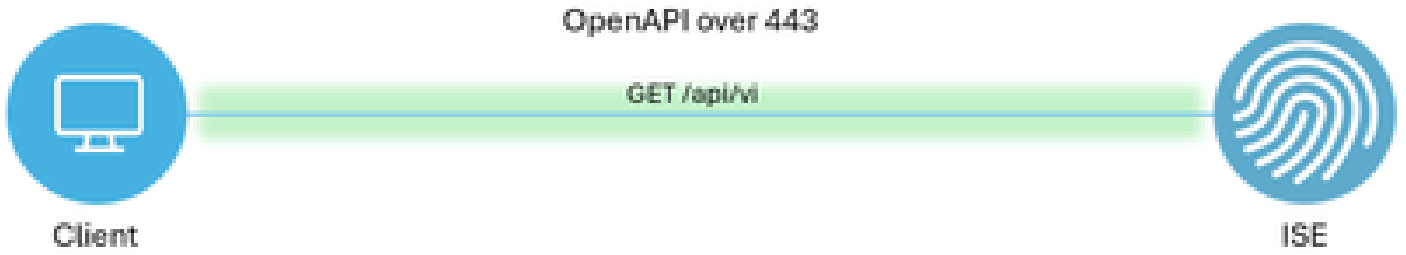


- ISE 3.3
- نوثياب 3.10.0

ةصاخ ةيلعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراول تامولعمل اءاشنإ مت تناك اذا (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمج تادب رما يال لمحتحمل ريثاتلل كمهف نم دكأتف ،ليغشتلا ديقتك تكتبش

