# Verwenden von OpenAPI zum Abrufen von ISE-Zertifikatinformationen auf ISE 3.3

## Inhalt

Einleitung
Hintergrund
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
Konfigurieren
Netzwerkdiagramm
Konfiguration auf der ISE
Python-Beispiele
Abrufen aller Systemzertifikate eines bestimmten Knotens
Systemzertifikat eines bestimmten Knotens nach ID abrufen
Liste aller vertrauenswürdigen Zertifikate abrufen
Vertrauenswürdiges Zertifikat nach ID abrufen
Fehlerbehebung

## Einleitung

In diesem Dokument wird das Verfahren zur Verwendung von openAPI zur Verwaltung von Cisco Identity Services Engine (ISE)-Zertifikaten beschrieben.

## Hintergrund

Angesichts der zunehmenden Komplexität der Sicherheit und Verwaltung von Unternehmensnetzwerken führt die Cisco ISE 3.1 APIs im OpenAPI-Format ein, die das Lebenszyklus-Management von Zertifikaten optimieren. Sie bieten eine standardisierte und automatisierte Schnittstelle für effiziente und sichere Zertifikatabläufe, die Administratoren dabei unterstützt, strenge Sicherheitsvorkehrungen durchzusetzen und die Netzwerk-Compliance aufrechtzuerhalten.

## 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.

## Konfigurieren

### Netzwerkdiagramm



## Konfiguration auf der ISE

Schritt 1: Hinzufügen eines offenen API-Administrationskontos

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

≡	diale Identity Services	Engine				Administra	tion / Syster	n			🔺 Uo	cense Warning	۹ ،	۞ (	φ	R
Щ	Bookmarks	Deployment Licensing	Cer	rtificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restor	e Admin	Access	Settings				
	Dashboard	Authentication		Adam	in interaction											
명	Context Visibility	Authorization	>	Adm	mstrate	DIS							Sele	cted 0 Tota	12 3	63
*	Operations	Administrators	~	0 Edit	+ Add	🖒 Change Status	🛛 Delete 📋	Duplicate					001			V
0	Policy	Admin Users Admin Groups			Status	Name	Descriptio	n First Name	Last Name Emai	I Address	Admin Grou	ups				
20	Administration				Enabled	admin 😛	Default Ac	dmin User			Super Adm	nin				
rill	WORK Centers	octonys	1		Enabled	4 ApiAdmin					ERS Admin					
?	Interactive Help															

API-Administrator

Schritt 2: Aktivieren der offenen API auf der ISE

Die offene API ist auf der ISE standardmäßig deaktiviert. Um sie zu aktivieren, navigieren Sie zu

Administration > System > API Settings > API Service Settings. Schalten Sie die Open API-Optionen um. Klicken Sie auf Speichern.

I betwars   I betwar

OpenAPI aktivieren

### Schritt 3: Erkunden der offenen ISE-API

navigieren Sie zu Administration > System > API Settings > Overview. Klicken Sie auf API-Besuchslink öffnen.

≡	dentity Services E	Engine				Administra	tion / Syster	n				Q	۵	3	0   A
н	Bookmarks	Deployment	Licensing	Certificat	s Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
51	Dashboard	Client Provisioni	ng												
망	Context Visibility	FIPS Mode Security Settings		AP	l Settings										
*	Operations	Alarm Settings		Oven	iew API Servic	e Settings API G	ateway Settings								
-0	Policy	General MDM / I	JEM Settings	API	Services Overvie	9W									
20	Administration	Posture		> You c	in manage Cisco IS g Cisco ISE Release	E nodes through two s	sets of API form vailable in the O	ats-External Restful Ser	rvices (ERS) and OpenAPI.						
di.	Work Centers	Profiling		The E Curre	RS and OpenAPI ser tily, ERS APIs also o	vices are HTTPS-only operate over port 906	REST APIs that 0. However, port	operate over port 443. 9060 might not be sup	ported for ERS APIs in late	r					
		Protocols		> Cisco Both	ISE releases. We re he API services are API Service Services	commend that you on disabled by default. E	ly use port 443 nable the API se	for ERS APIs. prvices by clicking the c	corresponding toggle buttor	15					
?	Interactive Help	Endpoint Script		> To us	either API service,	you must have the EF	S-Admin or ERS	S-Operator user group a	assignment.						
		Proxy SMTP Server SMS Gateway		For m https: For oj	ore information on I //10.106.33.92:442 enapi documention	SE ERS API, please vis 40/ers/sdk for ERS, click below:	sit:								
	1	System Time API Settings		For m	ve information on l' //10.106.33.92:442	SE Open API, please s 40/api/swagger-ui/in	dex_html								
		Data Connect				ERS API									

