

# Erstellen von ISE-Netzwerkgeräten mit ERS API

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[ERS aktivieren \(Port 9060\)](#)

[ERS-Administrator erstellen](#)

[Postbote einrichten](#)

[ISE SDK und grundlegende Postman-Autorisierung](#)

[Erstellen von NAD mithilfe von XML](#)

[Erstellen von NAD mithilfe von JSON](#)

[Überprüfung](#)

[Fehlerbehebung](#)

---

## Einleitung

In diesem Dokument wird der Prozess zum Erstellen von Netzwerkzugriffsgeräten (Network Access Devices, NADs) auf der ISE über die ERS-API mit PostMan als REST-Client beschrieben.

## Voraussetzungen

### Anforderungen

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

- ISE (Identity Services Engine)
- ERS (externe RESTful-Services)
- REST-Clients wie Postman, RESTED, Insomnia usw.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco ISE (Identity Services Engine) 3.1 Patch 6
- Postman-REST-Client v10.17.4



Hinweis: Das Verfahren ist für andere ISE-Versionen und REST-Clients ähnlich oder identisch. Sofern nicht anders angegeben, können Sie diese Schritte für alle ISE-Softwareversionen der Versionen 2.x und 3.x ausführen.

---

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

### ERS aktivieren (Port 9060)

ERS-APIs sind reine HTTPS-REST-APIs, die über Port 443 und Port 9060 betrieben werden. Port 9060 ist standardmäßig geschlossen, daher muss er zuerst geöffnet werden. Wenn Clients, die versuchen, auf diesen Port zuzugreifen, ERS nicht zuerst aktivieren, wird eine Zeitüberschreitung

vom Server angezeigt. Daher muss ERS zuerst über die Cisco ISE-Administrations-Benutzeroberfläche aktiviert werden.

Navigieren Sie zu Administration > Settings > API Settings, und aktivieren Sie die Umschaltfläche ERS (Read/Write).

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration - System' and various system management tabs like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar contains a menu with categories such as 'Client Provisioning', 'Feature', 'Profiling', 'Endpoint Scripts', 'Network Success Diagnostics', and 'DHCP & DNS Services'. The main content area is titled 'API Settings' and has three tabs: 'Overview', 'API Service Settings', and 'API Gateway Settings'. Under 'API Service Settings for Administration Node', there are two toggle switches: 'ERS (Read/Write)' which is currently turned on (indicated by a red arrow), and 'Open API (Read/Write)' which is turned off. Below this, there is a section for 'CSRF Check ( only for ERS Settings )' with two radio button options: 'Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)' and 'Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)'. At the bottom right of the settings area, there are 'Reset' and 'Save' buttons.



Hinweis: Die ERS-APIs unterstützen TLS 1.1 und TLS 1.2. ERS-APIs unterstützen TLS 1.0 nicht, unabhängig davon, ob TLS 1.0 im Fenster Sicherheitseinstellungen der Cisco ISE-GUI aktiviert wurde (Administration > System > Settings > Security Settings). Die Aktivierung von TLS 1.0 im Fenster "Security Settings" (Sicherheitseinstellungen) bezieht sich nur auf das EAP-Protokoll und hat keine Auswirkungen auf ERS APIs.

---

## ERS-Administrator erstellen

Erstellen Sie einen Cisco ISE-Administrator, weisen Sie ein Kennwort zu, und fügen Sie den Benutzer als ERS-Administrator zur Admin-Gruppe hinzu. Sie können den Rest der Konfiguration leer lassen.

Admin User

\* Name **ERS-USER** ←

Status **Enabled** ▾

Email   Include system alerts in emails

Expires

Hard Date

Inactive account never expires

---

Password

\* Password  ⓘ ←

\* Re-Enter Password  ⓘ

[Generate Password](#)