نيوكتلا

ةكبش للى طيختلا مسرلا

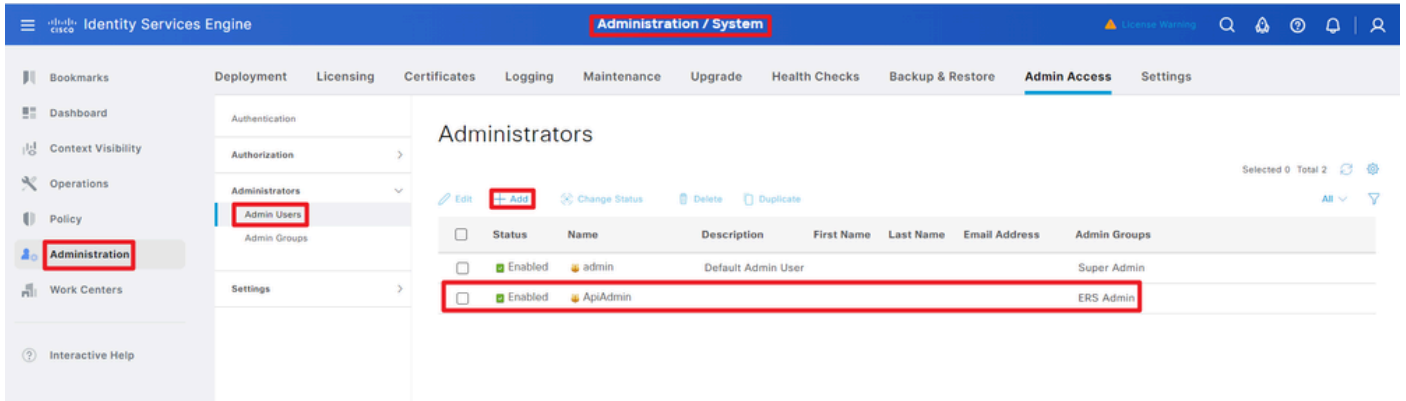


طخملا

ISE لىل نيوكتلا

ةحوتفم تاقيبطت ةجرمب ةهجاو لوؤسم باسح ةفاضل: 1 ةوطخل

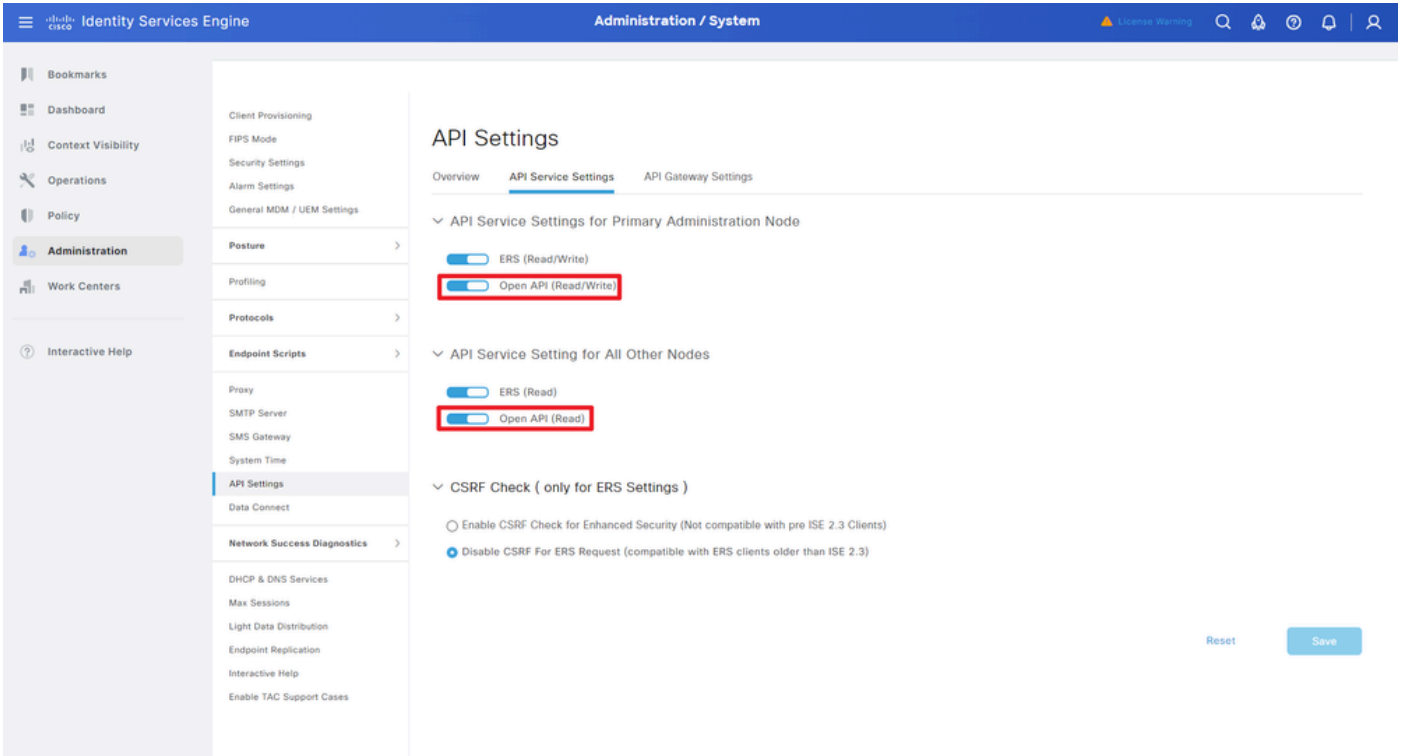
نومدختسمل -> نولوؤسملا -> ةرادال -> ماظنلا -> ةرادال لىل لقتنا ، API لوؤسم ةفاضل ةفاضل -> نويرادال



