

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

Contenido

[Introducción](#)

[Background](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración en ISE](#)

[Ejemplos de Python](#)

[Obtener Todos Los Certificados Del Sistema De Un Nodo Determinado](#)

[Obtener Certificado Del Sistema De Un Nodo Determinado Por ID](#)

[Obtener Lista De Todos Los Certificados Protegidos](#)

[Obtener certificado de confianza por ID](#)

[Troubleshoot](#)

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

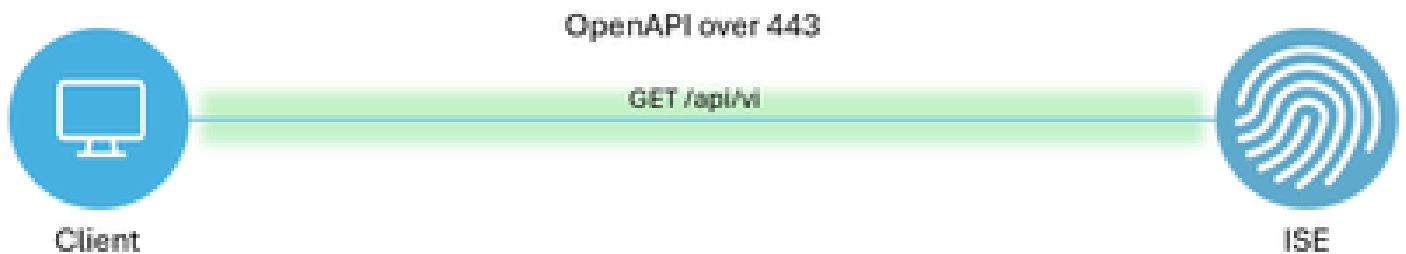
Componentes Utilizados

- 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 a Administración -> Sistema -> Administración -> Administradores -> Usuarios administrativos -> Agregar.

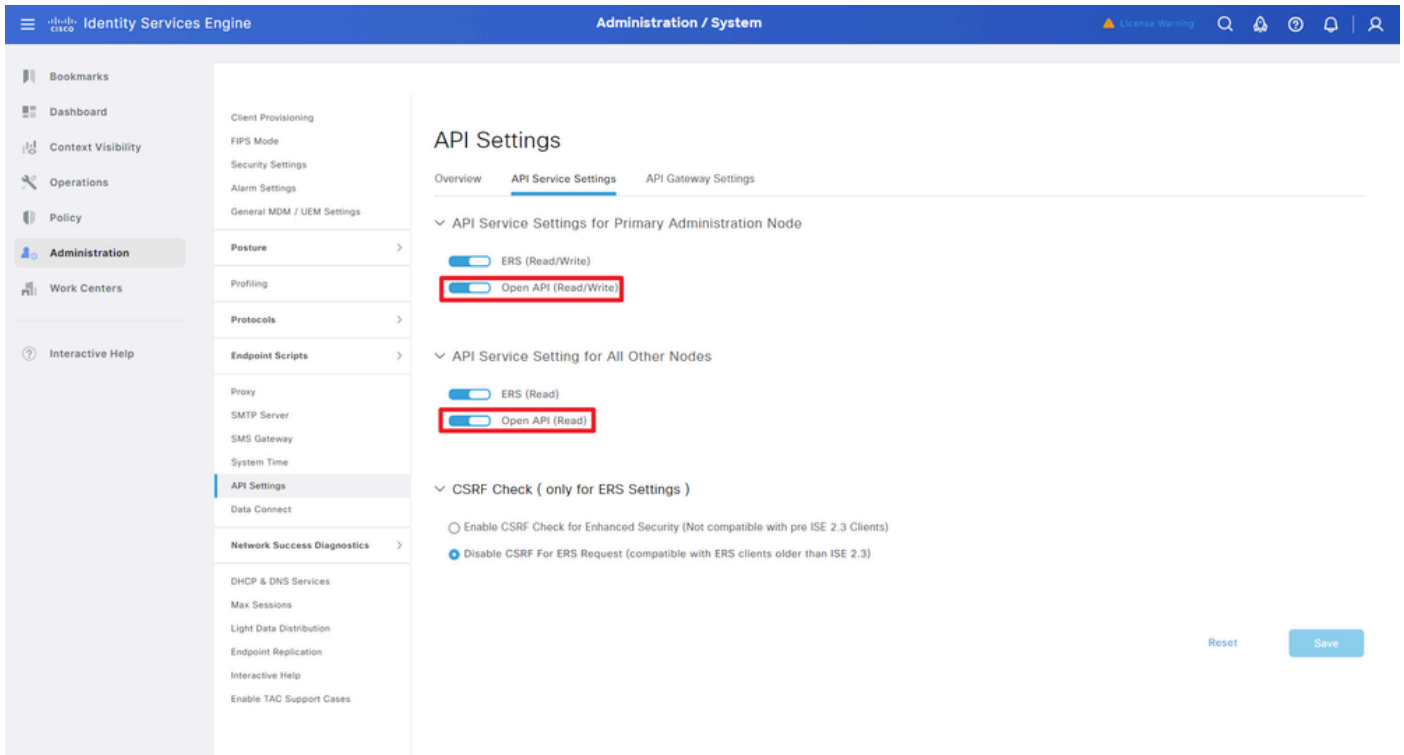
La imagen muestra la interfaz de usuario de Identity Services Engine (ISE) en la pestaña 'Administration / System'. En el menú de navegación a la izquierda, 'Administration' y 'Admin Users' están resaltados con recuadros rojos. En el panel principal, se muestra la sección 'Administrators' con una lista de usuarios. La siguiente tabla resume los datos de la lista:

Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
<input type="checkbox"/>	Enabled	admin				Super Admin
<input type="checkbox"/>	Enabled	ApiAdmin				ERS Admin

Administrador de API

Paso 2: Habilitar API abierta en ISE

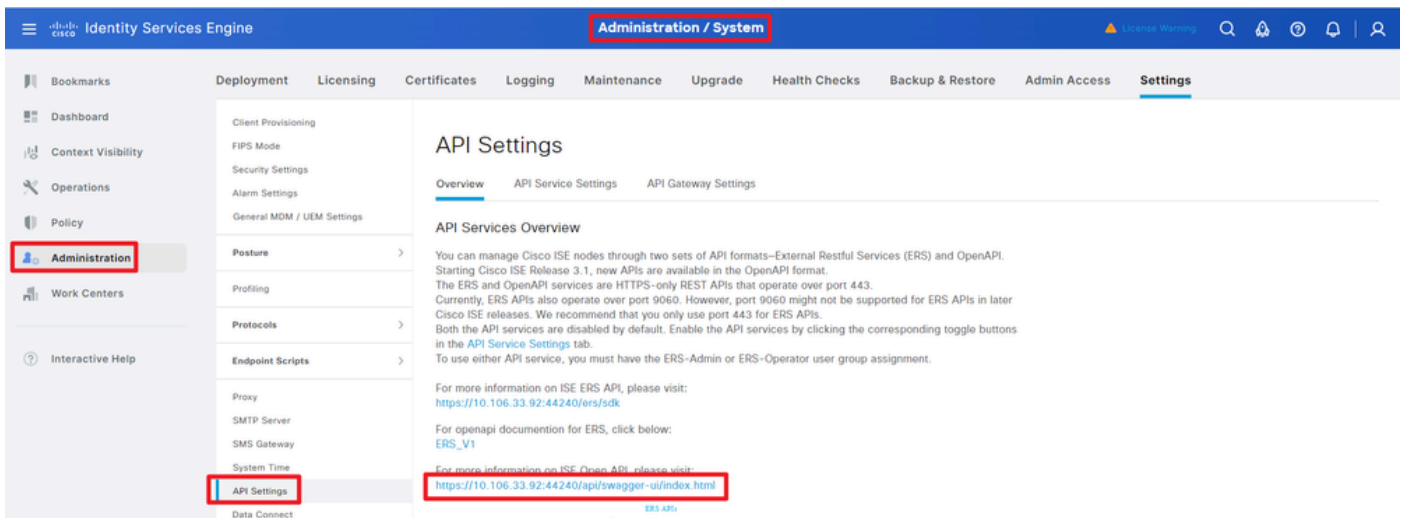
API abierta está desactivada de forma predeterminada en ISE. Para habilitarlo, navegue hasta Administration > System > API Settings > API Service Settings. Active o desactive las opciones de API abierta. Click Save.



