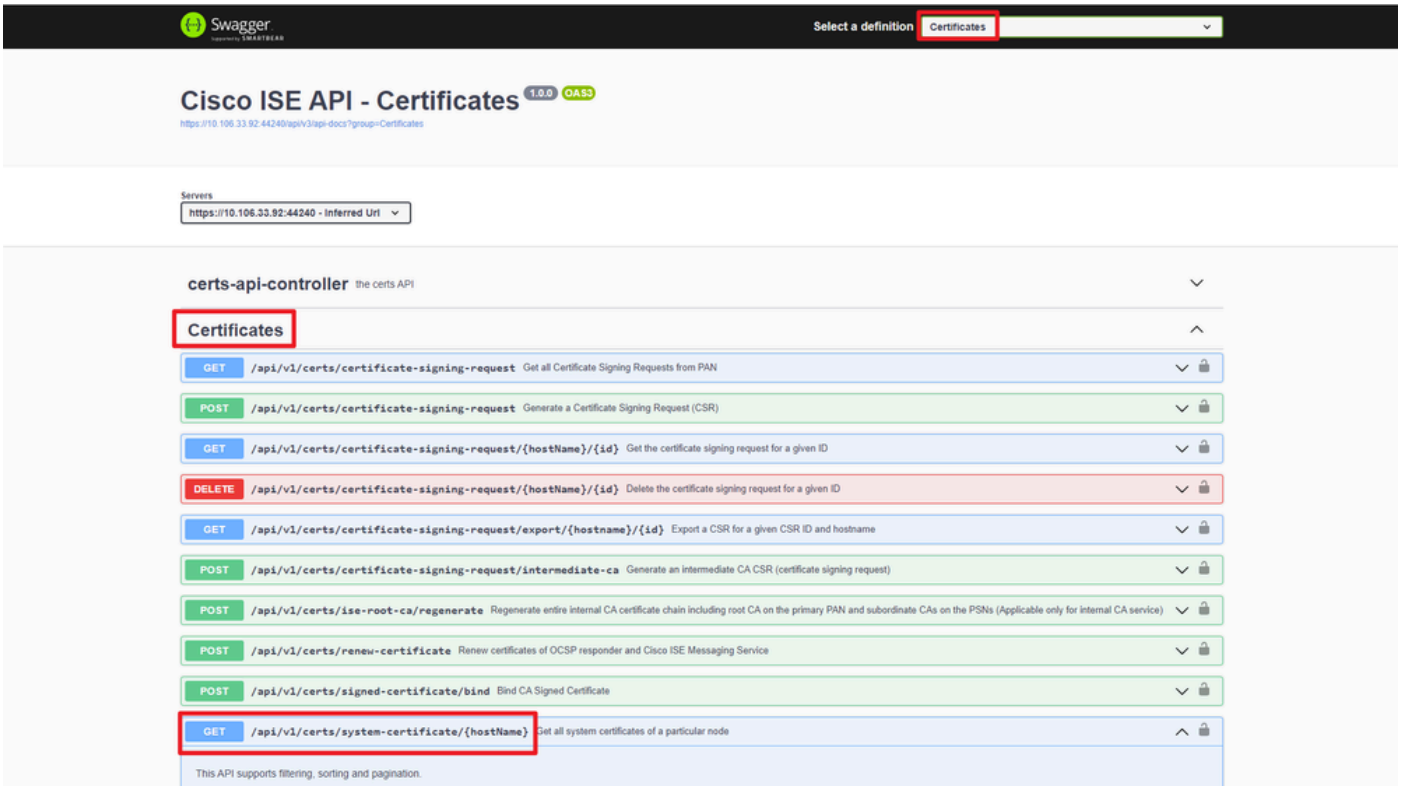
Obtener Todos Los Certificados Del Sistema De Un Nodo Determinado

La API enumera todos los certificados de un nodo de ISE determinado.

Paso 1: Información necesaria para una llamada de API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>
Credenciales	Usar credenciales de cuenta de API abierta
Encabezados	Aceptar: application/json Tipo de contenido: application/json

Paso 2: busque la URL que se utiliza para recuperar los certificados de un nodo de ISE determinado.



URI DE API

Paso 3: Este es el ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP, el nombre de usuario y la contraseña de ISE. Guardar como un archivo python para ejecutar.