API لوؤسم

ISE لىل ةحوتفملا تاقيبطتلا ةجرمب ةهجاو نيكتم: 2 ةوطخل

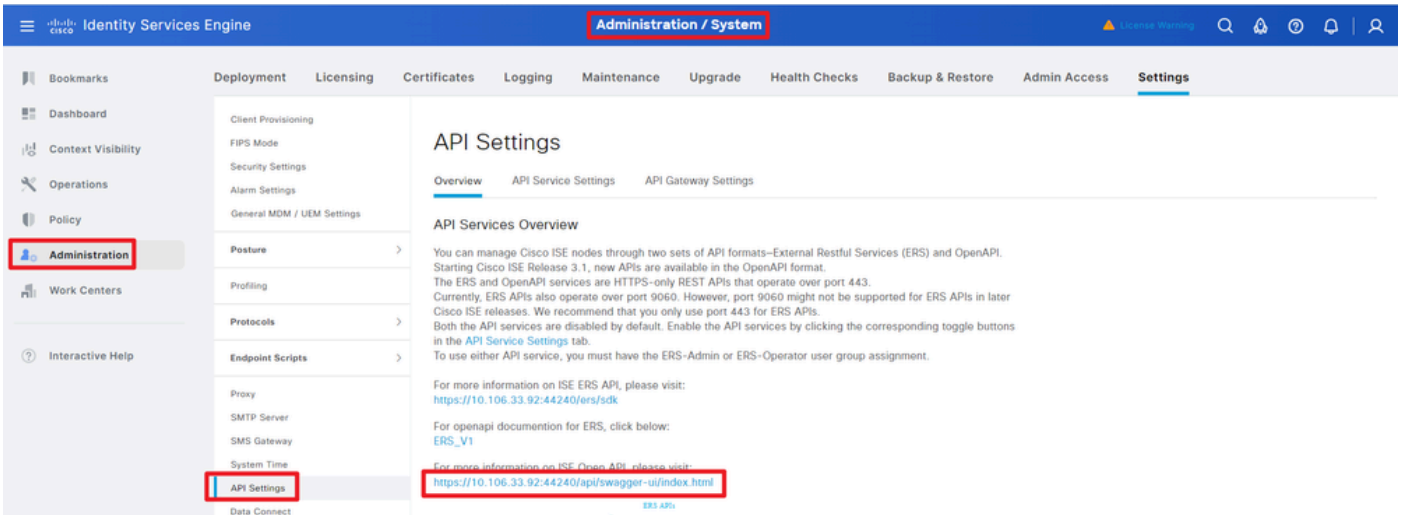
اذه نيكتم تل ISE لىل يضا رتفا لكشب ةحوتفملا تاقيبطتلا ةجرمب ةهجاو لىل طعت متي لىل دبت API ةمدختسمل اءادع > تاقيبطتلا ةجرمب ةهجاو اءادع > ماظن > ةرادال لىل لقتنا ، رايخل ظفح قوف رقتنا . ةحوتفملا تاقيبطتلا ةجرمب ةهجاو تارايل



OpenAPI نيكمت

ISE OPEN API ةحوتفملا تاقيبطتلا ةجرمب ةهجاو فاشكتسا: 3 ةوطخلا

حتف قوف رقنا . ةماع ةرطن > تاقيبطتلا ةجرمب ةهجاو تاداع | > ماظن > ةراد | لىل لقتنا تاقيبطتلا ةجرمب ةهجاو ةرايز طابترا .



OpenAPI ةرايز

نوئياب ةلثما

ةنيعم ةدقعل ماظنلا تاداهش عيمج لىل لوصحلا

ةنيعم ISE ةدق تاداهش عيمج (API) تاقيبطتلا ةجرمب ةهجاو درسي

(API) تاقيبطتلا ةجرمب ةهجاو ةاعدتسال ةبولطملا تامولعمل: 1 ةوطخلا

قوي رط	راضح
URL	https://<ISE-pan-IP>/API/v1/certs/system-certificate/<ISE-Node-Hostname>
دامت عال تاناي ب	حوت فم ل API باسح دامت عال تاناي ب م ادخت سا
يسيئر ل ناو نعال	قوي رط ل: لوبق قوي رط ل: يوت حمل اعون

ة. نيم ISE ةدق تاداهش دادر تسال هم ادخت سا متي يذال URL ع قوم ددح: 2 ةوطخل

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

الوطخل 3: ةوطخل Python زمر لعل لاثم انه. ةوصلو يوت حمل احسنا. ISE ip, username, هذيفنتل نوئي اب فلمك طفح. ةم لك

python زمر لاثم لغشي يذال زاه لال او ISE ني ب دي لال لاصتال نم دكأت

```
<#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())

```

ةةقوت مل جتاونل لىل لاثم لىل امىفو.