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

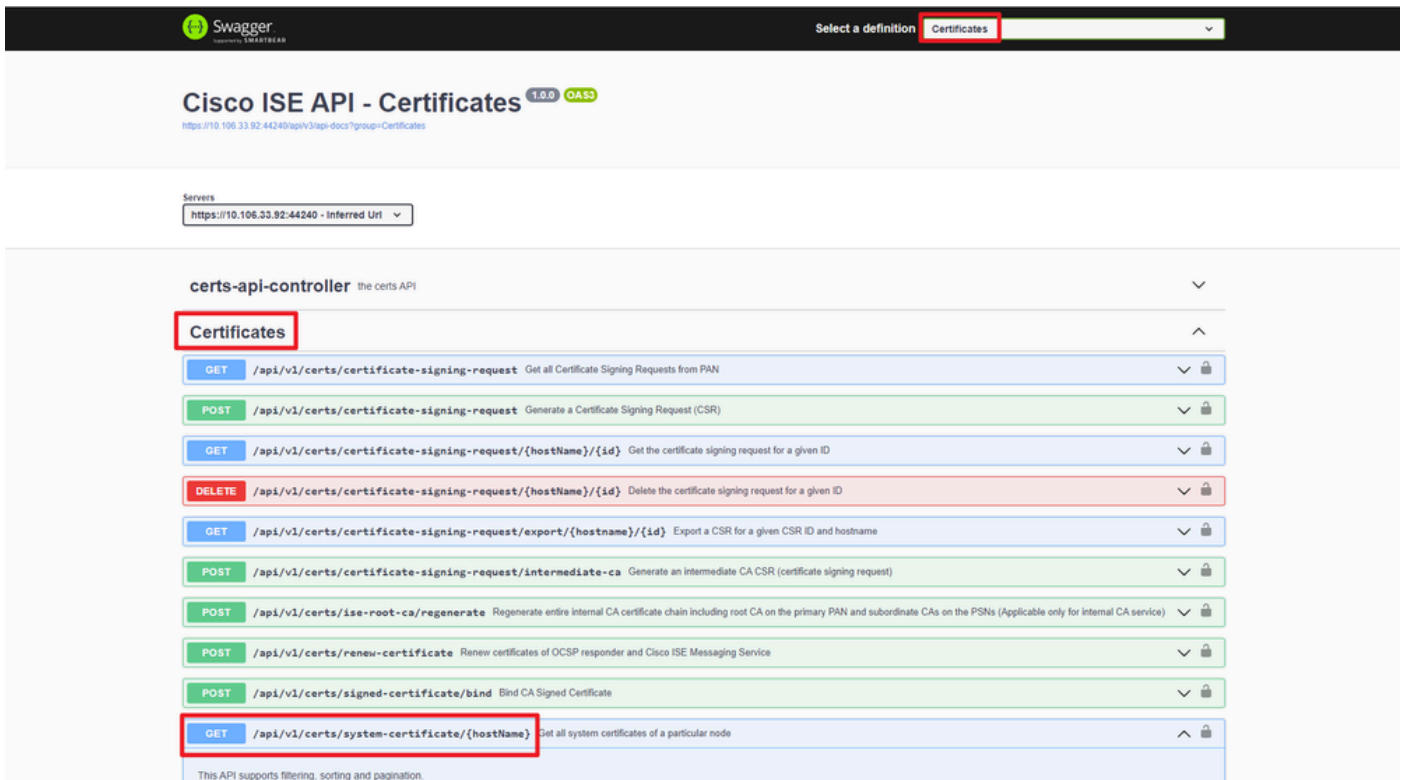
Obtener Todos Los Certificados Del Sistema De Un Nodo Determinado

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-CFME02-PSN'}]}
```

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.

Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v3/api-docs?group=Certificates>

Servers

certs-api-controller the certs API	
Certificates	
GET	/api/v1/certs/certificate-signing-request Get all Certificate Signing Requests from PAN
POST	/api/v1/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)
GET	/api/v1/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given ID
DELETE	/api/v1/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given ID
GET	/api/v1/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname
POST	/api/v1/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)
POST	/api/v1/certs/ise-root-ca/regenerate Regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)
POST	/api/v1/certs/renew-certificate Renew certificates of OCSF responder and Cisco ISE Messaging Service
POST	/api/v1/certs/signed-certificate/bind Bind CA Signed Certificate
GET	/api/v1/certs/system-certificate/{hostName} Get all system certificates of a particular node
GET	/api/v1/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID

This API provides details of a system certificate of a particular node based on given hostname and ID.

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-PSN.cisco.com'}}
```

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.

The screenshot shows a list of API endpoints. The endpoint `GET /api/v1/certs/trusted-certificate` is highlighted with a red box. Below the list, there is a section for filtering and sorting attributes.

This API supports Filtering, Sorting and Pagination.

Filtering and Sorting are supported for the following attributes:

- friendlyName
- subject
- issuedTo
- issuedBy
- validFrom
 - Supported Date Format: yyyy-MM-dd HH:mm:ss
 - Supported Operators: EQ, NEQ, GT and LT
- expirationDate
 - Supported Date Format: yyyy-MM-dd HH:mm:ss
 - Supported Operators: EQ, NEQ, GT and LT
- status
 - Allowed values: enabled, disabled
 - Supported Operators: EQ, NEQ

Note: ISE internal CA certificates will not be exported.

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.

Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v3/app-docs?group=Certificates>

Servers

<https://10.106.33.92:44240> - Inferred Url

certs-api-controller the certs API

Certificates

GET	/api/v1/certs/certificate-signing-request	Get all Certificate Signing Requests from PAN	⌵	🔒
POST	/api/v1/certs/certificate-signing-request	Generate a Certificate Signing Request (CSR)	⌵	🔒
GET	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Get the certificate signing request for a given ID	⌵	🔒
DELETE	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Delete the certificate signing request for a given ID	⌵	🔒
GET	/api/v1/certs/certificate-signing-request/export/{hostname}/{id}	Export a CSR for a given CSR ID and hostname	⌵	🔒
POST	/api/v1/certs/certificate-signing-request/intermediate-ca	Generate an intermediate CA CSR (certificate signing request)	⌵	🔒
POST	/api/v1/certs/ise-root-ca/regenerate	Regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)	⌵	🔒
POST	/api/v1/certs/renew-certificate	Renew certificates of OCSF responder and Cisco ISE Messaging Service	⌵	🔒
POST	/api/v1/certs/signed-certificate/bind	Bind CA Signed Certificate	⌵	🔒
GET	/api/v1/certs/system-certificate/{hostName}	Get all system certificates of a particular node	⌵	🔒
GET	/api/v1/certs/system-certificate/{hostName}/{id}	Get system certificate of a particular node by ID	⌵	🔒

This API provides details of a system certificate of a particular node based on given hostname and ID.

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 el **Nivel de registro** para el componente apiservicecomponent en **DEBUG** en la ventana **Configuración del registro de depuración**.

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

The screenshot shows the 'Debug Wizard' interface in the Cisco Identity Services Engine (ISE) console. The 'Debug Level Configuration' table is displayed, listing various components and their log levels. The 'apiservice' component is selected, and its log level is set to 'DEBUG'. The 'Save' button is highlighted.

Component Name	Log Level	Description	Log file Name	Log Filter
accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled
Active Directory	WARN	Active Directory client internal messages	ad_agent.log	Disabled
admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled
admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled
admin-license	INFO	License admin messages	ise-psc.log	Disabled
ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled
anc	INFO	Adaptive Network Control (ANC) debug...	ise-psc.log	Disabled
api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled
apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled
bootstrap-wizard	INFO	Bootstrap wizard messages	psc.log	Disabled
ca-service	INFO	CA Service messages	caservice.log	Disabled

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**.

The screenshot shows the 'Download Logs' interface in the Cisco Identity Services Engine (ISE) console. The 'api-service (13) (208 KB)' log file is selected. The 'api-service (all logs)' entry is highlighted.

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

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).