---

User Information

First Name

Last Name

---

Account Options

Description

Change password on next login

---

Admin Groups

ERS Admin ▾ + ←

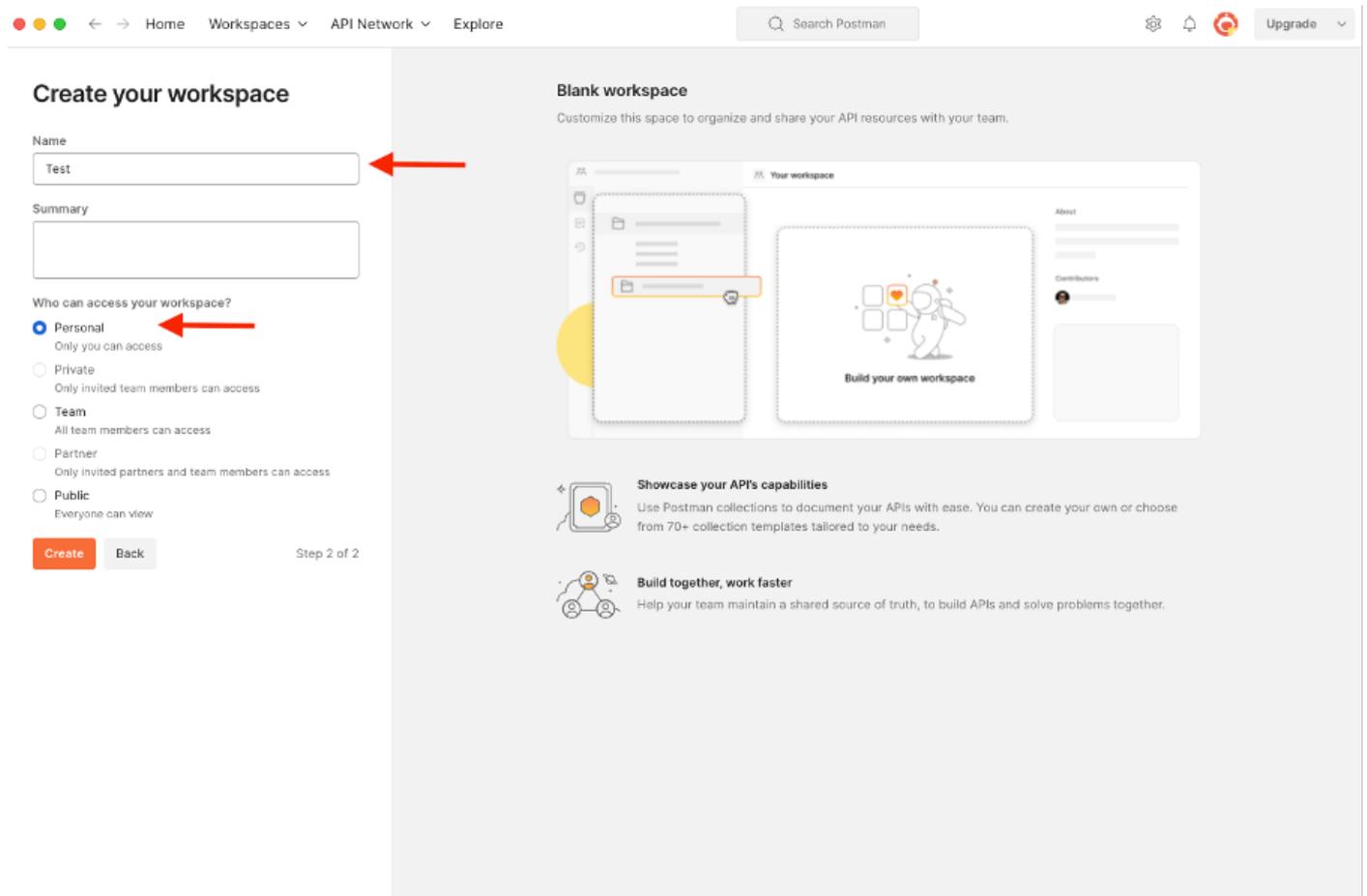
## Postbote einrichten

Laden Sie die Online-Version von Postman herunter oder verwenden Sie sie.

1. Erstellen Sie einen Benutzer, und erstellen Sie einen Arbeitsbereich, indem Sie auf der Registerkarte Arbeitsbereiche auf Arbeitsbereich erstellen klicken.

The screenshot shows the Postman web interface. At the top, there are navigation tabs for 'Home', 'Workspaces', 'API Network', and 'Explore'. A search bar for 'Search Postman' is visible. On the left side, there is a sidebar with various options like 'Create Team', 'Workspaces', 'Private API Network', etc. The 'Workspaces' dropdown menu is open, showing a search bar, a 'Create Workspace' button (highlighted with a red arrow), and a list of recently visited workspaces (currently showing 'Test'). Below the dropdown, there is a message 'No workspaces found' and a link to 'View all workspaces'. The main content area displays a list of API collections, including 'Checkout API (v70)', 'API (v3)', and 'API', each with details like 'Fork' and 'Watch' counts.

