OpenAPI를 사용하여 ISE 3.3에서 ISE 인증서 정 보 검색

목차
<u>소개</u>
사전 요구 사항
<u>요구 사항</u>
사용되는 구성 요소
<u>78</u>
<u>네트워크 다이어그램</u>
<u>ISE의 컨피그레이션</u>
Python 예
<u>특정 노드의 모든 시스템 인증서 가져오기</u>
<u>ID로 특정 노드의 시스템 인증서 가져오기</u>
<u>신뢰할 수 있는 모든 인증서 목록 가져오기</u>
<u>ID로 트러스트 인증서 가져오기</u>
<u>문제 해결</u>

소개

이 문서에서는 openAPI를 사용하여 Cisco ISE(Identity Services Engine) 인증서를 관리하는 절차에 대해 설명합니다.

배경

엔터프라이즈 네트워크 보안 및 관리의 복잡성이 증가하는 상황에서 Cisco ISE 3.1은 인증서 라이 프사이클 관리를 간소화하는 OpenAPI 형식의 API를 도입하여 효율적이고 안전한 인증서 운영을 위한 표준화되고 자동화된 인터페이스를 제공함으로써 관리자가 강력한 보안 방식을 적용하고 네 트워크 컴플라이언스를 유지할 수 있도록 지원합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

- ISE 3.3
- 파이썬 3.10.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



ISE의 컨피그레이션

1단계: Open API 관리자 계정 추가

API 관리자를 추가하려면 Administration(관리) > System(시스템) > Admin Access(관리자 액세스) > Administrators(관리자) > Admin Users(관리자 사용자) > Add(추가)로 이동합니다.

≡	distantion Identity Services	Engine			Administra	ntion / System			🔺 License Warning	۵ ۵	0	9 X
Щ	Bookmarks	Deployment Licensing	Certifica	tes Logging	Maintenance	Upgrade Hea	Ith Checks	Backup & Restore	Admin Access Settings			
	Dashboard	Authentication		dministrat	~ * ~							
10	Context Visibility	Authorization	> A	ammstrat	UIS					Selected 0	Total 2	a .a
*	Operations	Administrators	~ 0	ldit + Add	🛞 Change Status	Delete Duplicat	te				All	- V
0	Policy	Admin Users Admin Groups	(Status	Name	Description	First Name	Last Name Email A	ddress Admin Groups			
20	Administration			🗌 🛛 Enabled	y admin	Default Admin Us	er		Super Admin			
-file	Work Centers	Settings	>	Enabled	4 ApiAdmin				ERS Admin			
?	Interactive Help											

API 관리자

2단계: ISE에서 Open API 활성화

Open API는 ISE에서 기본적으로 비활성화되어 있습니다. 활성화하려면 Administration(관리) > System(시스템) > Settings(설정) > API Settings(API 설정) > API Service Settings(API 서비스 설정)로 이동합니다. Open API 옵션을 전환합니다. 저장을 클릭합니다.



OpenAPI 활성화

3단계: ISE 개방형 API 탐색

administration(관리) > System(시스템) > Settings(설정) > API Settings(API 설정) > Overview(개요))로 이동합니다. API 방문 열기 링크를 클릭합니다.

≡	dentity Services I	Engine				Administra	tion / Syster	•		-	License Warning	Q	۵ ۵	A A
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
51	Dashboard	Client Provision	ing											
망	Context Visibility	FIPS Mode Security Setting	5	API S	Settings									
×	Operations	Alarm Settings		Overview	API Service	e Settings API G	ateway Settings							
0	Policy	General MDM /	UEM Settings	API Serv	ices Overvie	w								
80	Administration	Posture		> You can m	anage Cisco ISE	nodes through two	sets of API forma	ets-External Restful Ser	rvices (ERS) and OpenAPI.					
đ.	Work Centers	Profiling		The ERS a Currently,	nd OpenAPI sen ERS APIs also o	vices are HTTPS-only perate over port 906	y REST APIs that 0. However, port	operate over port 443. 9060 might not be sup	ported for ERS APIs in later	r				
		Protocols		> Gisco ISE r Both the A	releases. We red PI services are o	commend that you or disabled by default. E	ily use port 443 mable the API se	for ERS APIs. Invices by clicking the c	corresponding toggle button	5				
?	Interactive Help	Endpoint Script	ts	> To use eith	Service Settings er API service,	i tab. you must have the Ef	S-Admin or ERS	Operator user group	assignment.					
		Proxy SMTP Server SMS Gateway		For more in https://10. For openap ERS_V1	nformation on IS 106.33.92:4424 pi documention	E ERS API, please vi t0/ers/sdk for ERS, click below:	sit:							
	I	System Time API Settings		For more in https://10.	formation on IS 106.33.92:4424	E Open APL please (t0/api/swagger-ui/in	dex_html							

OpenAPI 방문

Python 예

특정 노드의 모든 시스템 인증서 가져오기

API는 특정 ISE 노드의 모든 인증서를 나열합니다.

1단계: API 호출에 필요한 정보입니다.