Return Code:

200

Expected Outputs:

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

فر عمل بسح ةنى عم ةدق عل ماظن ةداهش لىل لوصح ل

مسا لىل اءانسا ةنى عم ةدق عل ماظن ةداهش لىل صافات هذة تاقي ببط ل ةجرم رب ةه جا ورفوت
نى دءح مل فر عمل او فىض مل

(API) تاقي ببط ةجرم رب ةه جا وءاءءتسال ةبول طمل تامول عمل ل: 1 ةوطخ ل

ةقيرط	راضل
URL	https://<ISE-pan-IP>/API/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-of-Certificate>
ءامءال اءاناب	ءوتف مل API باسء ءامءعا اءاناب ءاءءتسا
فىسئىرل ناونع ل	لوبق: لوبق/ءق ببط ل لوىءح مل عون: لوبق/ءق ببط ل

مسا لىل اءانسا ةنى عم ةدق ةداهش ءاءرتسال هماءءتسا لىل ءىل ذل URL ع قوم ءءح: 2 ةوطخ ل
ءءح مل فر عمل او فىض مل

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 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

هذيفنن تل نوٹياب فللمك طفح. ةم لك Python زم رىل لاثم انه 3 ةوطخل ل ISE ip، username، تل دبتسا. ةقصلو ىوتحمل ا خسنا.