2. Wählen Sie Leerer Arbeitsbereich und weisen Sie dem Arbeitsbereich einen Namen zu. Sie können eine Beschreibung hinzufügen und veröffentlichen. Für dieses Beispiel ist Personalis ausgewählt.



Nachdem Sie den Arbeitsbereich erstellt haben, können Sie API-Aufrufe konfigurieren.

## ISE SDK und grundlegende Postman-Autorisierung

Um einen Anruf zu konfigurieren, greifen Sie zunächst auf das ISE ERS SDK (Software Developer Kit) zu. Dieses Tool erstellt die gesamte Liste der API-Aufrufe, die die ISE ausführen kann:

1. Navigieren Sie zu <https://{ise-ip}/ers/sdk>.
2. Melden Sie sich mit Ihren ISE-Administratorrechten an.
3. Erweitern Sie die API-Dokumentation.
4. Blättern Sie nach unten, bis Sie Netzwerkgerät gefunden haben, und klicken Sie darauf.
5. Unter dieser Option finden Sie jetzt alle verfügbaren Vorgänge, die Sie für Netzwerkgeräte auf der ISE ausführen können. Wählen Sie Erstellen aus.

External RESTful Services (ERS) Online SDK

Quick Reference

API Documentation

- Filter Policy
- Guest Location
- Guest Sntp Notification Configur
- Guest Ssid
- Guest Type
- Guest User
- Hotspot Portal
- IP To SCT Mapping
- IP To SCT Mapping Group
- ISE Service Information
- Identity Group
- Identity Sequence
- Internal User
- My Device Portal
- Native Supplicant Profile
- Network Device
- Network Device Group
- Node Details
- PSN Node Details with Radius Ser
- Portal
- Portal Theme
- Profiler Profile
- Pull Deployment Info
- Pxgrid Node
- Pxgrid Settings
- Radius Server Sequence
- RestID Store
- SMS Server
- SXP Connections
- SXP Local Bindings
- SXP Vpns
- Security Groups
- Security Groups ACLs
- Security Groups to Virtual Netwo
- Self Registered Portal
- Sponsor Group
- Sponsor Group Member
- Sponsor Portal
- Sponsored Guest Portal
- Support Bundle Download

Network Device

- Overview
- Resource definition
- Revision History
- Update-By-Name
- Delete-By-Name
- Get-By-Name
- Get-By-Id
- Update
- Get-All
- Delete
- Create
- Get Version
- Bulk Request
- Monitor Bulk Status

Overview

Network Device API allows the client to add, delete, update, and search Network Devices. In this documentation, for each available API you will find the request syntax including the required headers and a response example of a successful flow. Please note that each API description shows weather the API is supported in bulk operation. The Bulk section is showing only 'create' bulk operation however, all other operation which are bulk supported can be used in same way.

Please note that these examples are not meant to be used as is because they have references to DB data. You should treat it as a basic template and edit it before sending to server.

Back to top

Resource definition

Attribute	Type	Required	Default value	Description
name	String	Yes		Resource name
id	String	No		Resource UUID, mandatory for update

Developer Resources

6. Sie können nun die erforderliche Konfiguration zum Durchführen des API-Aufrufs mit XML oder JSON auf einem beliebigen REST-Client sowie ein erwartetes Antwortbeispiel sehen.

Quick Reference

API Documentation

- Filter Policy
- Guest Location
- Guest Sntp Notification Configur
- Guest Ssid
- Guest Type
- Guest User
- Hotspot Portal
- IP To SCT Mapping
- IP To SCT Mapping Group
- ISE Service Information
- Identity Group
- Identity Sequence
- Internal User
- My Device Portal
- Native Supplicant Profile
- Network Device
- Network Device Group
- Node Details
- PSN Node Details with Radius Ser
- Portal
- Portal Theme
- Profiler Profile
- Pull Deployment Info
- Pxgrid Node
- Pxgrid Settings
- Radius Server Sequence
- RestID Store
- SMS Server
- SXP Connections
- SXP Local Bindings
- SXP Vpns
- Security Groups
- Security Groups ACLs
- Security Groups to Virtual Netwo
- Self Registered Portal
- Sponsor Group
- Sponsor Group Member
- Sponsor Portal
- Sponsored Guest Portal
- Support Bundle Download

Network Device

Create

Request:

Method: POST

URI: https://10.201.230.99/ers/config/networkdevice

HTTP 'Content-Type' Header: application/xml | application/json

HTTP 'Accept' Header: application/xml | application/json

HTTP 'ERS-Media-Type' Header (Not Mandatory): network.networkdevice.1.1

HTTP 'X-CSRF-TOKEN' Header (Required Only if Enabled from GUI): The Token value from the GET X-CSRF-TOKEN fetch request

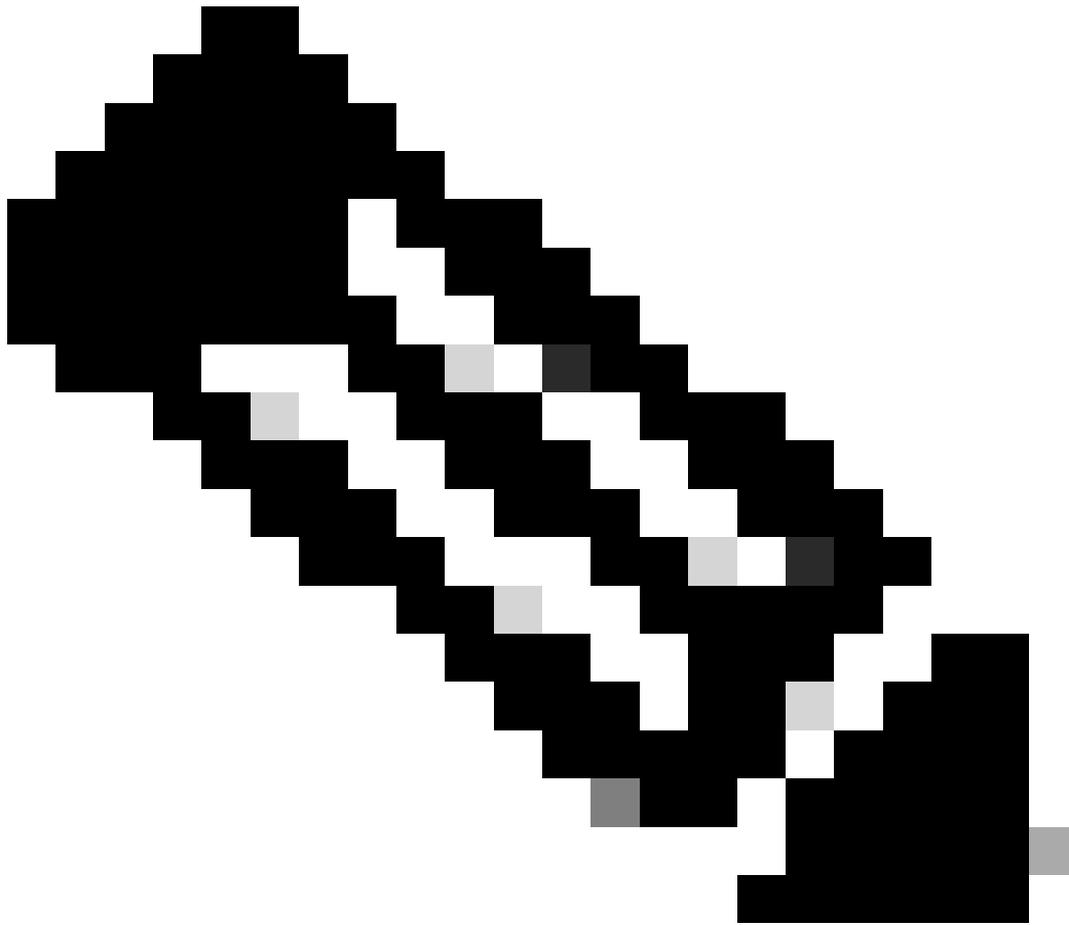
Request Content:

```

XML
<?xml version="1.0" encoding="UTF-8">
<ns0:networkdevice xmlns:ns0="network.ers.ise.cisco.com" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="example nd" ns="">
  <authenticationSettings>
    <dtlsRequired>true</dtlsRequired>
    <enableKeyWrap>true</enableKeyWrap>
    <keyEncryptionKey>1234567890123456</keyEncryptionKey>
    <keyInputFormat>ASCII</keyInputFormat>
    <messageAuthenticatorCodeKey>12345678901234567890</messageAuthenticatorCodeKey>
    <radiusSharedSecret>aaaaa</radiusSharedSecret>
  </authenticationSettings>
  <coaPort>1700</coaPort>
  <dtlsDnsName>ISE111.il.com</dtlsDnsName>
  <NetworkDeviceIPList>
    <NetworkDeviceIP>
      <ipaddress>1.1.1.1</ipaddress>
      <mask>32</mask>
    </NetworkDeviceIP>
  </NetworkDeviceIPList>
  <NetworkDeviceGroupList>
    <NetworkDeviceGroupLocationAll Locations</NetworkDeviceGroup>
    <NetworkDeviceGroupDevice TypeAll Device Types</NetworkDeviceGroup>
  </NetworkDeviceGroupList>
  <profileName>Cisco</profileName>
  <smppSettings>
    <linkTrapQuery>true</linkTrapQuery>
    <macTrapQuery>true</macTrapQuery>
    <originatingPolicyServicesNode>Auto</originatingPolicyServicesNode>
    <pollingInterval>300</pollingInterval>
    <roCommunity>roCommunity
  </smppSettings>
</ns0:networkdevice>

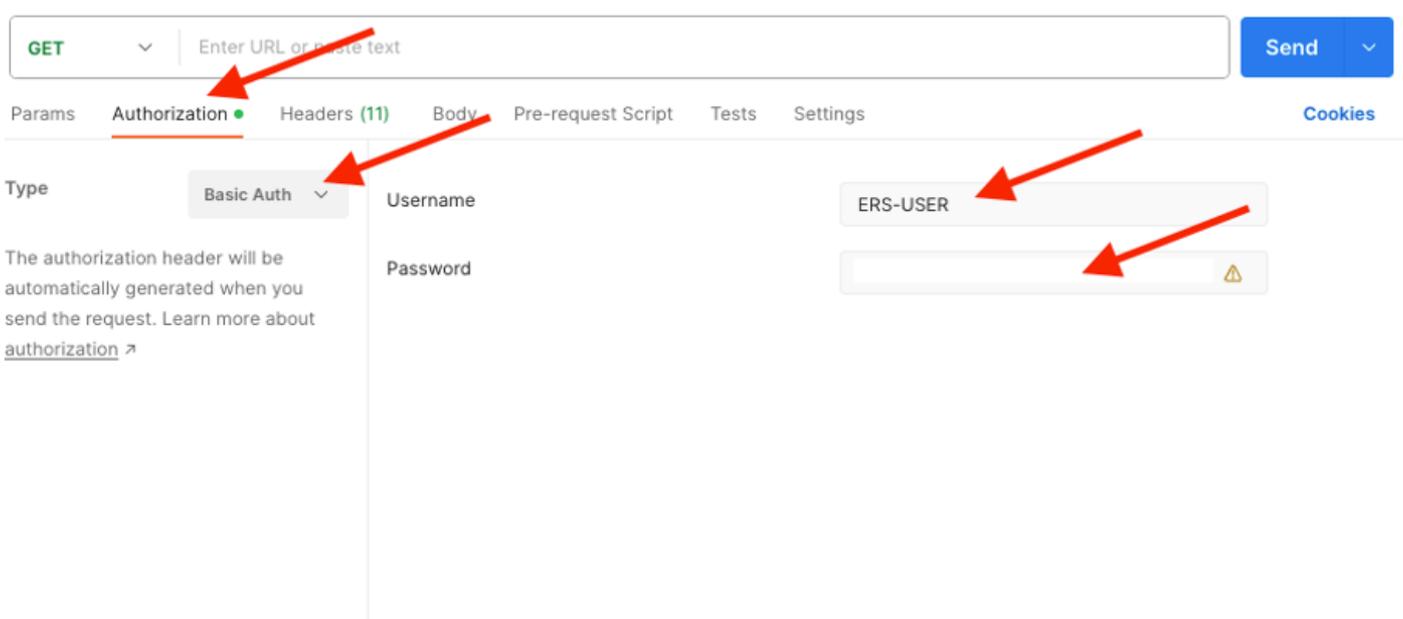
```

7. Zurück zu Postman konfigurieren Sie die grundlegende Authentifizierung zu ISE. Wählen Sie auf der Registerkarte Autorisierung die Option Einfache Authentifizierung als Authentifizierungstyp aus, und fügen Sie die zuvor auf der ISE erstellten ISE ERS-Benutzeranmeldeinformationen hinzu.