OpenAPI aufrufen

## Python-Beispiele

Abrufen aller Systemzertifikate eines bestimmten Knotens

Die API listet alle Zertifikate eines bestimmten ISE-Knotens auf.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname></ise-node-hostname></ise-pan-ip>
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von Zertifikaten eines bestimmten ISE-Knotens verwendet wird.

😁 Swag	ager. Select a definition Certificates	~
Cisco Https://10.106.33	D ISE API - Certificates (100) (75)	
Servers https://10.10	06.33.92:44240 - Inferred Urt 🗸	
certs-a	pi-controller the certs API	~
Certific	cates	^
GET	/api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	✓ â
POST	/api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	✓ â
GET	/api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given ID	✓ â
DELETE	/api/vl/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given ID	✓ â
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 entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)	vice) 🗸 🗎
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	✓ â
GET	/api/vl/certs/system-certificate/{hostName} Oet all system certificates of a particular node	∧ <sup>⊕</sup>
This API su	upports filtering, sorting and pagination.	

API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. 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 sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, 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/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())
```

Hier sehen Sie das Beispiel der erwarteten Ergebnisse.

Return Code: 200 Expected Outputs: {'response': [{'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML\_ISE-DLC-CFME0

Systemzertifikat eines bestimmten Knotens nach ID abrufen

Diese API stellt Details eines Systemzertifikats eines bestimmten Knotens basierend auf dem angegebenen Hostnamen und der angegebenen ID bereit.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname>/<id-of- Certificate&gt;</id-of- </ise-node-hostname></ise-pan-ip>
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen des Zertifikats eines bestimmten Knotens basierend auf dem angegebenen Hostnamen und der angegebenen ID verwendet wird.

	Cisco ISE API - Certificates (IDD) (CTS) https://10.106.33.92.442404pev/dept-doct/group-Certificates		
	Servers https://10.106.33.92:44240 - Inferred Url v		
	certs-api-controller the certs API	~	
[	Certificates	^	
	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 ID	∨ ≜	
	DELETE /api/vl/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/v1/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	✓ ≜	
	POST /api/vl/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/vl/certs/renew-certificate Ranew certificates of OCSP responder and Cisco ISE Messaging Service	✓ ≜	
	POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	✓ ≜	
	GET /api/v1/certs/system-certificate/{hostName} Get all system certificates of a particular node	✓ ≜	
	OET         /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.		

#### API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. 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 sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, 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/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:")
```



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von "Get All System Certificates Of A Particular Node", z. B. 5b5b28e4-2a51-495c-8413-610190e1070b ist "Default self-signed saml server certificate - CN=SAML\_ISE -DLC-CFME02-PSN.cisco.com".

Hier sehen Sie das Beispiel der erwarteten Ergebnisse.

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

Liste aller vertrauenswürdigen Zertifikate abrufen

Die API listet alle vertrauenswürdigen Zertifikate des ISE-Clusters auf.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate</ise-pan-ip>
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

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

POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	$\sim$	-
FOST /api/vl/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)	$\sim$	-
POST /api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	$\sim$	-
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Centificate	$\sim$	-
GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	$\sim$	-
GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular mode by ID	$\sim$	-
PUT /api/v1/certs/system-certificate/{hostName}/{id} Update data for existing system certificate	$\sim$	1
DELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname	$\sim$	â
POST /api/v1/certs/system-certificate/export Export a system certificate with a given a certificate ID	$\sim$	1
POST /api/v1/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Claco ISE	$\sim$	-
POST /api/vl/certs/system-certificate/import Import system certificate In Cisco ISE	$\sim$	1
GET /api/v1/certs/trusted-certificate Get list of all trusted certificates	^	â
This API supports Filtering. Sorting and Pagination.		
Filtering and Sorting are supported for the following attributes: filendly/tame subject issuedfly issuedfl		
Note: ISE internal CA certificates will not be exported.		

#### API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. 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 sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, 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/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:")

Hier ist das Beispiel der erwarteten Ausgaben. (weggelassen)

Return Code: 200 Expected Outputs: {'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=Ver

### Vertrauenswürdiges Zertifikat nach ID abrufen

Diese API kann Details eines Vertrauensstellungszertifikats basierend auf einer angegebenen ID anzeigen.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
Anmeldeinformationen	Open API-Kontoinformationen verwenden
Header	Akzeptieren: Anwendung/json Inhaltstyp: Anwendung/json

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

Cisco ISE API - Certificates (100) (ASS) https://lo.106.3.3.82.44240upiv.Siver-dec:Terrupe-Certificates	
Servers https://10.106.33.92:44240 - Inferred Url v	
certs-api-controller the certs API	~
Certificates	^
OET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	<ul> <li>✓ ≜</li> </ul>
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	<ul> <li>✓ ≜</li> </ul>
OET /api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given ID	<ul> <li>✓ ≜</li> </ul>
DELETE /api/vl/certs/certificate-signing-request/{hostName}/{id} Delete the cartificate signing request for a given ID	<ul> <li>✓ ≜</li> </ul>
OET /api/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	<b>∨</b> ≜
POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an Intermediate CA CSR (certificate signing request)	<ul> <li>✓ ≜</li> </ul>
POST /api/vl/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)	<ul> <li>✓ ∅</li> </ul>
POST /api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	<ul> <li>✓ ≜</li> </ul>
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	<ul> <li>✓ ≜</li> </ul>
OET         /api/vl/certs/system-certificate/{hostName}         Get all system certificates of a particular node	<ul> <li>✓ ≜</li> </ul>
OET         /api/v1/certs/system-certificate/{hostName}/{id}         Get system certificate of a particular node by ID	<u>∧</u> ≞
This API provides details of a system certificate of a particular node based on given hostname and ID.	

#### API-URI

Schritt 3: Hier ist das Beispiel des Python-Codes. 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 sicher, dass eine gute Verbindung zwischen der ISE und dem Gerät besteht, 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/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:")
```



**Hinweis:** Die ID stammt aus den API-Ausgaben in Schritt 3 von "Get List Of All Trusted Certificates" (Liste aller vertrauenswürdigen Zertifikate abrufen), z. B. 147d97cc-6ce9-43d7-9928-8cd0fa83e140 ist "VeriSign Class 3 Public Primary Certification Authority".

Hier sehen Sie das Beispiel der erwarteten Ergebnisse.

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

Um Probleme im Zusammenhang mit den Open APIs zu beheben, legen Sie **dieLog-**Ebene für die apiservicecomponent im Konfigurationsfenster**Debug Log** auf DEBUG fest.

Um das Debugging zu aktivieren, navigieren Sie zu **Operations -> Troubleshoot -> Debug Wizard -> Debug Log Configuration -> ISE** Node -> apiservice.

=	dentity Services	Engine	Operations / Troubleshoot					📥 License Warning	Q	۵	0	Q   A
н	Bookmarks	Diagnostic Tools Download Lo	gs Del	bug Wizard								
	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List	> ISE-BGL-CFME01-PAN.s ug Level Cc					ø			
0	Policy		0 Edit	🕁 Reset to Default	Log Filter Enable	Log Filter Disable					Alls	× 7
a.	Administration			Component Name	∧ Log Level	Description	Log file Name	Log Filter				
-fili	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled				ň
			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				

Debuggen von API-Diensten

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

≡	dentity Services	Engine	9		Operations / Troubleshoot					🔺 License Warning	Q	۵ (	9	0   A
Щ	Bookmarks	Diagn	iostic Tools	Download Logs	Debug Wiza	ard								
10	Dashboard		ISE-B	GL-CFME01-PAN										
명	Context Visibility		ISE-B	GL-CFME02-MNT	Delete	e <sup>3</sup> Expand All ≤>Colle	opse All		- de de -	<b>8</b> 1				
*	Operations		ISE-F	LC-CFME02-PSN	Debuş	g Log Type	Log File	Desc	Description	Size				
0	Policy		ISE-R	TP-CFME01-PAN	✓ Application	on Logs								î
4.	Administration		ISE-R	TP+CFME02+MNT	ba <	_agent (1) (100 KB)								_
d.	Work Centers		×		> ai-	analytics (11) (52 KB) i-gateway (16) (124 KB)								
					$\sim$ ap	i-service (13) (208 KB)								
?	Interactive Help						api-service (all logs)	API Ser	vice 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.