python زم ر لاثم لغشي يذلا زاوجل او ISE ني ب دي جلا لاصلتال نم دكأت

<#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:")
```

نم 3 ةوطخلال ي (API) تاقىبطلتلة جمر ب ةه او تاجرم نم وه فرعملال :ةظالم
لاثلما لى بس لىل ، 5b5b28e4-2a51-495c-8413-610190e1070b وه سامل ةءاهش عىم لىل لوصحل
- CN=SAML_ISE-DLC-CFME02-PSN.cisco.com سامل ةءاهش " وه

ةءقوتملال جتاونلال لىل لائل امىفو

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'}}

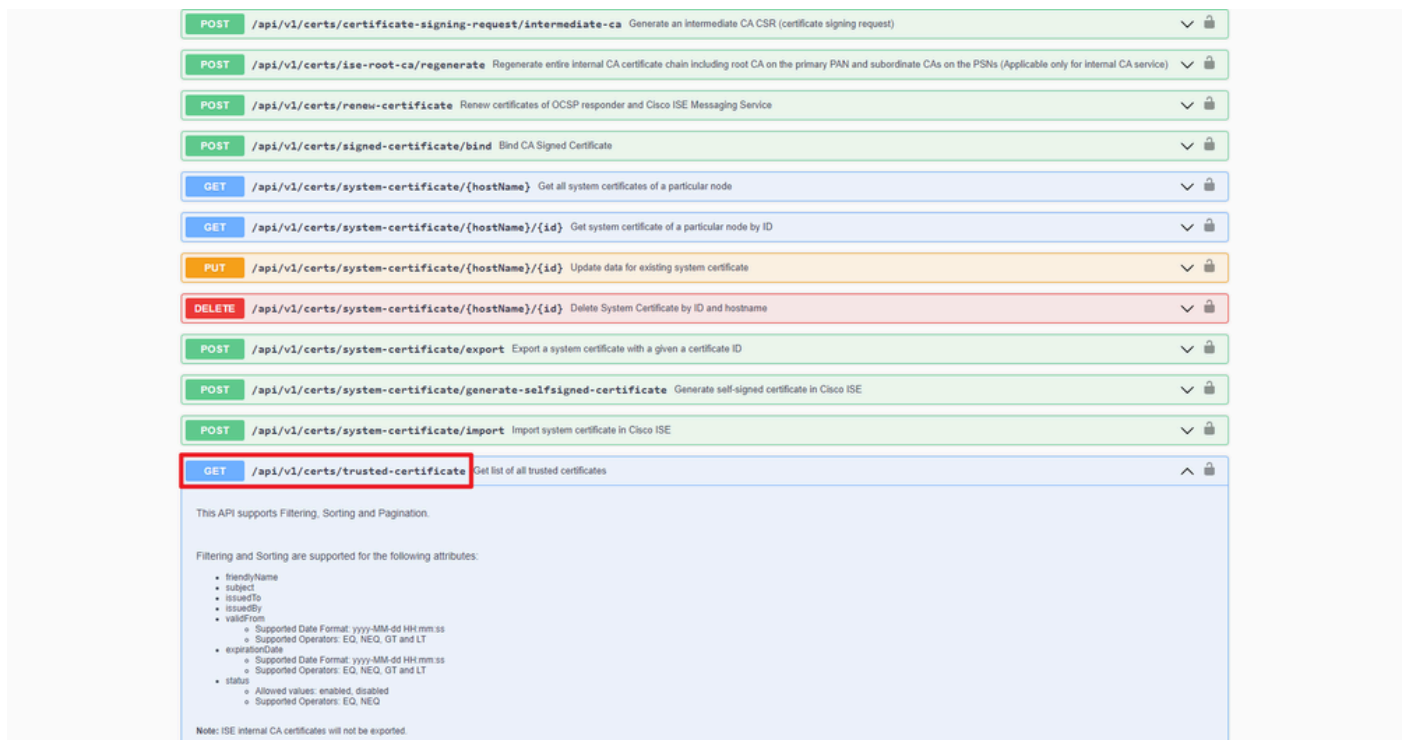
اهب قوئوملال تءاهشلال ةفالكب ةمئاق لىل لوصحل

ISE ةومجمل اهب قوئوملال تءاهشلال عىم (API) تاقىبطلتلة جمر ب ةه او درسى

(API) تاقى ببط ةجمر ب ةهجاو ةاعدت سالا ةبولطم لال تامول عملال 1: ةوطخلال

ةقيرط	راضا
URL	https://<ISE-pan-IP>/API/V1/CERTS/Trusted-certificate
دامت ةالال تانايب	حوت فم لال API باسح دامت ةالال تانايب مادخت سا
يسير لال ناونع لال	قوي ببط لال : لوبق قوي ببط لال : يوت حملال عون

اهب قوتوم لال تاداهش لال دادر ت سالا هم مادخت سا متي يذال URL ةقوم ددح 2: ةوطخلال



API URI

ةوطخلال 3: ةوطخلال Python زم رىل ةلالام انه. ةوصلو يوت حملال خسنا. ISE ip، username، هذيفنتل نوثياب فللمك ظفح. ةمللك

python زم رلالام لغشي يذال زاهجالل ISE ني ب ديجلال لاصتالال نم دكأت

<#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:")
```

فوذحم). ةقوت م ل ج تاو ن ل ل ع ل ا ث م ي ل ي ا م ي ف و

Return Code:

200

Expected Outputs:

```
{'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=VeriSign Class 3 Public Primary Certification Authority'}]}
```

فر ع م ل ا ب س ح ة ق ث ة د ا ه ش ل ع ل و ص ح ل ا

د د ح م فر ع م ل ا ل ا د ن ت س ت ة ق ث ة د ا ه ش ل ل ي ص ا ف ت ض ر ع ه ذ ه ت ا ق ي ب ط ت ل ا ة ج م ر ب ة ه ج ا و ل ن ك م ي