방법	가져오기
URL	https:// <ise-pan-ip>/api/v1/certs/system-</ise-pan-ip>

	certificate/ <ise-node-hostname></ise-node-hostname>
자격 증명	Open API 계정 자격 증명 사용
헤더	수락: application/json Content-Type: application/json

2단계: 특정 ISE 노드의 인증서를 검색하는 데 사용되는 URL을 찾습니다.

😝 Swa	gger.	Select a definition Certificates	×
Cisc https://10.106	o ISE API - Certificates (III) (III)		
Servers https://10	106.33.92:44240 - Inferred Urt 💙		
certs-	api-controller the certs API		~
Certif	cates		^
GET	/api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN		~ ≜
POST	/api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)		 ✓ ≜
GET	/api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given	n ID	 ✓ ≜
DELETE	/api/vl/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given by the signing request of a given by the signing request of the signing re	ven ID	 ✓ ≜
GET	/api/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID	and hostname	 ✓ ≜
POST	/api/vl/certs/certificate-signing-request/intermediate-ca Generate an Intermediate CA CSR (certificat	te signing request)	✓ ≜
POST	/api/vl/certs/ise-root-ca/regenerate Regenerate entire internal CA certificate chain including root CA on the prima	ary PAN and subordinate CAs on the PSNs (Applicable only for internal CA se	wice) 🗸 🗎
POST	/api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cloco ISE Messaging Service		 ✓ ≜
POST	/api/vl/certs/signed-certificate/bind Bind CA Signed CertBicate		✓ ∅
GET	/api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node		∧ ≜
This API	supports filtering, sorting and pagination.		

API URI

3단계: Python Code의 예를 소개합니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름, 비밀 번호를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행하는 디바이스 간의 올바른 연결을 확인합니다.

<#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())
```

다음은 예상 출력의 예입니다.

Return Code:

200

Expected Outputs:

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

ID로 특정 노드의 시스템 인증서 가져오기

이 API는 제공된 호스트 이름 및 ID를 기반으로 특정 노드의 시스템 인증서에 대한 세부 정보를 제 공합니다.

1단계: API 호출에 필요한 정보입니다.

방법	가져오기
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname>/<id-of- Certificate></id-of- </ise-node-hostname></ise-pan-ip>
자격 증명	Open API 계정 자격 증명 사용
헤더	수락: application/json Content-Type: application/json

2단계: 지정된 호스트 이름 및 ID를 기반으로 특정 노드의 인증서를 검색하는 데 사용되는 URL을 찾습니다.

	Cisco ISE API - Certificates (ISB) CASS https://d.100.33.02.402400apiv/30ap-doct/tgroup-Certificates		
	Servers https://10.108.33.92:44240 - Inferred Uri v		
	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)	 ✓ ≜ 	
	OET /api/vl/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/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	∨ ≜	
	POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	 ✓ ≜ 	
	POST /api/vl/certs/ise-root-ca/regenerate Regenerate enline 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/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	 ✓ ≜ 	
	POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	∨ ≜	
	OET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	∨ ≜	
	OET /api/vl/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

3단계: Python Code의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름, 비밀번호를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행하는 디바이스 간의 올바른 연결을 확인합니다.

<#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-8413-610190e2

" 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:")



참고: ID는 "특정 노드의 모든 시스템 인증서 가져오기"의 3단계에서 API 출력에서 가져온 것입니다. 예를 들어, 5b5b28e4-2a51-495c-8413-610190e1070b는 "Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com"입니다.

다음은 예상 출력의 예입니다.

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

신뢰할 수 있는 모든 인증서 목록 가져오기

API는 ISE 클러스터의 모든 신뢰할 수 있는 인증서를 나열합니다.

1단계: API 호출에 필요한 정보입니다.

방법	가져오기
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate</ise-pan-ip>
자격 증명	Open API 계정 자격 증명 사용
헤더	수락: application/json Content-Type: application/json

2단계: 신뢰할 수 있는 인증서를 검색하는 데 사용되는 URL을 찾습니다.

			2
POST	/api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (centricate 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)	\sim	۵
POST	/api/vi/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	\sim	ŵ
POST	/api/vi/certs/signed-certificate/bind Bind CASigned Certificate	\sim	ŵ
GET	/api/vi/certs/system-certificate/{hostName} Get all system certificates of a particular node	\sim	ŵ
GET	/api/vl/certs/system-certificate/{hostName}/{id} Get system certilicate of a particular node by ID	\sim	ŵ
PUT	/api/vi/certs/system-certificate/{hostName}/{id} Update data for existing system certificate	\sim	ŵ
DELETE	/api/vi/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname	\sim	ŵ
POST	/api/vi/certs/system-certificate/export Export a system certificate with a given a certificate ID	\sim	ŵ
POST	/api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE	\sim	ŵ
POST	/api/vi/certs/system-certificate/import Import system certificate in Cisco ISE	\sim	ŵ
GET	/api/v1/certs/trusted-certificate Get list of all busited certificates	^	۵
This API su	ports Filtering, Sorting and Pagination.		
Filtering and	Sorting are supported for the following attributes:		
 friendl 	Name		
 subject issued 			
 validFi 	om Spechted Date Format: yyyy-MM-4d HH mm ss		
• expira	Supported Operators: EG, NEO, GT and LT enclude		
0	Supported Date Format; yyyyAMA dd Hit mms s Supported Optamster: EQ. NEQ. CJ and LT		
• status 0	Alloved values: enabled, disabled Supported Operators: EQ, NEQ		
Note: ISE inte	mai CA certificates will not be exported.		

API URI

3단계: Python Code의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름, 비밀번호를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행하는 디바이스 간의 올바른 연결을 확인합니다.

<#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:")

다음은 예상 출력의 예입니다. (생략)

Return Code:

200

Expected Outputs:

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

ID로 트러스트 인증서 가져오기

이 API는 지정된 ID를 기반으로 신뢰 인증서의 세부 정보를 표시할 수 있습니다.

1단계: API 호출에 필요한 정보입니다.

방법	가져오기
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
자격 증명	Open API 계정 자격 증명 사용
헤더	수락: application/json Content-Type: application/json

2단계: 구축 정보를 검색하는 데 사용되는 URL을 찾습니다.

Cisco ISE API - Certificates C C C C C C C C C C C C C C C C C C C		
Servers https://10.106.33.92:44240 - Inferred Uri		
certs-api-controller the certs API	~	
Certificates	^	
CET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	∨ ≜	
POST /api/v1/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	∨ ≜	
CET /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	∨ ≜	
CET /api/v1/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	∨ ≜	1
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 enline 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/vl/certs/signed-certificate/bind Bind CA Signed Certificate	∨ ≜	
CET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	∨ ≜	
GET /api/vl/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

3단계: Python Code의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름, 비밀번호를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행하는 디바이스 간의 올바른 연결을 확인합니다.

<#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:")



참고: ID는 "모든 신뢰할 수 있는 인증서 목록 가져오기"의 3단계에서 API 출력에서 가져온 것입니다. 예를 들어 147d97cc-6ce9-43d7-9928-8cd0fa83e140은 "VeriSign Class 3 Public Primary Certification Authority"입니다.

다음은 예상 출력의 예입니다.

Return Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Content of the second seco

Open API와 관련된 문제를 해결하려면 Debug Log Configuration(디버그 로그 컨피그레이션) 창에서 Log Levelfor theapiservicecomponent를 DEBUG로 설정합니다.

디버그를 활성화하려면 Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug Log Configuration(디버그 로그 컨피그레이션) > ISE Node(ISE 노드) > apisservice(어플라이언스)로 이동합니다.

≡	dentity Services	Engine	Operations / Troubleshoot					🔺 License Warning	Q	۵	0	Q	۹
н	Bookmarks	Diagnostic Tools Download L	ogs Det	oug Wizard									
ः ।उ %	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List	ISE-BOL-CEMEO1-PAN.S	meld.com							£	3
0	Policy		0 Edit	Seset to Default	Log Filter Enable	Log Filter Disable					All	~ 7	7
80	Administration			Component Name	∧ Log Level	Description	Log file Name	Log Filter					
-fil	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled				í	í .
			0	Active Directory	WARN	Active Directory client internal messages	ad_agent.log						
?	Interactive Help		0	admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled					
			0	admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled					
			0	admin-license	INFO	License admin messages	ise-psc.log	Disabled					
			0	ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled					
			0	anc	INFO	Adaptive Network Control (ANC) debug	ise-psc.log	Disabled					
			0	api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled					
			•	apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled					
			0	bootstrap-wizard	INFO	Bootstrap wizard messages Save I Can	cel -psc.log	Disabled					
			0	ca-service	INFO	CA Service messages	caservice.log	Disabled					

API 서비스 디버그

디버그 로그를 다운로드하려면 Operations(운영) > Troubleshoot(문제 해결) > Download Logs(로그 다운로드) > ISE PAN Node(ISE PAN 노드) > Debug Logs(디버그 로그)로 이동합니다.

≡	diale Identity Services	Engine	9			🔺 License Warning	Q	۵	0	Q Q			
н	Bookmarks	Diagn	iostic Tools	Download Logs	Debug Wiza	ard							
10	Dashboard		ISE-BO	SL-CFME01-PAN									
1d	Context Visibility		ISE-BO	G-CEME01-PSN	Delete	2 ³ Expand All ≤>Colla							
*	Operations		ISE-DL	C-CFME02-PSN	Debug	Log Type	Log File	Description	Size				
0	Policy		ISE-RT	P-CFME01-PAN	✓ Applicatio					- i -			
8.	Administration		ISE-RT	P-CFME02-MNT	> ad_	_agent (1) (100 KB)							
đ	Work Centers		4		> ai-a	> al-analytics (11) (52 KB) > apl-gateway (16) (124 KB)							
?	Interactive Help				→ api	-service (13) (208 KB)	api-service (all logs)	API Service debug messages	208 KB				
							api-service.log		12 KB				
							api-service.log.2024-03-24-1		4.0 KB				
							api-service.log.2024-04-07-1		4.0 KB				
			1		-								

디버그 로그 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.