OpenAPI zum Abrufen von ISE-Richtlinieninformationen zu ISE 3.3 verwenden

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Netzwerkdiagramm
Konfiguration auf der ISE
Python-Beispiele
Device Admin - Liste der Richtliniensätze
Geräteadministrator - Authentifizierungsregeln abrufen
Geräteadministrator - Autorisierungsregeln abrufen
Netzwerkzugriff - Liste von Richtliniensätzen
Netzwerkzugriff - Authentifizierungsregeln abrufen
Netzwerkzugriff - Autorisierungsregeln abrufen
Fehlerbehebung

Einleitung

In diesem Dokument wird das Verfahren zur Verwendung von OpenAPI zur Verwaltung Cisco Identity Services Engine (ISE) Richtlinie.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

- ISE 3.3
- Python 3.10.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ab Cisco ISE 3.1 sind neuere APIs im OpenAPI-Format verfügbar. Die Managementrichtlinien optimieren die Netzwerksicherheit und das Netzwerkmanagement, indem sie die Interoperabilität verbessern, die Effizienz der Automatisierung verbessern, die Sicherheit stärken, Innovationen fördern und die Kosten senken. Diese Richtlinie ermöglicht der ISE die nahtlose Integration in andere Systeme, eine automatisierte Konfiguration und Verwaltung, eine präzise Zugriffskontrolle, die Förderung von Innovationen von Drittanbietern und die Vereinfachung von Managementprozessen. Auf diese Weise werden Wartungskosten gesenkt und die Investitionsrendite insgesamt gesteigert.

Konfigurieren

Netzwerkdiagramm



Konfiguration auf der ISE

Schritt 1: Fügen Sie ein OpenAPI-Administratorkonto hinzu.

Um einen API-Administrator hinzuzufügen, navigieren Sie zu Administration > System > Admin Access > Administrators > Admin Users > Add.

≡	dentity Services I	Engine			Administra	tion / System			License Warning	۵ ۵	0	0 A
Щ	Bookmarks	Deployment Licensing	Certificat	es Logging	Maintenance	Upgrade Health	Checks Backup	& Restore Admin	Access Settings			
5	Dashboard	Authentication										
16	Context Visibility	Authorization	> A0	ministrat	lors					0.1		0 B
*	Operations	Administrators	× 21	lit + Add	🛠 Change Status	Delete				Selected	All	v v
.0	Policy	Admin Users		Status	Name	Description	First Name Last Nam	e Email Address	Admin Groups			
80	Administration	Admin Groups) Enabled	admin	Default Admin User			Super Admin			
di.	Work Centers	Settings	>) Enabled	a ApiAdmin				ERS Admin			
?	Interactive Help											



Schritt 2: Aktivieren Sie OpenAPI auf der ISE.

Die offene API ist auf der ISE standardmäßig deaktiviert. Navigieren Sie zu Administration > System > Settings > API Settings > API Service Settings. Schalten Sie die OpenAPI-Optionen um. Klicken Sie auf Speichern.

≡ dentity Services Engine	Administration / System	🔺 License Warning 🛛 🖓 😨 🗘 🞗
Bookmarks Deployment Licensing C	ertificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
Bit Dashboard Client Provisioning Id Context Visibility FIPS Mode Security Settings Security Settings Operations Alarm Settings Display General MDM / UEM Settings Administration Posture	API Settings Overview API Service Settings API Gateway Settings ~ API Service Settings for Primary Administration Node ERS (Read/Write)	
Work Centers Protecols ? Interactive Help Endpoint Scripts	 Open API (Read/Write) API Service Setting for All Other Nodes 	
Proxy SMTP Server SMS Gateway System Time	ERS (Read) Open API (Read)	
API Settings Data Connect	CSRF Check (only for ERS Settings) C Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)	
Network Success Diagnostics > DHCP & DNS Services	 Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3) 	
Max Sessions Light Data Distribution Endpoint Replication		Reset Save

OpenAPI aktivieren

Schritt 3: Erkunden der ISE OpenAPI

Navigieren Sie zu Administration > System > Settings > API Settings > Overview. Klicken Sie auf OpenAPI, um den Link aufzurufen.

≡	dentity Services I	Engine	Administration / System	Q	ە	A A				
Щ	Bookmarks	Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access							
10	Dashboard Context Visibility	Client Provisioning FIPS Mode Security Settings	API Settings							
- % - 0	Operations Policy	Alarm Settings General MDM / UEM Settings	Overview API Service Settings API Gateway Settings							
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.	You can manage Cisco ISE Release 3.1 new APIs are available in the OsenAPI format.						
đ	Work Centers	Profiling	The ERS and OpenAPI services are HTTPS-only REST APIs that operate ever port 44.3. Currently, ERS APIs also operate over port 9060, However, port 9060 might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 44.3 for ERS APIs. Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API service are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API service are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API service are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API service are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API service are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API service, you must have the ERS-Admin or ERS-Operator user group assignment. > To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment. For more information on ISE ERS API, please visit: For openapi documention for ERS, click below: ERS_V1 Ext APIs Ext APIs Ext APIs							
?	Interactive Help	Protocols Endpoint Scripts								
		Proxy SMTP Server SMS Gateway								
	I	API Settings Data Connect								

OpenAPI aufrufen

Python-Beispiele

Device Admin - Liste der Richtliniensätze

Diese API ruft Informationen zu den Admin-Richtliniensätzen des Geräts ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set</ise-pan-ip>
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von Informationen zu den Admin-Richtlinien für Geräte verwendet wird.

(i) Swagger.	Select a definition Policy	*
Cisco ISE API - Policy (CSS) https://10.106.33.82.442404epev3/age-decr?group-Policy		
Servers https://10.106.33.92:44240 - Inferred Uri		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

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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())
```

Dies ist das Beispiel der erwarteten Ergebnisse.

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

GGeräteadministrator - Authentifizierungsregeln abrufen

Diese API ruft Authentifizierungsregeln eines bestimmten Richtliniensatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set>/authentication</id-of-policy- </ise-pan-ip>
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von Authentifizierungsregelinformationen verwendet wird.

	Select a definition	Policy	×	
Cisco ISE API - Policy (10) (15)				
Servers https://10.106.33.92;44240 - Inferred Uri			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 authentic	ation rules.		^ ≞	
Device Admin - Get authentication rules.				

API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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/authents'
    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())



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von Device Admin - List Of Policy Sets. 41ed8579-429b-42a8-879e-61861cb82bbf ist beispielsweise der TACACS-Standardrichtliniensatz.

Dies ist das Beispiel der erwarteten Ergebnisse.

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

Geräteadministrator - Autorisierungsregeln abrufen

Diese API ruft Autorisierungsregeln eines bestimmten Richtliniensatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/policy/device- admin/policy-set/<id-of-policy- Set>/authorization</id-of-policy- </ise-pan-ip>
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen der Autorisierungsregelinformationen verwendet wird.

Cisco ISE API - Policy (ISB) CASS https://10.106.33.92-4424Mapev3app-docr1grapp-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	~
Device Administration - Authorization Rules	^
GET /api/v1/policy/device-admin/policy-set/{policyId}/authorization Device Admin - Get authorization rules.	<u>^ ≜</u>
Device Admin - Get authorization rules.	

API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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:")



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von Device Admin - List Of Policy Sets. 41ed8579-429b-42a8-879e-61861cb82bbf ist beispielsweise der TACACS-Standardrichtliniensatz.

Dies ist das Beispiel der erwarteten Ergebnisse.

Return Code: 200

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

Netzwerkzugriff - Liste von Richtliniensätzen

Diese API ruft Netzwerkzugriffsrichtliniensätze von ISE-Bereitstellungen ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set</ise-pan-ip>
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Geben Sie die URL an, die zum Abrufen der spezifischen ISE-Knoteninformationen verwendet wird.

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

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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())
```

Dies ist das Beispiel der erwarteten Ergebnisse.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': False, 'id': 'ba71a417-4a48-4411-8bc3-d5df9b115769', 'name': 'BGL_CFME0

Netzwerkzugriff - Authentifizierungsregeln abrufen

Diese API ruft Authentifizierungsregeln eines bestimmten Richtliniensatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/policy/network- access/policy-set/<id-of-policy- Set>/authentication</id-of-policy- </ise-pan-ip>
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen der Authentifizierungsregelinformationen verwendet wird.