ا ل ا (API) ت ا ق ي ب ط ت ة ج م ر ب ة ه ج ا و ا ع ا د ت س ا ل ة ب و ل ط م ل ا ت ا م و ل ع م ل ا : 1 ة و ط خ ل ا

ة ق ي ر ط	ر ا ض ح ا
URL	https://<ISE-pan-IP>/API/v1/certs/trusted-certificate/<id-of-certificate>
د ا م ت ع ا ل ا ت ا ن ا ي ب	ح و ت ف م ل ا API ب ا س ح د ا م ت ع ا ت ا ن ا ي ب م ا د خ ت س ا
ي س ي ئ ر ل ا ن ا و ن ع ل ا	ل و ب ق /json ق ي ب ط ت ل ا ي و ت ح م ل ا ع و ن /json ق ي ب ط ت ل ا

ر ش ن ل ا ت ا م و ل ع م د ا د ر ت س ا ل ه م ا د خ ت س ا م ت ي ي ذ ل ا URL ع ق و م د د ح : 2 ة و ط خ ل ا

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.

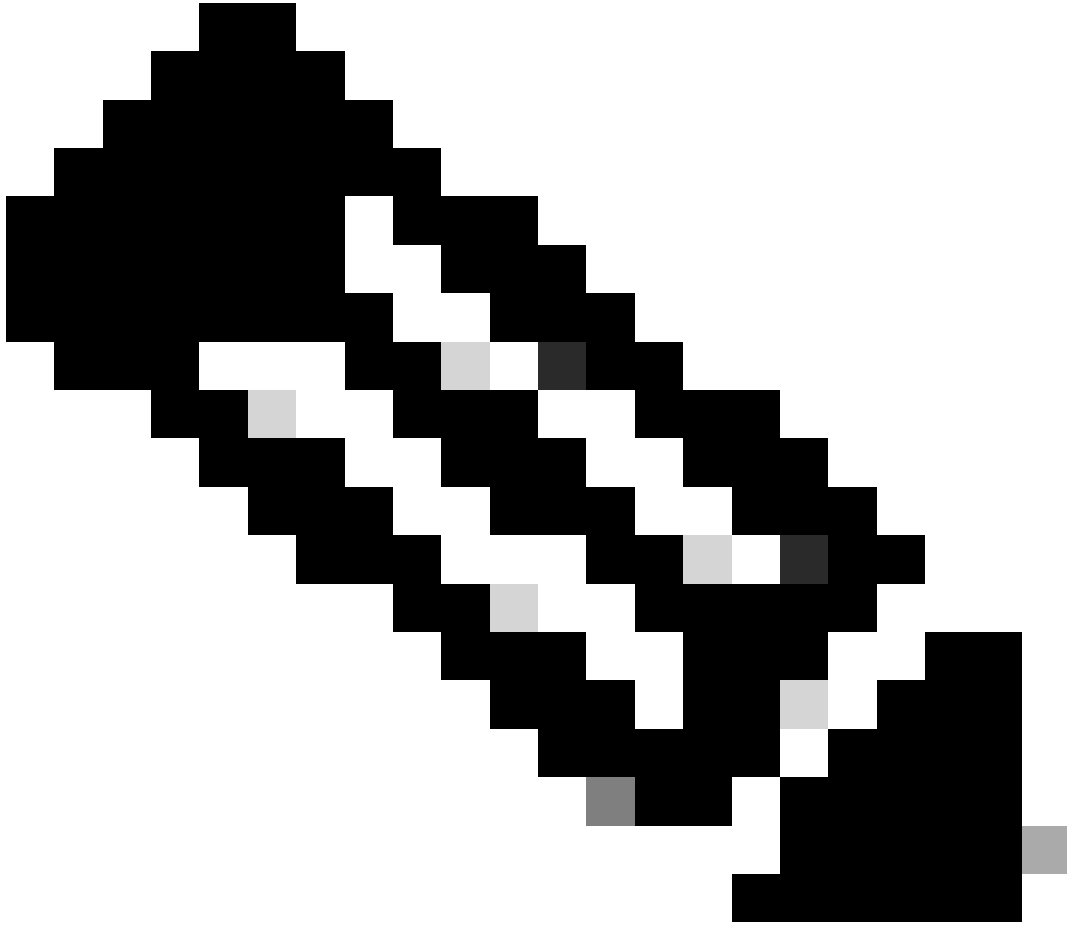
API URI

هذيفنتل نوثي اب فل مك ظفح .ةم لك
Python. زمر لىل ع لاثم انه :3 ةوطخلل
ISE ip، username، ل ل دبت سا .ه قصلو يوتحم لاخ سنا .

