

OpenAPI zum Abrufen von ISE-Zertifikatinformationen auf ISE 3.3 verwenden

Inhalt

[Einleitung](#)

[Hintergrund](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration auf der ISE](#)

[Python-Beispiele](#)

[Abrufen aller Systemzertifikate eines bestimmten Knotens](#)

[Systemzertifikat eines bestimmten Knotens nach ID abrufen](#)

[Liste aller vertrauenswürdigen Zertifikate abrufen](#)

[Vertrauenswürdigen Zertifikat nach ID abrufen](#)

[Fehlerbehebung](#)

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

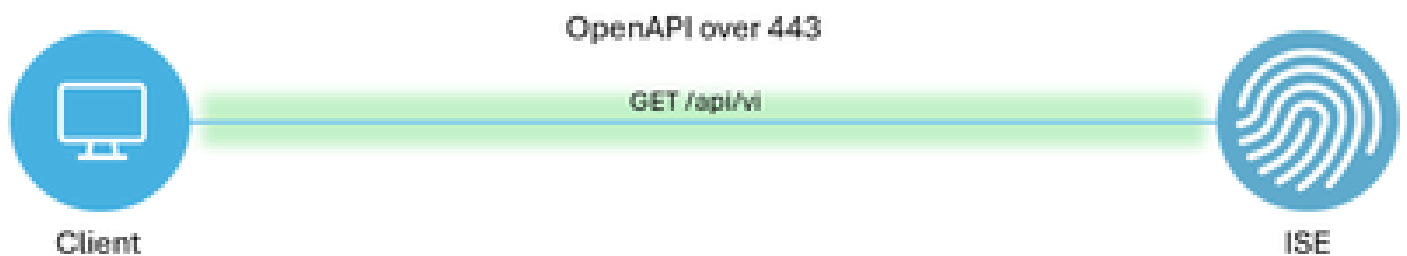
Verwendete Komponenten

- 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

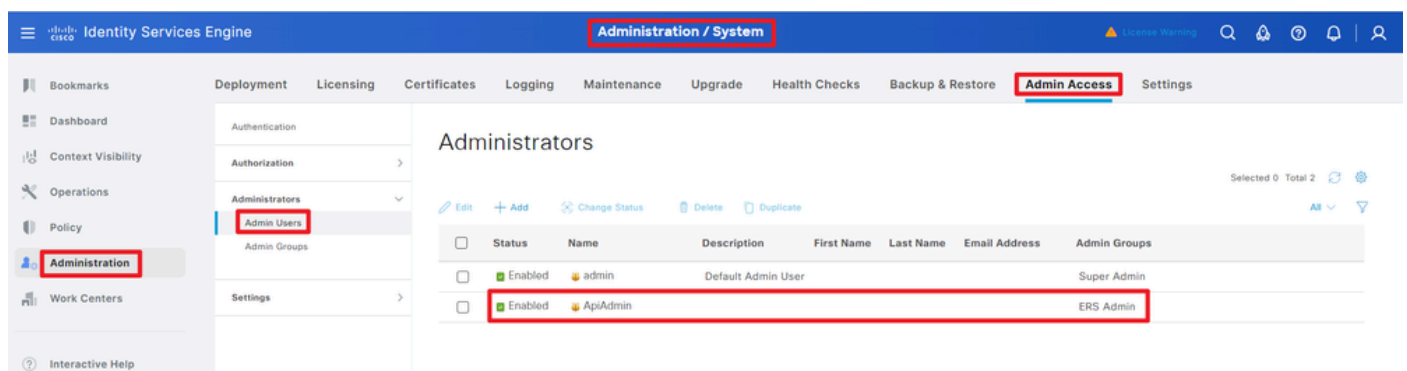


Topologie

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.

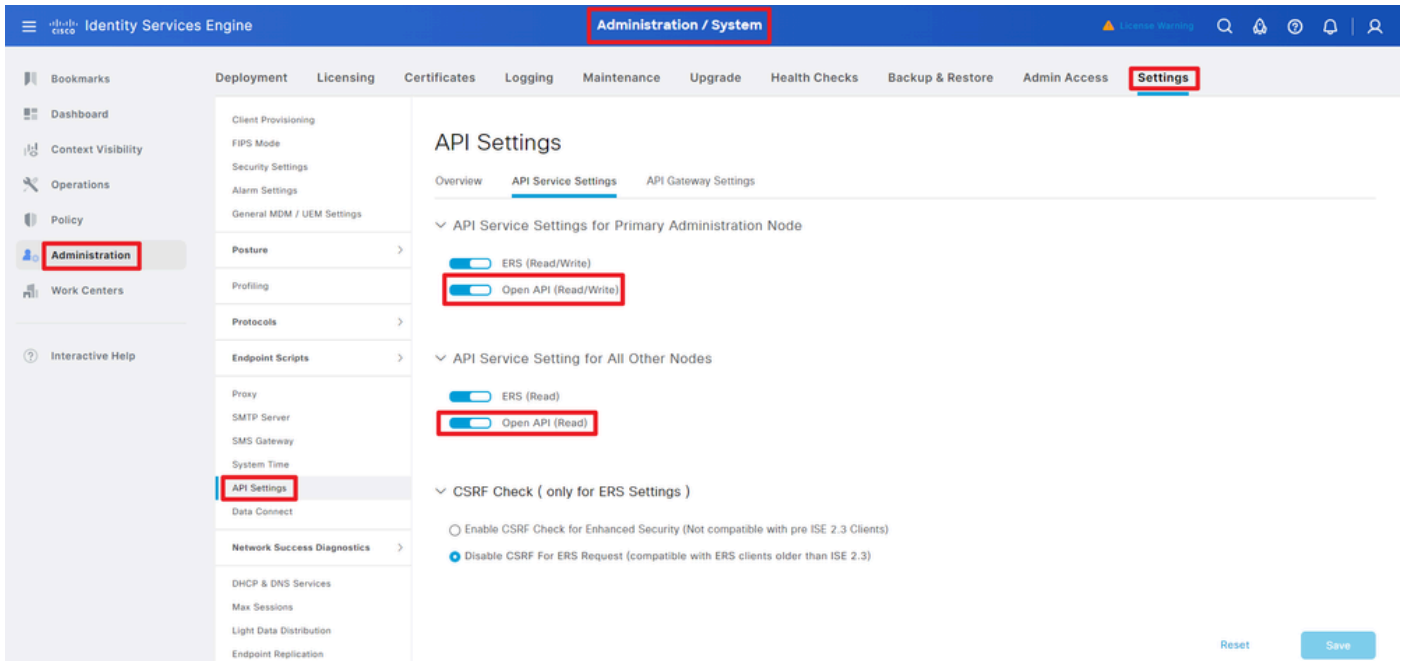


API-Administrator

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

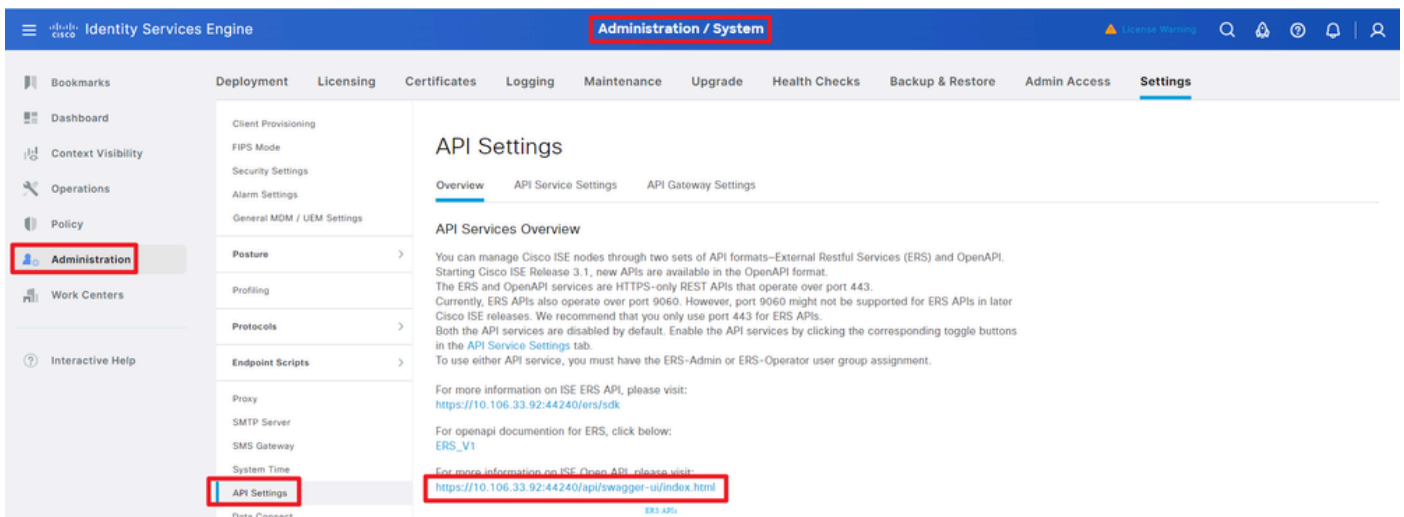
API-Optionen um. Klicken Sie auf Speichern.



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.

The screenshot shows the Swagger UI for the Cisco ISE API. The 'Certificates' section is expanded and highlighted with a red box. The endpoint '/api/v1/certs/system-certificate/{hostname}' is also highlighted with a red box. The endpoint description is 'Get all system certificates of a particular node'.

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-CFME02-PSN'}]}
```

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.

Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v3/app-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.

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

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.

The screenshot shows the Cisco ISE API Explorer interface. The endpoint `/api/v1/certs/trusted-certificate` is highlighted with a red box. The interface lists various API endpoints with their methods (POST, GET, PUT, DELETE) and descriptions. Below the endpoint list, there is a section for filtering and sorting attributes, including `friendlyName`, `subject`, `issuedTo`, `issuedBy`, `validFrom`, `expirationDate`, and `status`. A note at the bottom states: "Note: ISE internal CA certificates will not be exported."

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
```

Vertrauenswürdigen 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.

Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v3/api-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 OCSP 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.

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 die **Log**-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**.

The screenshot shows the 'Debug Wizard' interface in the Cisco Identity Services Engine. The 'Debug Level Configuration' table is displayed with the following data:

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

Debuggen von API-Diensten

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

The screenshot shows the 'Download Logs' interface in the Cisco Identity Services Engine. The 'api-service' log type is selected, and the 'api-service.log' file is highlighted for download.

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

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.