Netwo	ork 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

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen. Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#root>

from requests.auth import HTTPBasicAuth import requests

requests.packages.urllib3.disable_warnings()

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

url = "

```
\tt https://10.106.33.92/api/v1/policy/network-access/policy-set/ba71a417-4a48-4411-8bc3-d5df9b115769/autherstates and the set of th
```

"

```
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())
```



Hinweis: Die ID stammt aus API-Ausgaben in Schritt 3 von Network Access - List Of Policy Sets. Zum Beispiel ba71a417-4a48-4411-8bc3-d5df9b115769 ist BGL_CFME02-FMC.

Dies ist das Beispiel der erwarteten Ergebnisse.

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

Netzwerkzugriff - Autorisierungsregeln abrufen

Diese API ruft Autorisierungsregeln eines bestimmten Richtliniensatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/policy/network-</ise-pan-ip>

	access/policy-set/ <id-of-policy- Set>/authorization</id-of-policy-
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen der Autorisierungsregelinformationen verwendet wird.

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

API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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())
```



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von "Network Access - List Of Policy Sets". Beispiel: ba71a417-4a48-4411-8bc3-d5df9b115769 lautet BGL_CFME02-FMC.

Dies ist das Beispiel der erwarteten Ergebnisse.

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

Fehlerbehebung

Um Probleme im Zusammenhang mit den OpenAPIs zu beheben, legen Sie dieProtokollstufe für dieAPIsKomponente im Fenster Konfiguration des Debug-Protokolls auf DEBUG fest.

Um das Debuggen zu aktivieren, navigieren Sie zu Operations > Troubleshoot > Debug Wizard >

Debug Log Configuration > ISE Node > apiservice.

=	dentity Services	Engine			O	peratio	ons / Trout	pleshoot		A License Warning	Q	۵	0	٩	A
J	Bookmarks	Diagnostic Tools	Download Logs	Del	bug Wizard										
■ 13 ★	Dashboard Context Visibility	Debug Profile Configuration	ation	Node List	ug Level Co	onfig	uratio	n						4	3
0	Policy			/ Edit	← Reset to Default	Log Fi	Iter Enable	Log Filter Disable					AI	~ 1	7
2	O Administration				Component Name	~ L	og Level	Description	Log file Name	Log Filter					
1	Work Centers			0	accessfilter	I	NFO	RBAC resource access filter	ise-psc.log	Disabled					*
				0	Active Directory	V	WARN	Active Directory client internal messages	ad_agent.log						
?) Interactive Help			0	admin-ca	1	NFO	CA Service admin messages	ise-psc.log	Disabled					
				0	admin-infra	I	NFO	infrastructure action messages	ise-psc.log	Disabled					
				0	admin-license	1	NFO	License admin messages	ise-psc.log	Disabled					
				0	ai-analytics	1	NFO	AI Analytics	ai-analytics.log	Disabled					
				0	anc	1	NFO	Adaptive Network Control (ANC) debug	ise-psc.log	Disabled					
				0	api-gateway		NFO	API Gateway native objects logs	api-gateway.log	Disabled					
				•	apiservice		DEBUG	ISE API Service logs	api-service.log	Disabled					
				0	bootstrap-wizard	1	NFO	Bootstrap wizard messages Save Can	-psc.log	Disabled					
				0	ca-service	I	NFO	CA Service messages	caservice.log	Disabled					

Debuggen von API-Diensten

Um die Debug-Protokolldatei herunterzuladen, navigieren Sie zu Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs.

≡	diale Identity Services	Engine		Operations / Troubleshoot			A License Warning	Q	۵	0	$\varphi \mid \varphi$
н	Bookmarks	Diagnostic Tool	s Download Logs	Debug Wizard							
11	Dashboard	ISI	-BGL-CFME01-PAN								
망	Context Visibility	ISI	BGL-CFME02-MNT	Delete 2 ⁸ Expand All Collapse A	all and a second se						
*	Operations	158 158	-DLC-CFME01-PSN	Debug Log Type	Log File	Description	Size				
0	Policy	ISI	-RTP-CFME01-PAN	✓ Application Logs							î.
8.	Administration	ISE	-RTP-CFME02-MNT	> ad_agent (1) (100 KB)							-1-
nii:	Work Centers			> api-gateway (16) (124 KB)							-1-
				✓ 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				

Debug-Protokolle herunterladen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.