python. زمر ل لاثم ل غشي يذلا زاهجلاو ISE نيب دي جلا لاصتالا نم دكأت

<#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:")
```



تاداهشللا عيمجب ةمئاق ىلع لوصحلا نم 3 ةوطخلا يف (API) تاقببطللا ةجمرب ةهجاو تاجرخم نم وه فرعما :ةظحالم
ةئفلا نم ماعلا يساسألا قيصتلا عجرم" وه 147d97cc-6ce9-43d7-9928-8cd0fa83e140 ،لاثملا لابس ىلع ،ةقوثوملا
3 يف VeriSign".

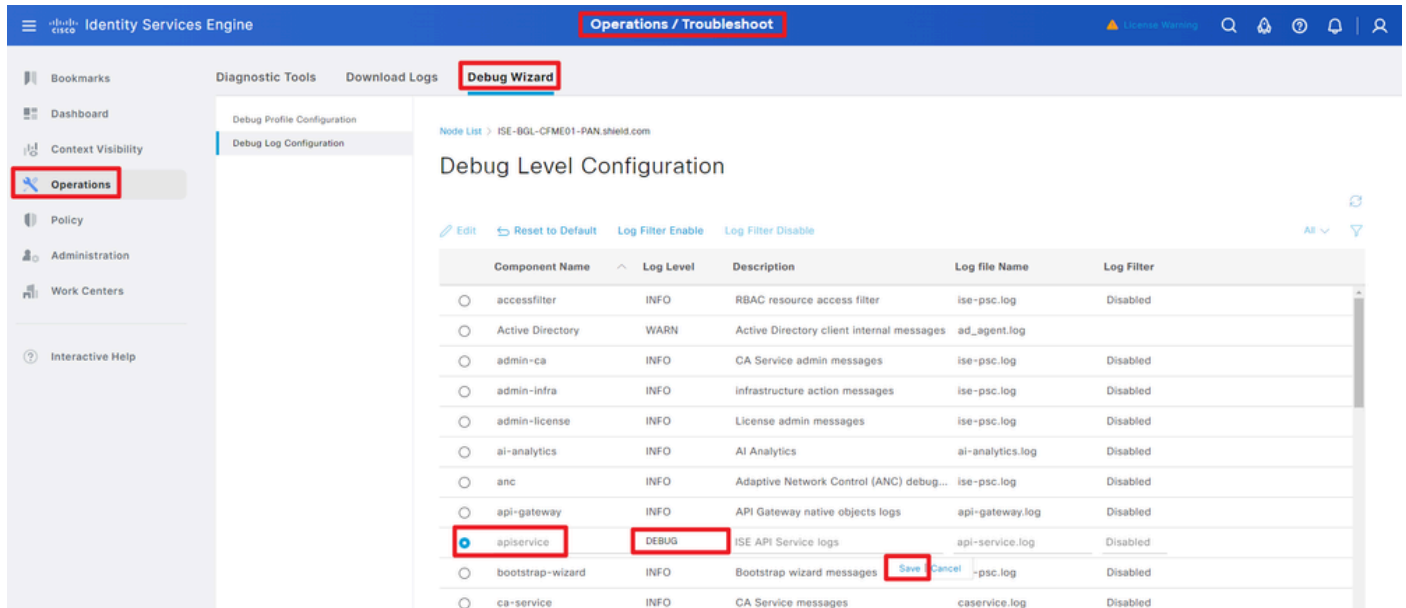
ةقوثوملا جتاونلا ىلع لاثم يلي اميفو.

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

اهالصا وءاطخألا فاشكتسا

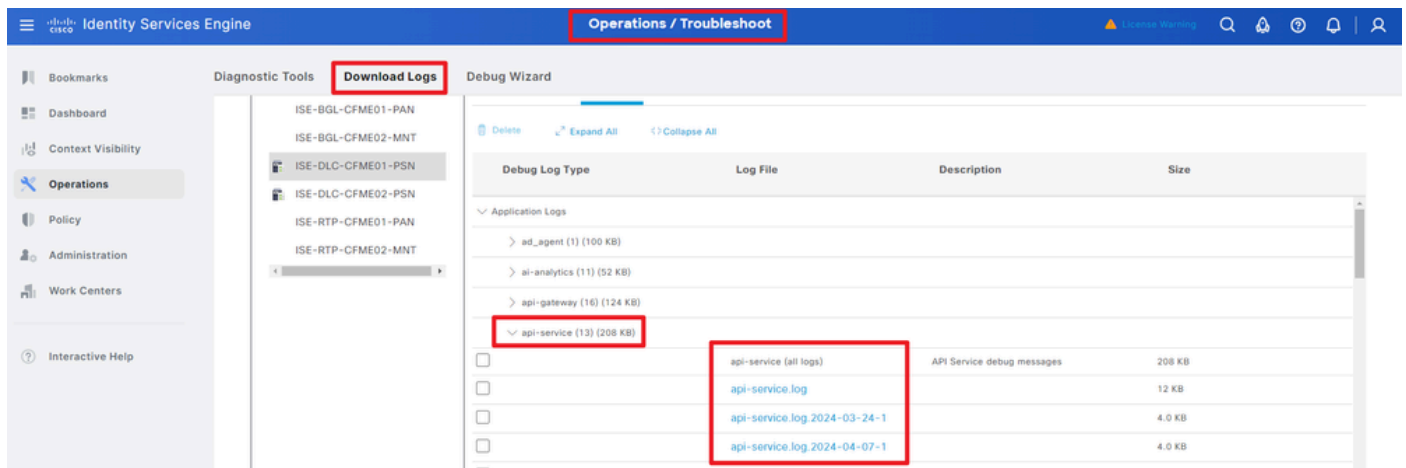
