

Uso di OpenAPI per ottenere informazioni sui certificati ISE su ISE 3.3

Sommario

[Introduzione](#)

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione su ISE](#)

[Esempi di Python](#)

[Ottieni Tutti I Certificati Di Sistema Di Un Nodo Specifico](#)

[Ottieni Il Certificato Di Sistema Di Un Nodo Specifico In Base All'ID](#)

[Ottieni Elenco Di Tutti I Certificati Attendibili](#)

[Ottieni certificato di attendibilità per ID](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la procedura per utilizzare openAPI per gestire il certificato Cisco Identity Services Engine (ISE).

Introduzione

Di fronte alla crescente complessità nella gestione e nella sicurezza della rete aziendale, Cisco ISE 3.1 introduce API in formato OpenAPI che semplificano la gestione del ciclo di vita dei certificati, offrendo un'interfaccia standardizzata e automatizzata per operazioni di certificazione efficienti e sicure, aiutando gli amministratori ad applicare procedure di sicurezza efficaci e a mantenere la conformità della rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

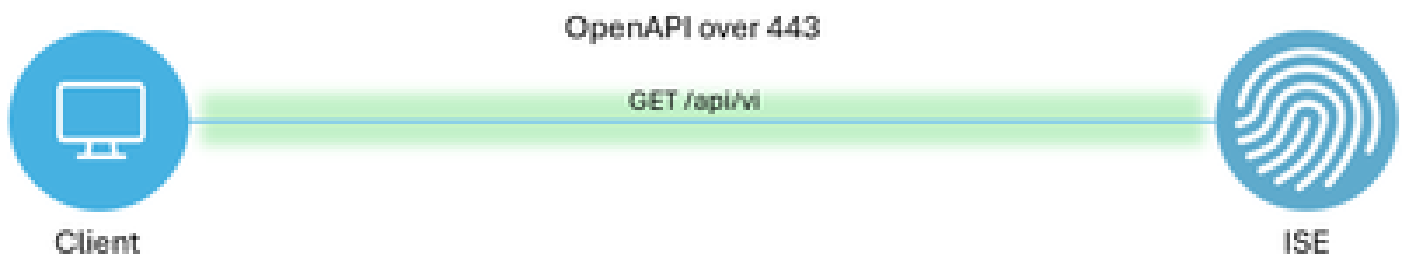
Componenti usati

- ISE 3.3
- Python 3.10.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Topologia

Configurazione su ISE

Passaggio 1: Aggiungere un account amministratore Open API

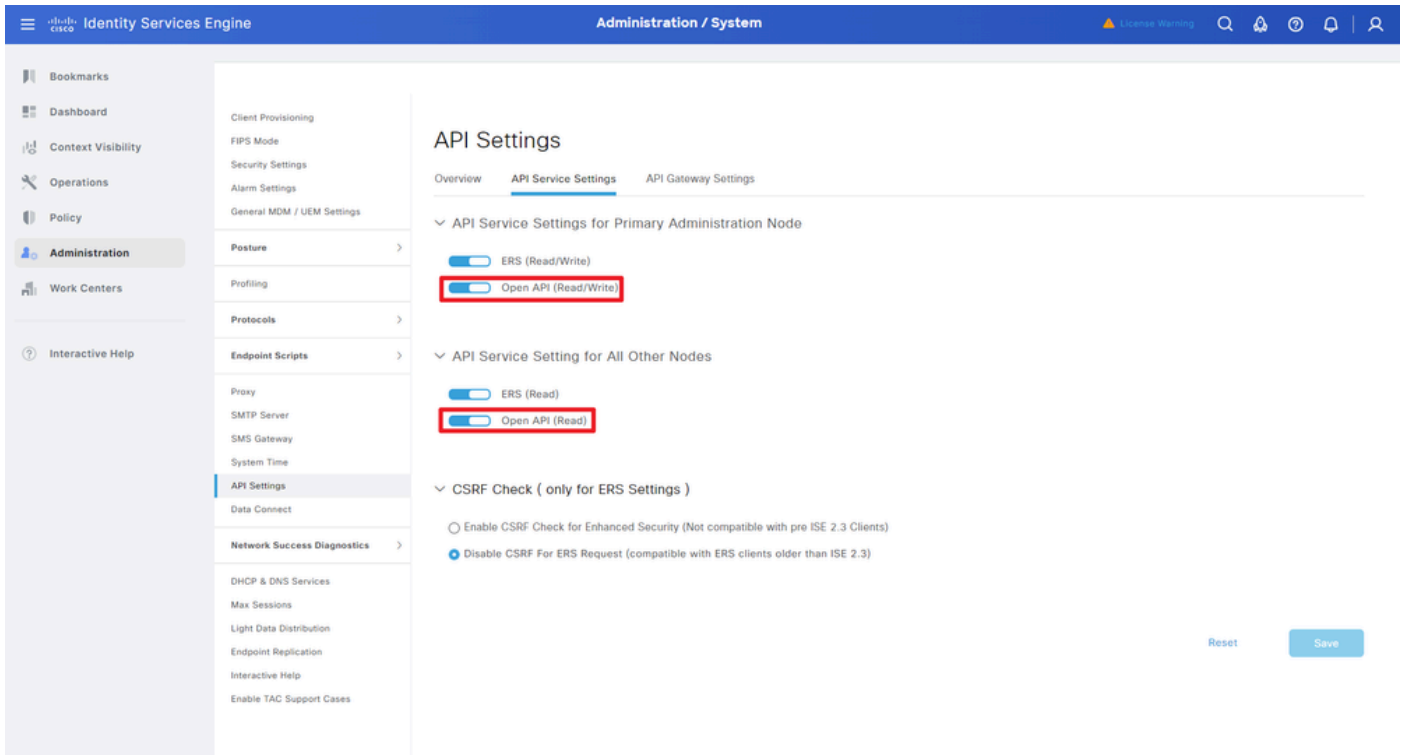
Per aggiungere un amministratore API, selezionare Amministrazione -> Sistema -> Amministrazione -> Amministratori -> Utenti amministratori -> Aggiungi.

Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
Enabled	admin	Default Admin User				Super Admin
Enabled	ApiAdmin					ERS Admin

Amministratore API

Fase 2: Abilitare Open API su ISE

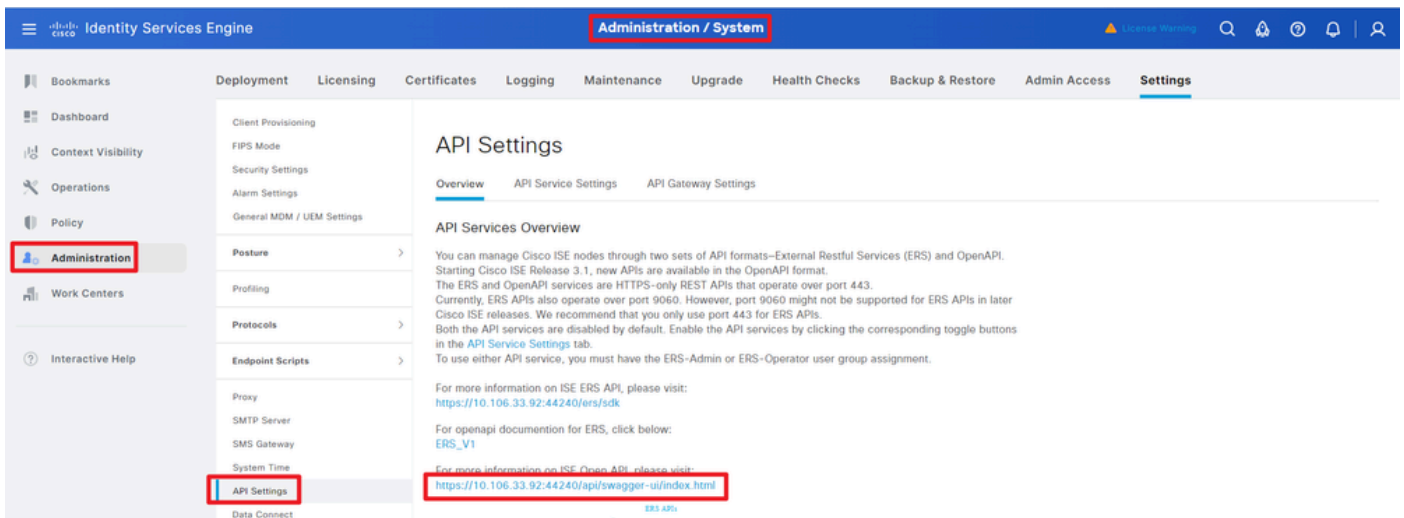
Open API è disabilitato per impostazione predefinita su ISE. Per abilitarlo, selezionare Amministrazione > Sistema > Impostazioni API > Impostazioni servizio API. Attivate o disattivate le opzioni di Open API. Fare clic su Save (Salva).



Abilita OpenAPI

Passaggio 3: Esplora ISE open API

passare ad Amministrazione > Sistema > Impostazioni API > Panoramica. Fare clic sul collegamento Apri API.



Visita OpenAPI

Esempi di Python

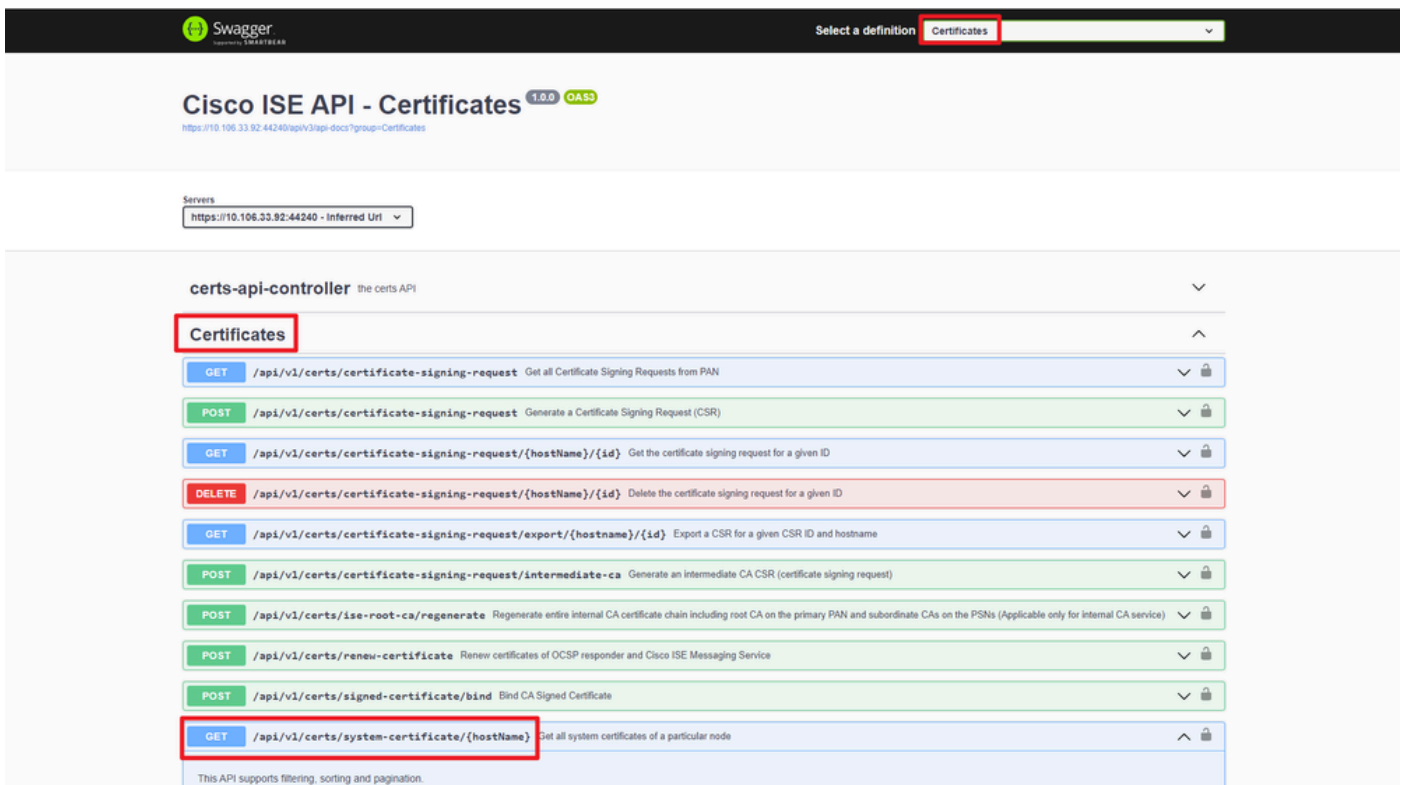
Ottieni Tutti I Certificati Di Sistema Di Un Nodo Specifico

L'API elenca tutti i certificati di un particolare nodo ISE.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare i certificati di un particolare nodo ISE.



URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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())

```

Di seguito è riportato l'esempio degli output previsti.

Return Code:

200

Expected Outputs:

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

Ottieni Il Certificato Di Sistema Di Un Nodo Specifico In Base All'ID

Questa API fornisce i dettagli di un certificato di sistema di un particolare nodo in base al nome host e all'ID specificati.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-of-Certificate>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare il certificato di un particolare nodo in base al nome host e all'ID specificati.

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.

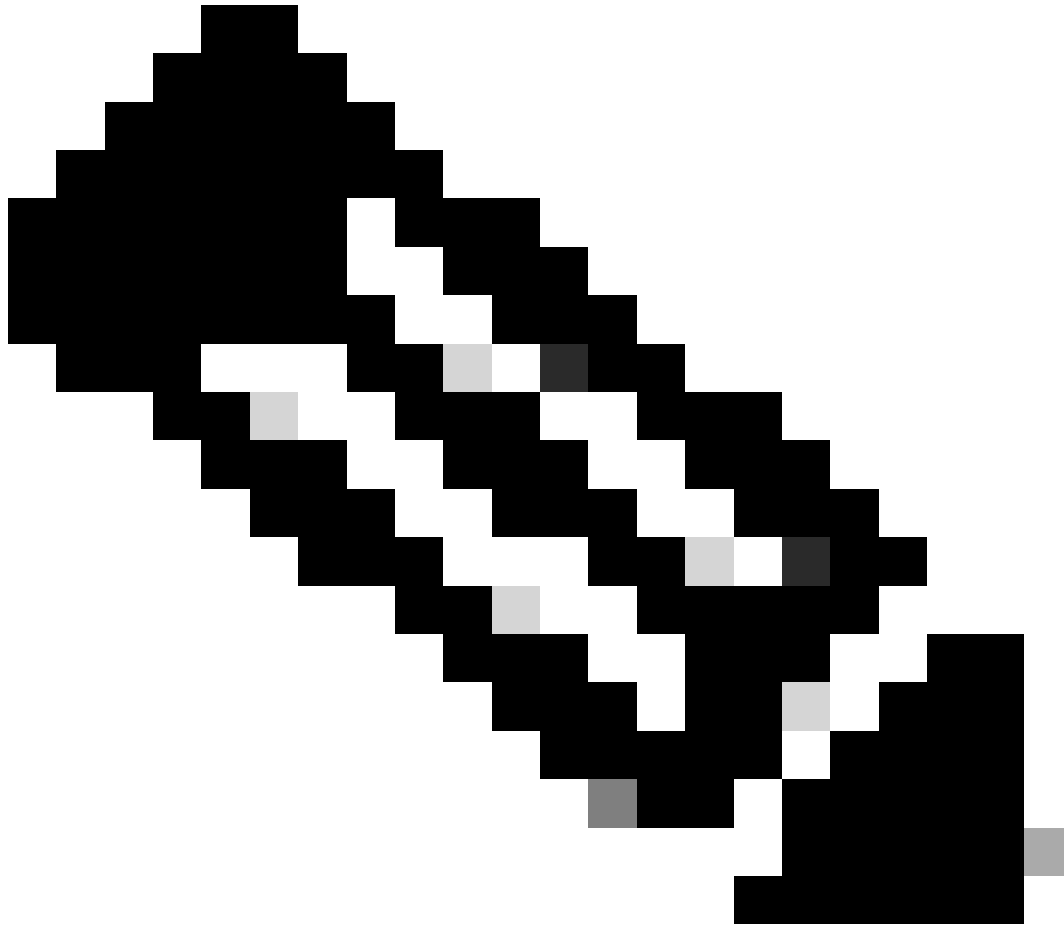
URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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: l'ID deriva dagli output API al passaggio 3 di "Get All System Certificates Of A Particular Node", ad esempio, 5b5b28e4-2a51-495c-8413-610190e1070b è "Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com".

Di seguito è riportato l'esempio degli output previsti.

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'}}
```

Otteni Elenco Di Tutti I Certificati Attendibili

L'API elenca tutti i certificati attendibili del cluster ISE.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: individuare l'URL utilizzato per recuperare i certificati attendibili.

The screenshot shows a list of API endpoints in the Cisco ISE API Explorer. 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, including `friendlyName`, `subject`, `issuedTo`, `issuedBy`, `validFrom`, `expirationDate`, and `status`. A note at the bottom states: "Note: ISE internal CA certificates will not be exported."

URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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:")
```

Di seguito è riportato l'esempio degli output previsti.(Omesso)

Return Code:

200

Expected Outputs:

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

Ottieni certificato di attendibilità per ID

Questa API consente di visualizzare i dettagli di un certificato di attendibilità in base a un determinato ID.

Passaggio 1: Informazioni obbligatorie per una chiamata API.

Metodo	OTTIENI
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-of-Certificate>
Credenziali	Usa credenziali dell'account API aperto
Intestazioni	Accetta: application/json Content-Type: applicazione/json

Passaggio 2: Individuare l'URL utilizzato per recuperare le informazioni sulla distribuzione.

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.		

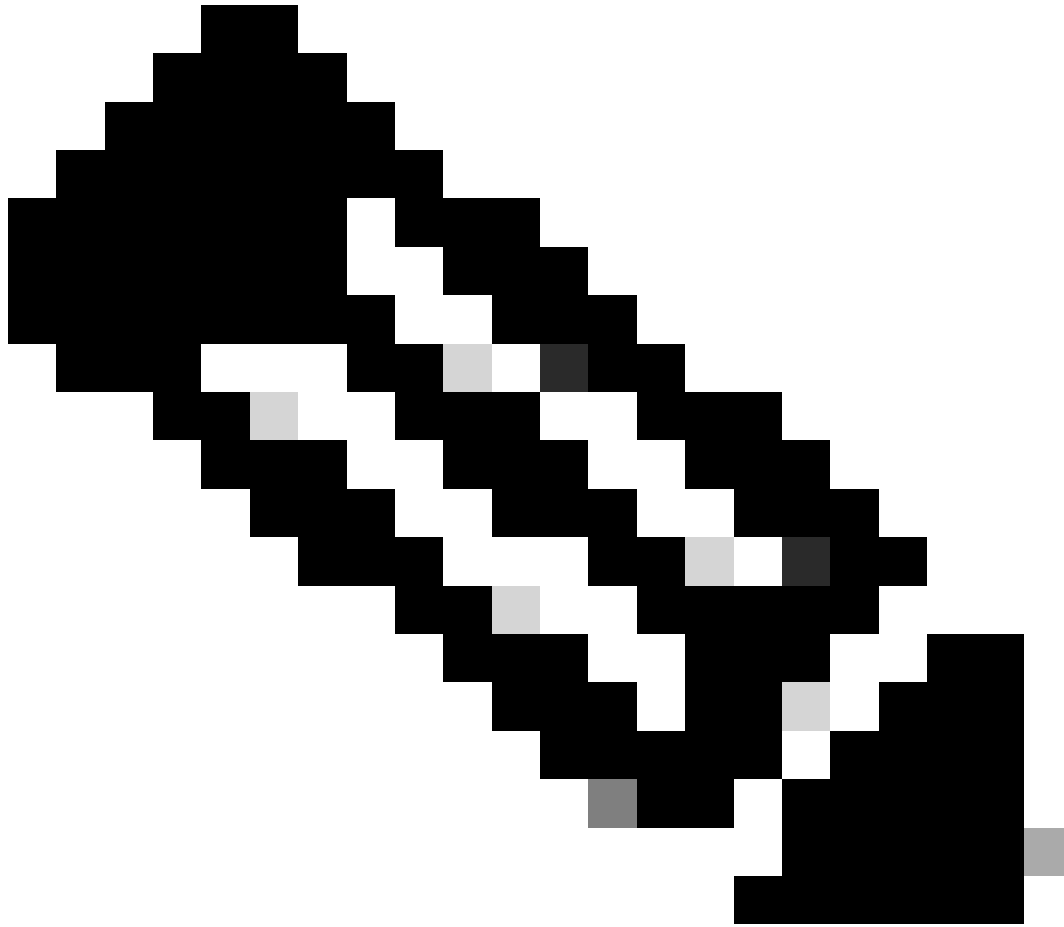
URI API

Passaggio 3: Ecco l'esempio del Codice Python. Copiare e incollare il contenuto. Sostituire l'indirizzo IP, il nome utente e la password ISE. Salva come file Python da eseguire.

Verificare la buona connettività tra ISE e il dispositivo su cui è in esecuzione il codice 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: l'ID deriva dagli output API al passaggio 3 di "Get List Of All Trusted Certificates", ad esempio, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 è "VeriSign Class 3 Public Primary Certification Authority".

Di seguito è riportato l'esempio degli output previsti.

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

Risoluzione dei problemi

Per risolvere i problemi relativi alle API aperte, impostare il livello di **log** per **apiservicecomponent** su **DEBUG** nella finestra di configurazione del **log di debug**.

Per abilitare il debug, selezionare **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > apiservice**.

The screenshot shows the 'Debug Level Configuration' page in the Identity Services Engine. The 'Operations / Troubleshoot' menu is active. The 'Debug Wizard' tab is selected. The table below lists various components and their log levels. The 'apiservice' component is highlighted with a red box, and its log level is set to 'DEBUG'.

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

Debug del servizio API

Per scaricare i log di debug, selezionare **Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs (Operazioni > Risoluzione dei problemi > Log di download > Nodo PAN ISE > Log di debug)**.

The screenshot shows the 'Download Logs' page in the Identity Services Engine. The 'Operations / Troubleshoot' menu is active. The 'Download Logs' tab is selected. The table below lists various debug log types and their sizes. The 'api-service (13) (208 KB)' log file is highlighted with a red box.

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

Scarica log di debug

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).