Asegúrese de que haya una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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())
```

Este es el ejemplo de resultados esperados.

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

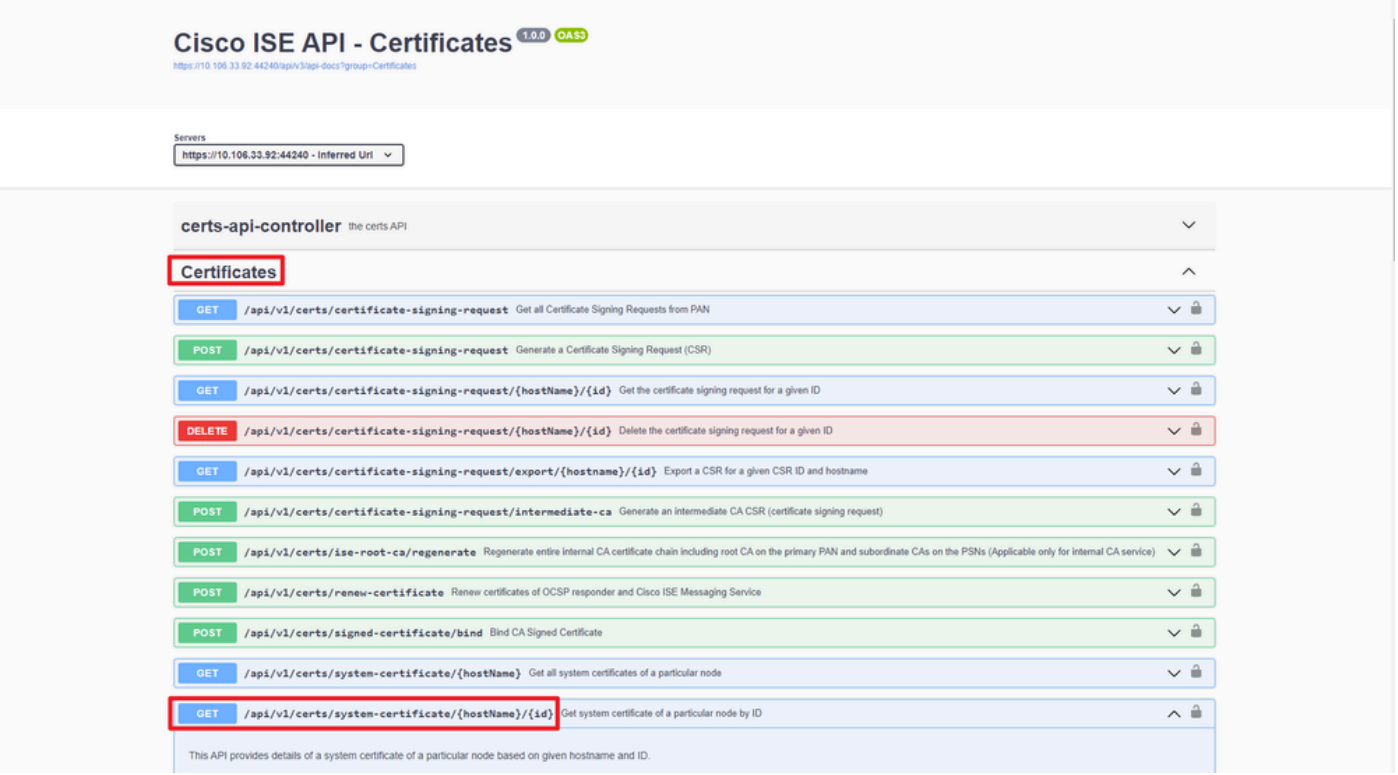
Obtener Certificado Del Sistema De Un Nodo Determinado Por ID

Esta API proporciona detalles de un certificado del sistema de un nodo determinado basado en el nombre de host y la ID dados.

Paso 1: Información necesaria para una llamada de API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-Of-Certificate>
Credenciales	Usar credenciales de cuenta de API abierta
Encabezados	Aceptar: application/json Tipo de contenido: application/json

Paso 2: Localice la URL que se utiliza para recuperar el certificado de un nodo determinado basado en el nombre de host y la ID dados.



URI DE API

Paso 3: Este es el ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP, el nombre de usuario y la contraseña de ISE. Guardar como un archivo python para ejecutar.

Asegúrese de que haya una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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

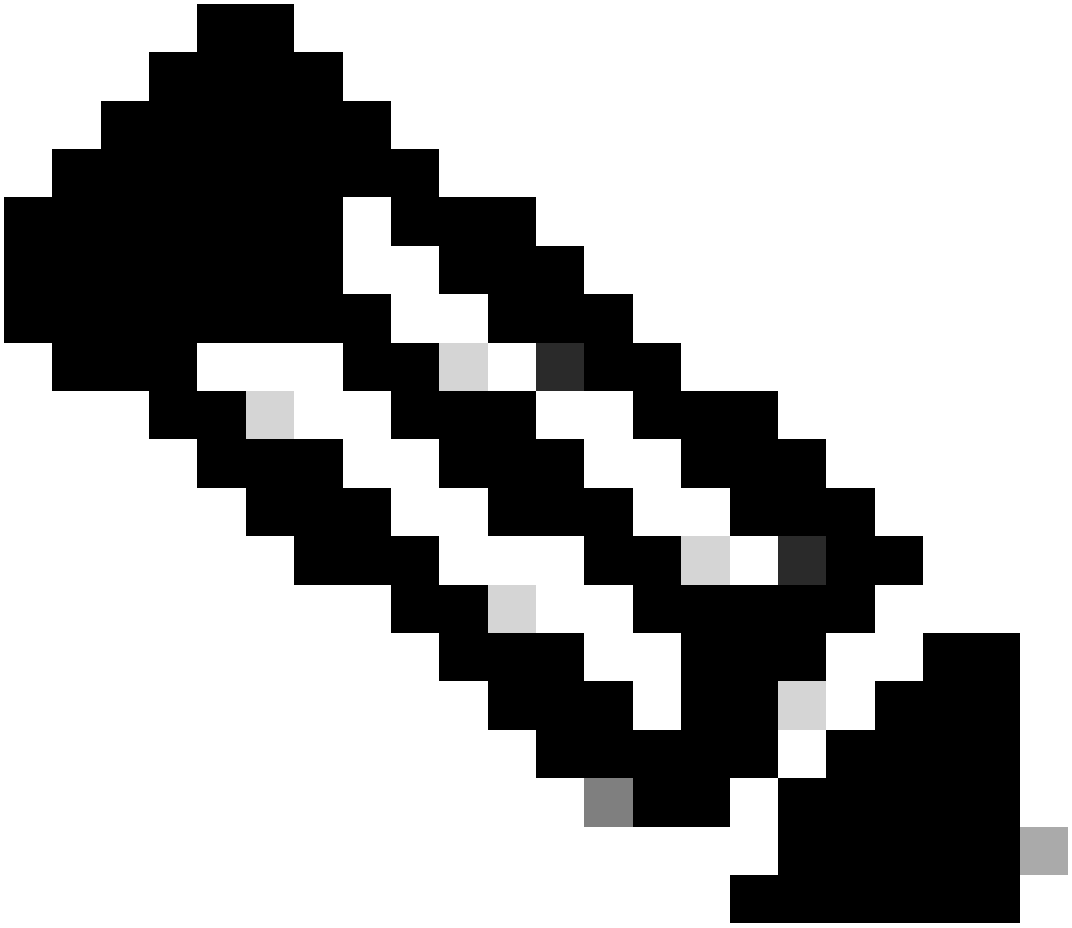
" headers = {

"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: El ID proviene de las salidas de API del paso 3 de "Obtener todos los certificados del sistema de un nodo determinado", por ejemplo, 5b5b28e4-2a51-495c-8413-610190e1070b es "Certificado de servidor saml autofirmado predeterminado - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com".

Este es el ejemplo de resultados esperados.

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

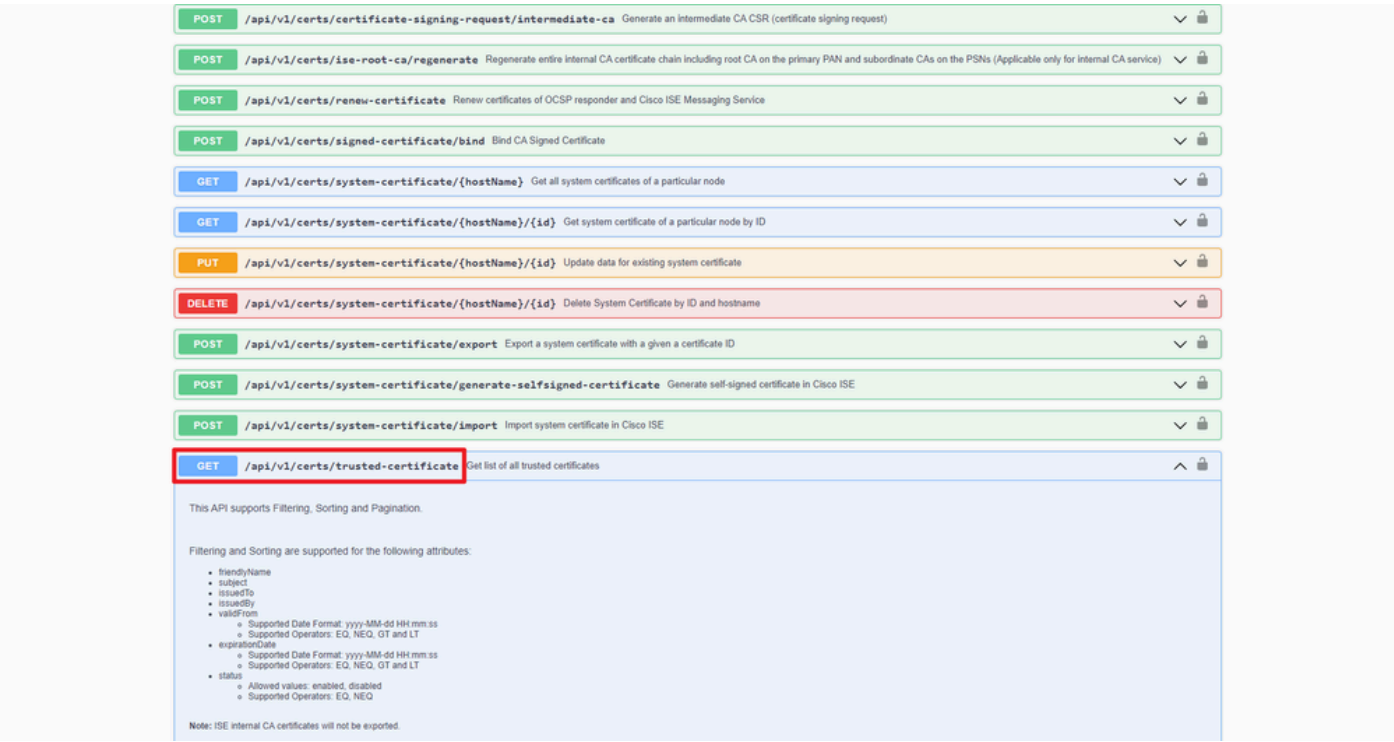
Obtener Lista De Todos Los Certificados Protegidos

La API enumera todos los certificados de confianza del clúster de ISE.

Paso 1: Información necesaria para una llamada de API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate
Credenciales	Usar credenciales de cuenta de API abierta
Encabezados	Aceptar: application/json Tipo de contenido: application/json

Paso 2: busque la dirección URL que se utiliza para recuperar certificados de confianza.



URI DE API

Paso 3: Este es el ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP, el nombre de usuario y la contraseña de ISE. Guardar como un archivo python para ejecutar.

Asegúrese de que haya una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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:")
```

Este es el ejemplo de resultados esperados.(Omitido)

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

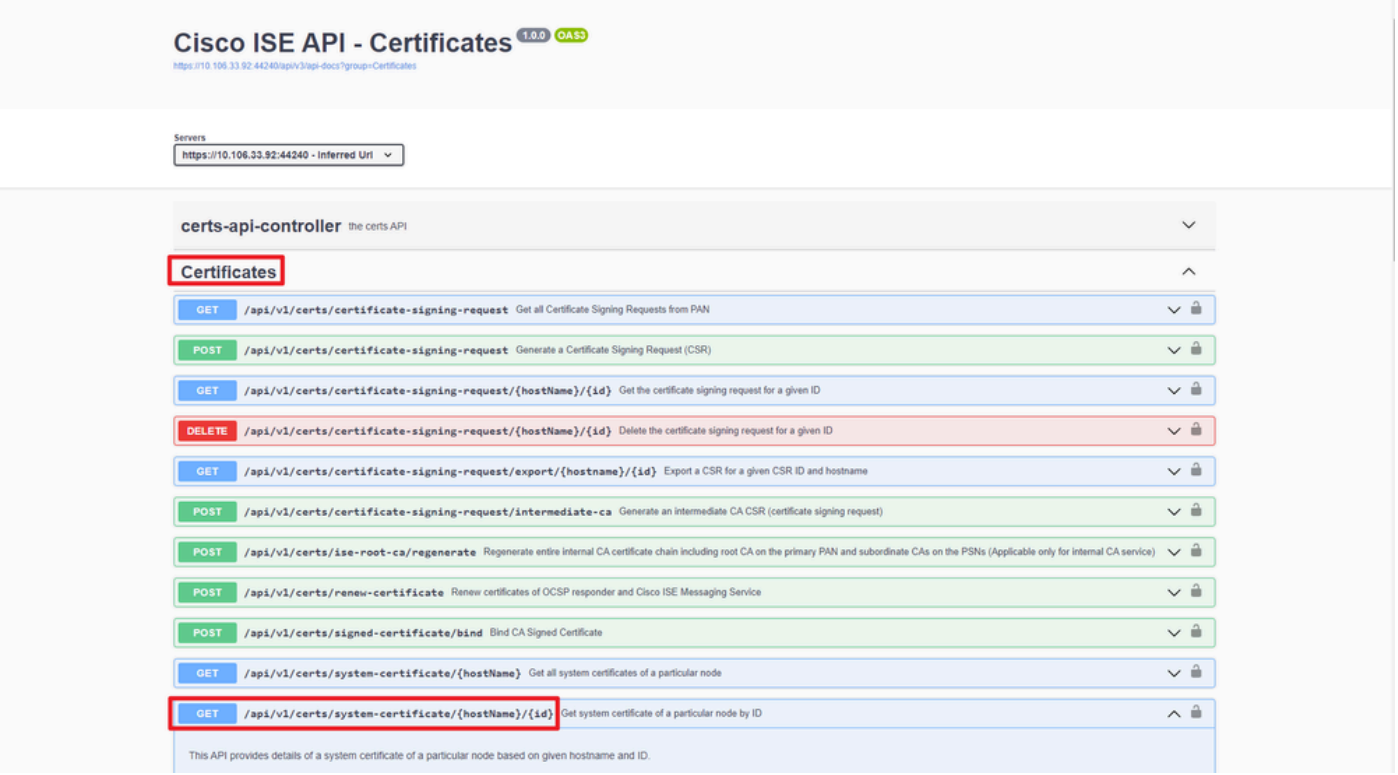
Obtener certificado de confianza por ID

Esta API puede mostrar detalles de un certificado de confianza basados en una ID determinada.

Paso 1: Información necesaria para una llamada de API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-Of-Certificate>
Credenciales	Usar credenciales de cuenta de API abierta
Encabezados	Aceptar: application/json Tipo de contenido: application/json

Paso 2: Localice la URL que se utiliza para recuperar la información de implementación.



URI DE API

Paso 3: Este es el ejemplo de código Python. Copiar y pegar el contenido. Reemplace la IP, el nombre de usuario y la contraseña de ISE. Guardar como un archivo python para ejecutar.

Asegúrese de que haya una buena conectividad entre ISE y el dispositivo que ejecuta el ejemplo de código de 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

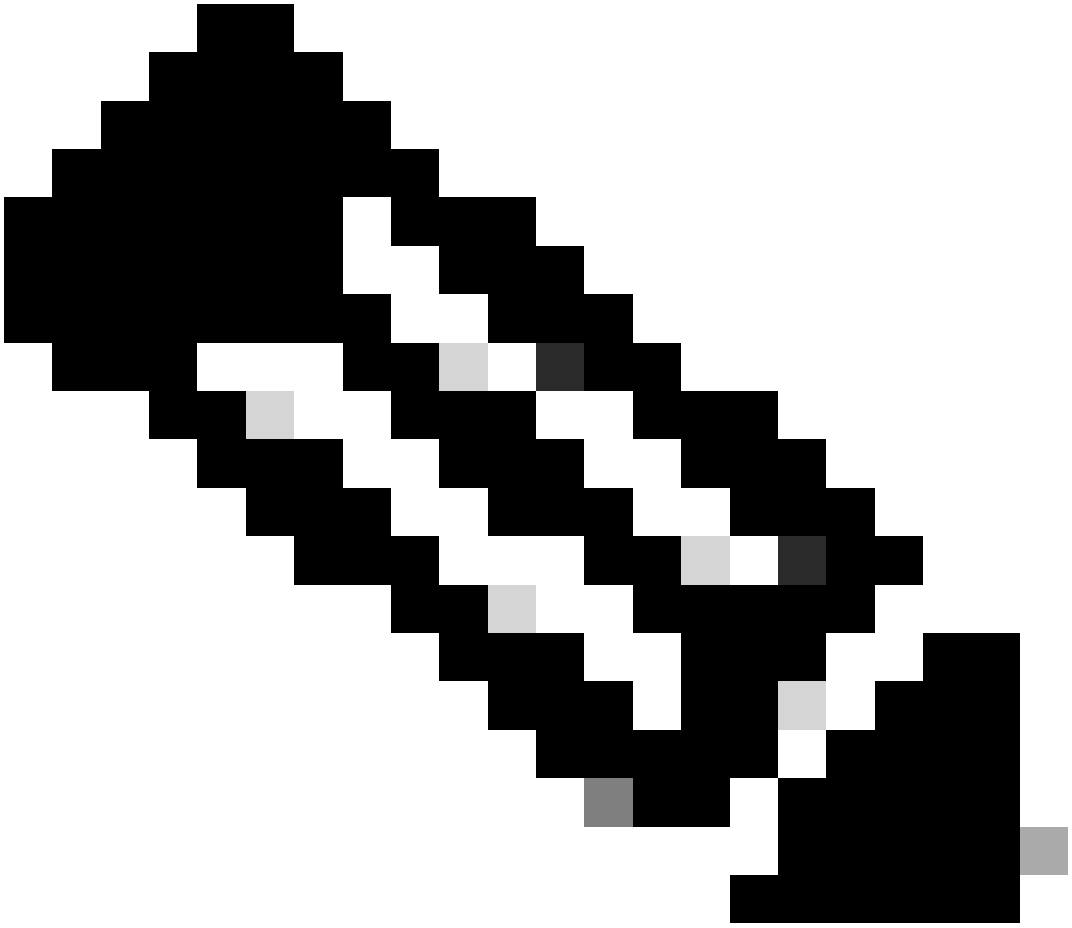
" headers = {

"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: La ID procede de las salidas de la API del paso 3 de "Obtener lista de todos los certificados de confianza", por ejemplo, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 corresponde a "Autoridad de certificación principal pública de clase 3 de VeriSign".

