# OpenAPIを使用したISE 3.3でのISEポリシー情 報の取得

内容
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>ネットワーク図</u>
<u>ISEでの設定</u>
<u>Pythonの例</u>
<u>デバイス管理者 – ポリシーセットの一覧</u>
<u> デバイス管理者 – 認証ルールの取得</u>
<u> デバイス管理者 – 許可ルールの取得</u>
<u>ネットワークアクセス:ポリシーセットのリスト</u>
<u>ネットワークアクセス – 認証ルールの取得</u>
<u>ネットワークアクセス – 許可ルールの取得</u>
トラブルシュート

## はじめに

このドキュメントでは、OpenAPIを使用して Cisco Identity Services Engine(ISE) ポリシーに 該当するトラフィックを区別します。

## 前提条件

## 要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

- ISE 3.3
- Python 3.10.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

## 背景説明

Cisco ISE 3.1以降では、新しいAPIがOpenAPI形式で使用できます。管理ポリシーは、相互運用 性の強化、自動化の効率化、セキュリティの強化、イノベーションの促進、コストの削減によっ て、ネットワークのセキュリティと管理を最適化します。このポリシーにより、ISEは他のシス テムとシームレスに統合し、自動化された設定と管理を実現し、きめ細かなアクセス制御を提供 し、サードパーティの革新を奨励し、管理プロセスを簡素化することができます。その結果、メ ンテナンスコストが削減され、全体的な投資回収率が向上します。

## 設定

## ネットワーク図



#### ISEでの 設定

ステップ1: anOpenAPI adminアカウントを追加します。

API管理者を追加するには、Administration > System > Admin Access > Administrators > Admin Users > Addの順に移動します。

≡	dentity Services I	Engine			Administra	ition / System		🔺 License Warning	Q & Ø	0   A
н	Bookmarks	Deployment Licensing	Certificate	Logging	Maintenance	Upgrade Health Checks	Backup & Restore	Admin Access Settings		
	Dashboard	Authentication	٨d	ministrat	ore					
명	Context Visibility	Authorization	> Au	ministrat	015				Colored & Total S	a a
×	Operations	Administrators	× 2 Ed	+ Add	Change Status	Delete			Selected 0 Total 2	v ⊽
.0	Policy	Admin Users	0	Status	Name	Description First Nac	ne LastName EmailAdd	ress Admin Groups		
20	Administration	Admin Groups		Enabled	admin	Default Admin User		Super Admin		
di.	Work Centers	Settings	,	Enabled	a ApiAdmin			ERS Admin		
?	Interactive Help									

API管理者

ステップ2:ISEでOpenAPIを有効にします。

ISEでは、オープンAPIはデフォルトで無効になっています。有効にするには、に移動します。 [管理]>[システム]>[設定]>[API設定]>[APIサービス設定].OpenAPIオプションを切り替えます。ク リック 保存します。

$\equiv \frac{-\mathrm{diads}}{\mathrm{cases}}$ Identity Services I	Engine	Administration / System	🔺 License Warning 🛛 🖓 😗 🗘   🎗
Bookmarks	Deployment Licensing	ertificates Logging Maintenance Upgrade Health Checks Backup & Ri	estore Admin Access Settings
Dashboard Context Visibility Coperations Policy Administration Work Centers Interactive Help Interactive Help	Client Provisioning FIPS Mode Security Settings Alarm Settings General MDM / UEM Settings Posture > Profiling Protocols > Endpoint Scripts > Proxy. SMTD Server SMS Gateware	API Settings Overview API Service Settings API Gateway Settings ~ API Service Settings for Primary Administration Node ERS (Read/Write) ~ API Service Setting for All Other Nodes ERS (Read) Copen API (Read)	
	System Time API Settings Data Connect Network Success Diagnostics DHCP & DNS Services Max Sessions Light Data Diarribution Endpoint Replication	<ul> <li>CSRF Check ( only for ERS Settings )</li> <li>Cable 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>	Reset Save