ل Log Level نبي عيب مق ، ةحوت فم ال تاقبي بط ل ا ةم ررب ت ا ةو ب ةق ل ع ل م ال ا ة حال ص و ا ة ط خ ا ا ة ط خ ا فاش ك ت س ال TaskServiceClient لى DEBUG In Debug Log Configuration Window.

ةدق ع -> ا ة ط خ ا ل ج س ن ي و ك ت -> ا ة ط خ ا ل ا ة ح ص ت ج ل ا ع م -> ا ة حال ص و ا ة ط خ ا ل ا فاش ك ت س ا -> ت ا ي ل م ع ل ا ل ل ل ق ت ن ا ، ا ة ط خ ا ل ا ة ح ص ت ن ي ك م ت ل ةز ي م -> ISE.



ةم د خ ا ة ط خ ا ل ا ة ح ص ت API

ت ال ج س -> ISE PAN ةدق ع -> ل ي ز ن ت ل ا ت ال ج س -> ا ة حال ص و ا ة ط خ ا ل ا فاش ك ت س ا -> ت ا ي ل م ع ل ا ل ل ل ق ت ن ا ، ا ة ط خ ا ل ا ة ح ص ت ت ال ج س ل ي ز ن ت ل ا ة ط خ ا ل ا ة ح ص ت .



ا ة ح ص ت ل ا ت ال ج س ل ي ز ن ت

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل