# OpenAPI를 사용하여 ISE 3.3에서 ISE 정책 정보 검색

목차
<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
사용되는 구성 요소
<u>배경 정보</u>
<u>구성</u>
네트워크 다이어그램
<u>ISE의 컨피그레이션</u>
<u>Python 예</u>
<u>장치 관리자 - 정책 집합 목록</u>
<u>디바이스 관리 - 인증 규칙 가져오기</u>
<u>장치 관리자 - 권한 부여 규칙 가져오기</u>
<u>네트워크 액세스 - 정책 집합 목록</u>
<u>네트워크 액세스 - 인증 규칙 가져오기</u>
<u>네트워크 액세스 - 권한 부여 규칙 가져오기</u>
문제 해결

# 소개

이 문서에서는 OpenAPI를 사용하여 관리하는 절차에 대해 설명합니다 Cisco ISE(Identity Services Engine) 정책.

# 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.

# 배경 정보

Cisco ISE 3.1 이상에서는 OpenAPI 형식으로 새로운 API를 사용할 수 있습니다. 관리 정책은 상호 운용성을 높이고, 자동화 효율성을 개선하며, 보안을 강화하고, 혁신을 촉진하고, 비용을 절감하여 네트워크 보안 및 관리를 최적화합니다. 이 정책을 통해 ISE는 다른 시스템과 원활하게 통합되고, 자동화된 구성 및 관리를 달성하고, 세분화된 액세스 제어를 제공하고, 서드파티 혁신을 장려하고, 관리 프로세스를 간소화하여 유지 관리 비용을 줄이고 전반적인 ROI를 높일 수 있습니다.

구성

네트워크 다이어그램



ISE의 컨피그레이션

1단계. OpenAPI 관리자 계정을 추가합니다.

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

≡	dentity Services E	Ingine				Administra	tion / System			🔺 Uce	nse Warning	Q	۵ ۵	٥	
Ц	Bookmarks	Deployment Licens	ing C	ertificates	Logging	Maintenance	Upgrade Hea	th Checks	Backup & Restore	Admin Access	Settings				
51	Dashboard	Authentication		Admi	nietrot	or0									
망	Context Visibility	Authorization	>	Aum	mstrat	015						Sele	ted 0 Total 2	a	ø
×	Operations	Administrators	Ŷ	0 Edit	+ Add	Change Status	Delete Duplicat							a V	v.
0	Policy	Admin Users Admin Groups			Status	Name	Description	First Name	Last Name Email A	ddress Admin Group	ps				
20	Administration			0	Enabled	admin 😛	Default Admin Use	er.		Super Admir	n				
đ.	Work Centers	Settings	>		Enabled	a ApiAdmin				ERS Admin					
	Internative Vale														

API 관리자

2단계. ISE에서 OpenAPI를 활성화합니다.

Open API는 ISE에서 기본적으로 비활성화되어 있습니다. 활성화하려면 Administration(관리) > System(시스템) > Settings(설정) > API Settings(API 설정) > API Service Settings(API 서비스 설정

# ). OpenAPI 옵션을 전환합니다. 클릭 저장.

$\equiv$ $\frac{\mathrm{death}}{\mathrm{casce}}$ identity Services E	ngine	Administration / System	🔺 License Warning 🛛 🖓 🞯 🗘   🎗
I Bookmarks	Deployment Licensing C	rtificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
Image: Context Visibility       Context Visibility       Operations       Policy       Administration       Work Centers       Interactive Help	Client Provisioning FIPS Mode Security Settings Alarm Settings General MDM / UEM Settings Profiling Profocols > Endpoint Scripts > Proxy SMTP Server SMS Gateway	API Settings         Overview       API Service Settings         API Service Settings for Primary Administration Node         ERS (Read/Write)         Open API (Read/Write)         API Service Setting for All Other Nodes         ERS (Read)         Open API (Read)	
	API Settings Data Connect Network Success Diagnostics DHCP & DNS Services	<ul> <li>CSRF Check ( only for ERS Settings )</li> <li>Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)</li> <li>Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)</li> </ul>	
	Max Sessions Light Data Distribution Endpoint Replication		Reset Save

OpenAPI 활성화

# 3단계. ISE OpenAPI를 탐색합니다.

로 이동합니다 관리 > 시스템 > 설정 > API 설정 > 개요. 링크를 방문하려면 OpenAPI를 클릭합니다

	dentity Services I	Engine				Administrat	tion / Systen	n				Q	۵	0	<b>д</b>   <b>д</b>
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
53	Dashboard	Client Provisioni	ing	1010											
15	Context Visibility	FIPS Mode		APIS	settings										
×	Operations	Alarm Settings	-	Overview	API Service	e Settings API G	ateway Settings								
0	Policy	General MDM / I	UEM Settings	API Ser	vices Overvie	w									
20	Administration	Posture		> You can m	You can manage Cisco ISE nodes through two sets of API formats-External Restful Services (ERS) and OpenAPI.										
đ	Work Centers	Profiling		The ERS a Currently,	The ERS and OpenAPI services are HTTPS-only REST APIs that operate over open deriver to the approximate. Currently ERS APIs also approximate over pert 900-1000 million to the supported for ERS APIs in later										
		Protocols		> Cisco ISE Both the /	releases. We ree API services are	commend that you on disabled by default. E	ly use port 443 nable the API se	for ERS APIs. rvices by clicking the c	corresponding toggle buttor	15					
?	Interactive Help	Endpoint Script	5	> To use eit	Service Settings her API service,	i tab. you must have the ER	tS-Admin or ERS	Operator user group a	assignment.						
		Proxy		For more https://10	information on IS	E ERS API, please vis IO/ers/sdk	it:								
		SMTP Server		For opena	pi documention	for ERS, click below:									
		SMS Gateway		ERS_V1											
		System Time		For more	information on IS	F Onen API, niease v	isit-								
		API Settings		nttps://10	106.33.92:4424	to/api/swagger-ui/ind	Jex.html								

OpenAPI 방문

Python 예

장치 관리자 - 정책 집합 목록

이 API는 디바이스 관리 정책 집합 정보를 검색합니다.

1단계. API 호출에 필요한 정보입니다.

바	버
O	H

URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set</ise-pan-ip>
자격 증명	OpenAPI 계정 자격 증명을 사용합니다.
헤더	수락 : application/json Content-Type : application/json

2단계. 디바이스 관리 정책 집합 정보를 검색하는 데 사용되는 URL을 찾습니다.

H Swagger,	Select a definition Policy ~	
Cisco ISE API - Policy (500) (755) https://10.103.31.02.442404pg/v3api-docs?group=Policy		
Servers https://10.106.33.92-44240 - Inferred Url v	Authorize 🔒	
device-admin-api-controller the device-admin API	*	
network-access-api-controller the network-access API	~	
Device Administration - Command Sets	~	
Device Administration - Conditions	~	
Device Administration - Dictionary Attributes List	~	
Device Administration - Identity Stores	~	
Device Administration - Network Conditions	~	
Device Administration - Policy Sets	^	
GET /api/vi/policy/device-admin/policy-set Device Admin - List of policy sets.	<u>^</u> ≜	
Device Admin - List of policy sets.		

API URI

3단계. Python 코드의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름 및 비밀번호 를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행 중인 디바이스 간의 양호한 연결을 보장합니다.

#### <#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable\_warnings()

if \_\_\_\_\_name\_\_\_ == "\_\_\_\_main\_\_\_":

url = "

https://10.106.33.92/api/v1/policy/device-admin/policy-set

..

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())
```

```
이는 예상 출력의 예입니다.
```

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': True, 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'name': 'Default', 'describert': 'Default', 'describert': 'Default': 'Default': True, 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'name': 'Default', 'describert': 'Default': True, 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'name': 'Default': 'Default': True, 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'name': 'Default': 'Defau

```
D장치 관리자 - 인증 규칙 가져오기
```

이 API는 특정 정책 집합의 인증 규칙을 검색합니다.

### 1단계. API 호출에 필요한 정보입니다.

방법	가져오기
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set&gt;/authentication</id-of-policy- </ise-pan-ip>
자격 증명	OpenAPI 계정 자격 증명을 사용합니다.
헤더	수락 : application/json Content-Type : application/json

2단계. 인증 규칙 정보를 검색하는 데 사용되는 URL을 찾습니다.

		Select a definition Policy	*	
	Cisco ISE API - Policy (100 0.5) https://to.03.3192-44240mpiv/Japp-docs/spreage-Policy			
	Servers https://10.106.33.92:44240 - Inferred Uri v		Authorize 🔒	
	device-admin-api-controller the device-admin API		~	
	network-access-api-controller the network-access API		~	
	Device Administration - Command Sets		~	
	Device Administration - Conditions		~	
	Device Administration - Dictionary Attributes List		~	
	Device Administration - Identity Stores		~	
	Device Administration - Network Conditions		~	
	Device Administration - Policy Sets		~	
	Device Administration - Authorization Global Exception Rules		~	
	Device Administration - Authentication Rules		^	
	GET /api/vl/policy/device-admin/policy-set/{policyId}/authentication Device Admin - Get authentica	tion rules.	^ ≜	
	Device Admin - Get authentication rules.			

API URI

3단계. Python 코드의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름 및 비밀번호 를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행 중인 디바이스 간의 양호한 연결을 보장합니다.

#### <#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable\_warnings()

```
if _____name___ == "____main___":
```

url = "

https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authenti

```
"
```

```
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:")
```



참고: ID는 Device Admin(디바이스 관리) - List Of Policy Sets(정책 집합 목록)의 3단계에 서 API 출력에서 가져옵니다. 예를 들어 41ed8579-429b-42a8-879e-61861cb82bbf는 TACACS 기본 정책 집합입니다.

이는 예상 출력의 예입니다.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '73461597-0133-45ce-b4cb-6511ce56f262', 'name': 'Default': 'True, 'name': 'Default': 'Default': 'True, 'name': 'Default': 'Default': 'Default': 'Default': 'Default': 'Default': 'Default': 'Default': 'True, 'name': 'Default': 'Default'

장치 관리자 - 권한 부여 규칙 가져오기

이 API는 특정 정책 세트의 권한 부여 규칙을 검색합니다.

## 1단계. API 호출에 필요한 정보입니다.

방법	가져오기
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set&gt;/authorization</id-of-policy- </ise-pan-ip>
자격 증명	OpenAPI 계정 자격 증명을 사용합니다.
헤더	수락 : application/json Content-Type : application/json

# 2단계. 권한 부여 규칙 정보를 검색하는 데 사용되는 URL을 찾습니다.

Cisco ISE API - Policy (ISE) (ASS) https://10.108.33.92.4424bhpe/Valapi-docs/Tgroupi-Policy	
Servers https://10.106.33.92:44240 - Inferred Uri v	Authorize
device-admin-api-controller the device-admin API	~
network-access-api-controller the network-access API	~
Device Administration - Command Sets	~
Device Administration - Conditions	~
Device Administration - Dictionary Attributes List	~
Device Administration - Identity Stores	~
Device Administration - Network Conditions	~
Device Administration - Policy Sets	~
Device Administration - Authorization Global Exception Rules	~
Device Administration - Authentication Rules	~
Device Administration - Authorization Rules	^
GET /api/vl/policy/device-admin/policy-set/{policyId}/authorization Device Admin - Get authorization rules.	▲
Device Admin - Get authorization rules.	

API URI

3단계. Python 코드의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름 및 비밀번호 를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행 중인 디바이스 간의 양호한 연결을 보장합니다.

#### <#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable\_warnings() if \_\_name\_\_ == "\_\_main\_\_": url = "

https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authorized and the set of the set of

" 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 Device Admin(디바이스 관리) - List Of Policy Sets(정책 집합 목록)의 3단계에 서 API 출력에서 가져옵니다. 예를 들어 41ed8579-429b-42a8-879e-61861cb82bbf는 TACACS 기본 정책 집합입니다.

이는 예상 출력의 예입니다.

Return Code: 200 Expected Outputs:

{'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '39d9f546-e58c-4f79-9856-c0a244b8a2ae', 'name': 'Default', 'hitCounts': 0, 'rank': 0, 'state': 'enable

### 네트워크 액세스 - 정책 집합 목록

이 API는 ISE 구축의 네트워크 액세스 정책 집합을 검색합니다.

#### 1단계. API 호출에 필요한 정보입니다.

방법	가져오기				
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set</ise-pan-ip>				
자격 증명	OpenAPI 계정 자격 증명을 사용합니다.				
헤더	수락 : application/json Content-Type : application/json				

### 2단계. 특정 ISE 노드 정보를 검색하는 데 사용되는 URL을 찾습니다.

Network Access - Policy Sets							
GET /api/v1/policy/network-access/policy-set Network Access - List of policy sets.	^ ≜						
Get all network access policy sets.							

API URI

3단계. Python 코드의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름 및 비밀번호 를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행 중인 디바이스 간의 양호한 연결을 보장합니다.

#### <#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable\_warnings()

if \_\_\_\_\_name\_\_\_ == "\_\_\_\_main\_\_\_":

url = "

https://10.106.33.92/api/v1/policy/network-access/policy-set

"

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())
```

이는 예상 출력의 예입니다.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': False, 'id': 'ba71a417-4a48-4411-8bc3-d5df9b115769', 'name': 'BGL\_CFME0

네트워크 액세스 - 인증 규칙 가져오기

### 이 API는 특정 정책 집합의 인증 규칙을 검색합니다.

1단계. API 호출에 필요한 정보입니다.

방법	가져오기
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set/<id-of-policy- Set&gt;/authentication</id-of-policy- </ise-pan-ip>
자격 증명	OpenAPI 계정 자격 증명을 사용합니다.
헤더	수락 : application/json Content-Type : application/json

2단계. 인증 규칙 정보를 검색하는 데 사용되는 URL을 찾습니다.

Network Access - Authentication Rules									
GET	/api/v1/policy/network-access/policy-set/{policyId}/authentication Network Access - Get authentication rules.	^ ≜							
Network	Access - Get authentication rules.								

API URI

3단계. Python 코드의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름 및 비밀번호 를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행 중인 디바이스 간의 양호한 연결을 보장합니다.

#### <#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable\_warnings()

```
if __name__ == "__main__":
    url = "
https://10.106.33.92/api/v1/policy/network-access/policy-set/ba71a417-4a48-4411-8bc3-d5df9b115769/auther
"
    headers = {
    "Accept": "application/json", "Content-Type": "application/json"
    basicAuth = HTTPBasicAuth(
    "ApiAdmin", "Admin123"
)
    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
```

```
response = requests.get(url=url, autn=basicAutn, neaders=neaders, verity=F
print("Return Code:")
print(response.status_code)
print("Expected Outputs:")
print(response.json())
```



참고: ID는 Network Access - List Of Policy Sets(네트워크 액세스 - 정책 집합 목록) 3단계 의 API 출력에서 가져옵니다. 예를 들어 ba71a417-4a48-4411-8bc3-d5df9b115769 는 입니다BGL\_CFME02-FMC.

이는 예상 출력의 예입니다.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default':

네트워크 액세스 - 권한 부여 규칙 가져오기

이 API는 특정 정책 세트의 권한 부여 규칙을 검색합니다.

1단계. API 호출에 필요한 정보입니다.

방법	가져오기

URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set/<id-of-policy- Set&gt;/authorization</id-of-policy- </ise-pan-ip>
자격 증명	OpenAPI 계정 자격 증명을 사용합니다.
헤더	수락 : application/json Content-Type : application/json

## 2단계. 권한 부여 규칙 정보를 검색하는 데 사용되는 URL을 찾습니다.

Network Access - Authorization Rules	^
GET /api/v1/policy/network-access/policy-set/{policyId}/authorization Network Access - Get authorization rules.	^ ≜
Network Access - Get authorization rules.	

API URI

3단계. Python 코드의 예입니다. 내용을 복사하여 붙여넣습니다. ISE IP, 사용자 이름 및 비밀번호 를 교체합니다. 실행할 python 파일로 저장합니다.

ISE와 python 코드 예제를 실행 중인 디바이스 간의 양호한 연결을 보장합니다.

#### <#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable\_warnings()

if \_\_\_\_\_name\_\_\_ == "\_\_\_main\_\_\_":

url = "

"

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())
```



참고: ID는 Network Access(네트워크 액세스) - List Of Policy Sets(정책 집합 목록)의 3단 계에서 API 출력에서 가져옵니다. 예를 들어 ba71a417-4a48-4411-8bc3-d5df9b115769은 BGL\_CFME02-FMC입니다.

이는 예상 출력의 예입니다.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': False, 'id': 'bc67a4e5-9000-4645-9d75-7c2403ca22ac', 'name': 'FMC A

# 문제 해결

OpenAPI와 관련된 문제를 해결하려면 Debug Log Configuration(디버그 로그 컨피그레이션) 창에 서 Theapiservicecomponent의 Log Level(로그 레벨)을 DEBUG로 설정합니다.

디버그를 활성화하려면 Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법

사) > Debug Log Configuration(디버그 로그 컨피그레이션) > ISE Node(ISE 노드) > apisservice(어 플라이언스)로 이동합니다.

≡	diale Identity Services	Engine			Of	perati	ons / Trout	pleshoot		License Warning	Q	۵	0	٥	A
н	Bookmarks	Diagnostic Tools	Download Logs	Deb	oug Wizard										
ा ह	Dashboard Context Visibility Operations	Debug Profile Configuratio	n	Node List	ISE-BOL-CEMEDI-PANU	onfig	guration	ı							8
0	Policy			/ Edit	← Reset to Default	Log F	ilter Enable	Log Filter Disable					AI		7
8.	Administration				Component Name	~ 1	Log Level	Description	Log file Name	Log Filter					
nii.	Work Centers			0	accessfilter		INFO	RBAC resource access filter	ise-psc.log	Disabled					
				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	Al 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					
				0	apiservice	C	DEBUG	ISE API Service logs	api-service.log	Disabled					
				0	bootstrap-wizard		INFO	Bootstrap wizard messages Save I Can	-psc.log	Disabled					
				0	ca-service		INFO	CA Service messages	caservice.log	Disabled					

API 서비스 디버그

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

≡	≡ dentity Services Engine					Operat	ions / Trou	bleshoot		🔺 License Warning	Q	۵	0	Q	۹
Ц	Bookmarks	Diagnost	tic Tools	Download Logs	Debug Wiza	ird									
- 22	Dashboard		ISE-BGI	L-CFME01-PAN	-		-								
명	Context Visibility		ISE-BGI	L-CFME02-MNT	Colete	2 <sup>8</sup> Expand All	<>Collapse A								
20	Operations		SE-DLC	C-CFME01-PSN	Debug	Log Type		Log File	Description	Size					
~	operations		ISE-DLC	C-CFME02-PSN	N/ Application	a 1 aaa									
0	Policy		ISE-RTF	P-CFME01-PAN	- Approxim	ii collo									
8.	Administration		ISE-RTF	P-CFME02-MNT	_ba <	agent (1) (100 KB)									
			<.	•	> ai-a	analytics (11) (52 KB)									
- fili	Work Centers				> api	-gateway (16) (124 KB)	)								
					$\checkmark$ api	-service (13) (208 KB)	].		-						
?	Interactive Help							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					
					0										

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.