OpenAPIの有効化

ステップ3:ISE OpenAPIを確認します。

移動先: [管理]>[システム]>[設定]>[API設定]>[概要].OpenAPIをクリックしてリンクにアクセスします。

≡	dentity Services I	Engine	Administration / System	🔺 License Warning	Q	۵	0	0   A
н	Bookmarks	Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admir	in Access Settings				
- 55	Dashboard	Client Provisioning						
뱅	Context Visibility	FIPS Mode Security Settings	API Settings					
*	Operations	Alarm Settings	Overview API Service Settings API Gateway Settings					
-0	Policy	General MDM / UEM Settings	API Services Overview					
8.	Administration	Posture	You can manage Cisco ISE nodes through two sets of API formats-External Restful Services (ERS) and OpenAPI. Starting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format.					
đ	Work Centers	Profiling	The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443. Currently, ERS APIs also operate over port 9060. However, port 9060 might not be supported for ERS APIs in later					
		Protocols	Cisco ISE releases. We recommend that you only use port 443 for ERS APIs. Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API Service Service the					
?	Interactive Help	Endpoint Scripts	To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.					
		Proxy SMTP Server SMS Gateway	For more information on ISE ERS API, please visit: https://10.106.33.82244240/ers/sdk For openapi documention for ERS, click below: ERS_V1					
		System Time	For more information on ISE Onen API, please visit:					
		API Settings Data Connect	mtps://10.109.33.92/94.240/apt/swagger-ut/mox.nom E83.8%					

OpenAPIにアクセス

## Pythonの例

デバイス管理者 – ポリシーセットの一覧

このAPIは、デバイス管理ポリシーセット情報を取得します。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set</ise-pan-ip>
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ2:デバイス管理者ポリシーセット情報の取得に使用されるURLを見つけます。

H Swagger.	Select a definition Policy ~	
Cisco ISE API - Policy CAS		
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/vl/policy/device-admin/policy-set Device Admin - List of policy sets.	^ ≜	
Device Admin - List of policy sets.		

API URI(API URI)

ステップ 3:これはPythonコードの例です。 コンテンツをコピーして貼り付けます。ISE IP、ユ ーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

#### <#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())
```

## 次に、予想される出力例を示します。

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

### Dデバイス管理者 – 認証ルールの取得

このAPIは、特定のポリシーセットの認証ルールを取得します。

## ステップ1:APIコールに必要な情報。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set&gt;/authentication</id-of-policy- </ise-pan-ip>
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

ステップ2:認証ルール情報の取得に使用するURLを探します。

	H Swagger.	Select a definition	Policy ~	
	Cisco ISE API - Policy (300) (ASS) https://10.106.33.92.4424/https://docs/tgroup-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		~	
	Device Administration - Authorization Global Exception Rules		~	
	Device Administration - Authentication Rules		^	
	CET /api/vl/policy/device-admin/policy-set/(policyId)/authentication Device Admin - Get authentication	n rules.	^ <b>≜</b>	
	Device Admin - Get authentication rules.			

API URI(API URI)

ステップ3:これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユ ーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

#### <#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:")
```



注:IDは、「デバイス管理者 – ポリシーセットのリスト」のステップ3のAPI出力からのも のです。たとえば、41ed8579-429b-42a8-879e-61861cb82bbfはTACACSのデフォルトポ リシーセットです。

次に、予想される出力例を示します。

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

デバイス管理者 – 許可ルールの取得

このAPIは、特定のポリシーセットの認可ルールを取得します。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set&gt;/authorization</id-of-policy- </ise-pan-ip>
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

## ステップ2:許可ルール情報の取得に使用されるURLを探します。

Cisco ISE API - Policy (100) (100) https://to.106.33.82-44240eev/Jage-doct/group-Policy		
Servers https://10.108.33.92:44240 - 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	~	
Device Administration - Authorization Global Exception Rules	~	
Device Administration - Authentication Rules	~	
Device Administration - Authorization Rules	^	
CET /api/vl/policy/device-admin/policy-set/{policyId}/authorization Device Admin - Get authorization rules.	^ ≞	
Device Admin - Get authorization rules.		

API URI(API URI)

ステップ 3:これはPythonコードの例です。 コンテンツをコピーして貼り付けます。ISE IP、ユ ーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

#### <#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:")



注:IDは、「デバイス管理者 – ポリシーセットのリスト」のステップ3のAPI出力からのも のです。たとえば、41ed8579-429b-42a8-879e-61861cb82bbfはTACACSのデフォルトポ リシーセットです。

次に、予想される出力例を示します。

Return Code:

200

Expected Outputs:

{'version': '10.0', 'response': [{'rule': {'default': True, 'id': '39d9f546-e58c-4f79-9856-c0a244b8a2ae', 'name': 'Default', 'hitCounts': 0, 'rank': 0, 'state': 'enable

ネットワークアクセス:ポリシーセットのリスト

このAPIは、ISE導入のネットワークアクセスポリシーセットを取得します。

### ステップ1:APIコールに必要な情報。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set</ise-pan-ip>
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