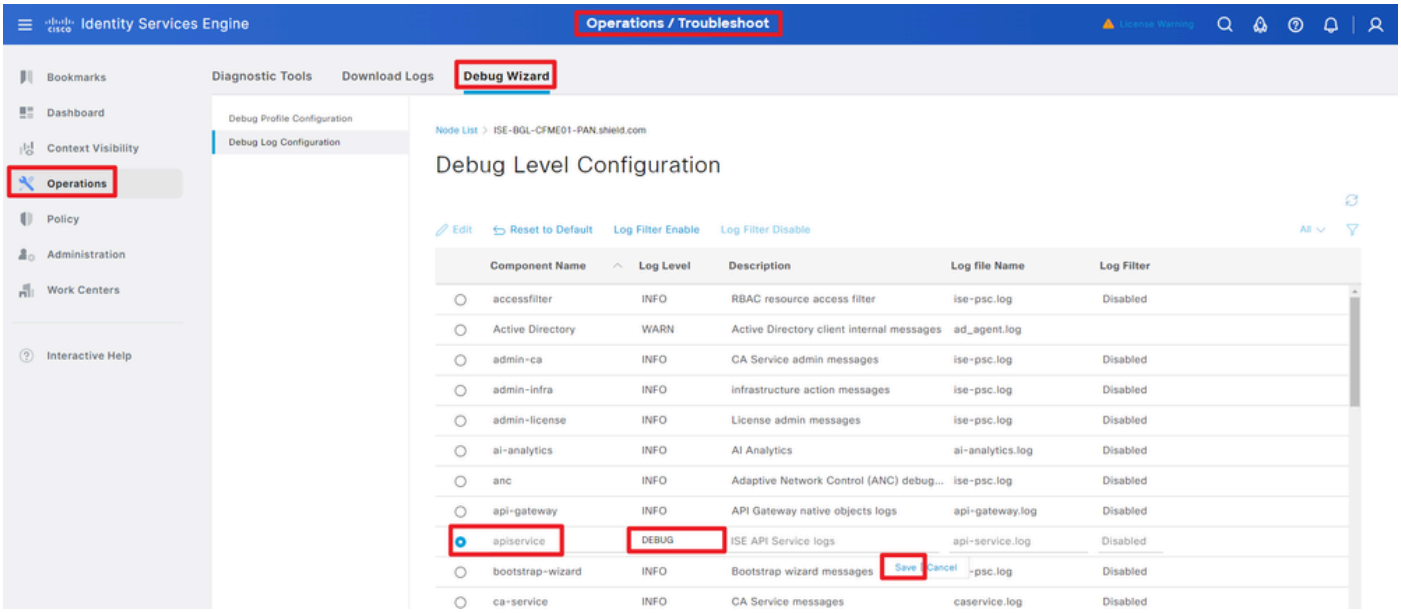
Este es el ejemplo de resultados esperados.

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

Troubleshoot

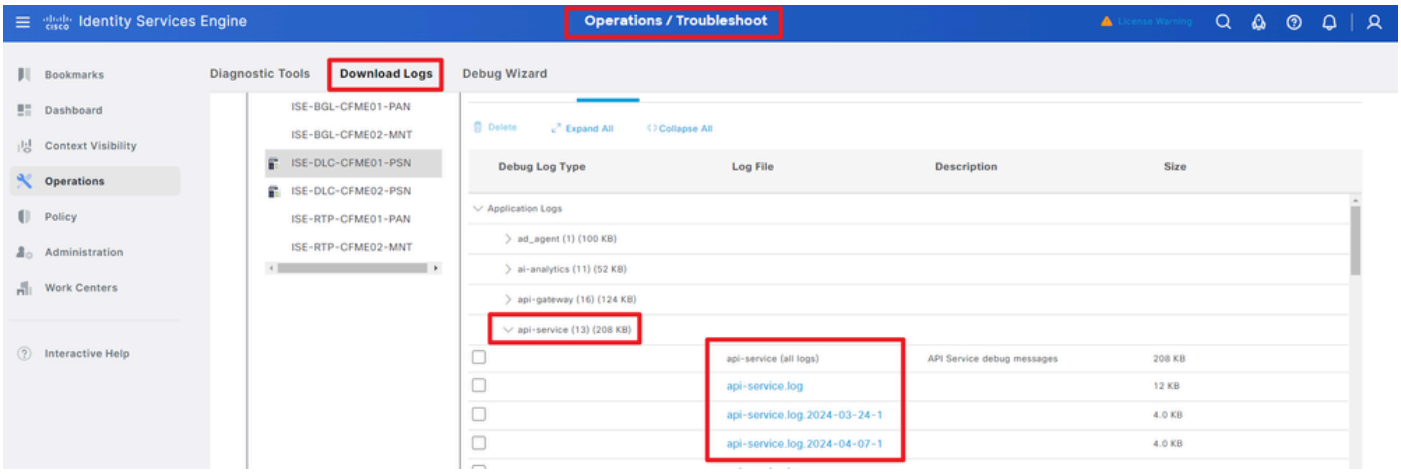
Para resolver problemas relacionados con las API abiertas, establezca **elNivel de registro** para el componente apiservicecomponent enDEBUGen la ventanaConfiguracióndel registro de depuración.

Para habilitar la depuración, vaya a **Operaciones -> Solución de problemas -> Asistente de depuración -> Configuración del registro de depuración -> Nodo ISE -> apiservice.**



Depuración del servicio API

Para descargar los registros de depuración, vaya a **Operaciones -> Solución de problemas -> Registros de descarga -> Nodo ISE PAN -> Registros de depuración.**



Descargar registros de depuración

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).