### ステップ2:特定のISEノード情報を取得するために使用されるURLを見つけます。

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(API URI)

ステップ 3:これはPythonコードの例です。 コンテンツをコピーして貼り付けます。ISE IP、ユ ーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

#### <#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())
```

## 次に、予想される出力例を示します。

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

#### ネットワークアクセス – 認証ルールの取得

#### このAPIは、特定のポリシーセットの認証ルールを取得します。

## ステップ1:APIコールに必要な情報。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set/<id-of-policy- Set&gt;/authentication</id-of-policy- </ise-pan-ip>
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

## ステップ2:認証ルール情報の取得に使用するURLを探します。

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(API URI)

ステップ3:これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユ ーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

#### <#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())
```



注:このIDは、「ネットワークアクセス:ポリシーセットのリスト」の手順3のAPI出力 から取得されます。たとえば、ba71a417-4a48-4411-8bc3-d5df9b115769はBGL\_CFME02-FMCです。

## 次に、予想される出力例を示します。

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default': '048875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default': '048875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default': '048875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Default': '048875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default': 'Def

## ネットワークアクセス – 許可ルールの取得

#### このAPIは、特定のポリシーセットの認可ルールを取得します。

## ステップ1:APIコールに必要な情報。

メソッド	GET
URL	https:// <ise-pan-ip>/api/v1/policy/network-</ise-pan-ip>

	access/policy-set/ <id-of-policy- Set&gt;/authorization(許可)</id-of-policy- 
Credentials	OpenAPIアカウントの資格情報を使用します。
ヘッダー	Accept : application/json Content-Type : application/json

## ステップ2:許可ルール情報の取得に使用されるURLを探します。

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(API URI)

ステップ3:これはPythonコードの例です。コンテンツをコピーして貼り付けます。ISE IP、ユ ーザ名、およびパスワードを置き換えてください。実行するPythonファイルとして保存します。

ISEとPythonコード例を実行しているデバイスの間の接続が良好であることを確認します。

#### <#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/author

...

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())
```



注:IDは、「ネットワークアクセス:ポリシーセットのリスト」の手順3のAPI出力からの ものです。たとえば、ba71a417-4a48-4411-8bc3-d5df9b115769はBGL\_CFME02-FMCで す。

次に、予想される出力例を示します。

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

## トラブルシュート

OpenAPIに関連する問題をトラブルシューティングするには、デバッグログ設定ウィンドウで theapiservicecomponentのログレベルをDEBUGに設定します。

デバッグを有効にするには、Operations > Troubleshoot > Debug Wizard > Debug Log

## Configuration > ISE Node > apiserviceの順に移動します。

=	dentity Services	Engine		Ор	erations / Troubl	eshoot		License Warning	Q	۵	0	Q   8	٩
р	Bookmarks	Diagnostic Tools Download Lo	ogs De	bug Wizard									
	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List	) ISE-BOL-CFME01-PANU Ug Level Co	nfiguration							ß	
0	Policy		0 Edit	← Reset to Default	Log Filter Enable	Log Filter Disable					Allis	<ul> <li>V</li> </ul>	
2.	Administration			Component Name	∧ Log Level	Description	Log file Name	Log Filter					
ń	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled				î.	
			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					
			0	apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled					
			0	bootstrap-wizard	INFO	Bootstrap wizard messages Save Can	-psc.log	Disabled					
			0	ca-service	INFO	CA Service messages	caservice.log	Disabled					

APIサービスのデバッグ

デバッグログファイルをダウンロードするには、Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logsの順に移動します。

≡	dentity Services	Engine		Operations / Trou	bleshoot		🔺 License Warning	<b>a</b>	Q. @	0 Q   P	٤
Щ	Bookmarks	Diagn	oostic Tools Download Logs	Debug Wizard							
53	Dashboard		ISE-BGL-CFME01-PAN								
망	Context Visibility		ISE-BGL-CFME02-MNT	Delete 2 <sup>3</sup> Expand All Collapse A		Barrad Mar	<b>0</b> 1				
*	Operations		ISE-DLC-CEME02-PSN	Debug Log Type	Log File	Description	Size				
0	Policy		ISE-RTP-CFME01-PAN	✓ Application Logs						^	
80	Administration		ISE-RTP-CFME02-MNT	> ad_agent (1) (100 KB)							
ก็เ	Work Centers		x	> ai-analytics (11) (52 KB) > api-gateway (16) (124 KB)							
				✓ 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				
				0	api-service.log.2024-04-07-1		4.0 KB				
				-							

デバッグログのダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。