Hinweis: Das Passwort wird als Klartext angezeigt, es sei denn, es wurden Variablen für Postman konfiguriert.

---

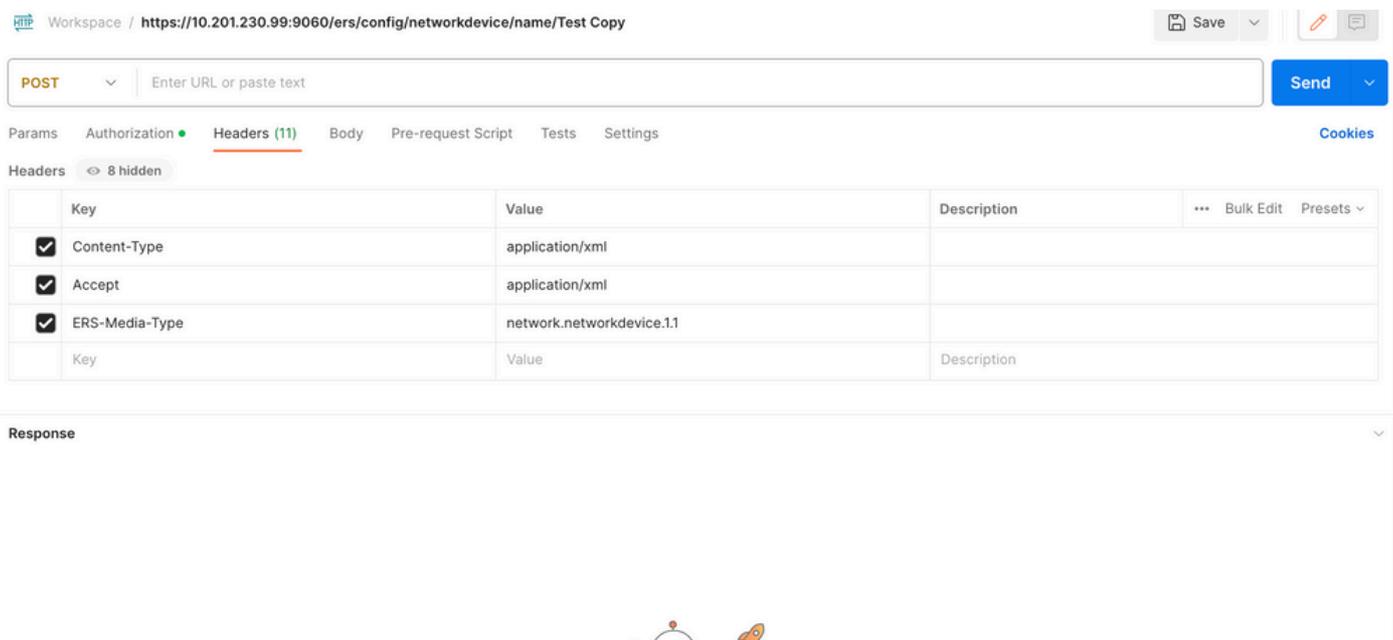


## Erstellen von NAD mithilfe von XML

Erstellen Sie TESTNAD1 mit RADIUS TACACS-, SNMP- und TrustSec-Einstellungen unter Verwendung von XML.

1. Auf dem SDK befinden sich unter Erstellen die Header und Vorlagen, die für den Anruf sowie die erwartete Antwort erforderlich sind.

2. Wechseln Sie zur Registerkarte Headers, und konfigurieren Sie die erforderlichen Header für den API-Aufruf, wie im SDK dargestellt. Die Header-Konfiguration muss wie folgt aussehen:



3. Navigieren Sie zur Kopfzeile des Hauptteils, und wählen Sie unformatiert aus. Auf diese Weise können Sie die XML-Vorlage einfügen, die zum Erstellen der NAD erforderlich ist.

Workspace / <https://10.201.230.99:9060/ers/config/networkdevice/name/Test Copy> Save Send

POST Enter URL or paste text

Params Authorization Headers (11) **Body** Pre-request Script Tests Settings

none form-data x-www-form-urlencoded **raw** binary GraphQL XML

1

Response



#### 4. Die XML-Vorlage sieht wie folgt aus (ändern Sie die Werte nach Bedarf):

```
<?xml version="1.0" encoding="UTF-8"?> <ns0:networkdevice xmlns:ns0="network.ers.ise.cisco.com" xmlns:xs="Schema XML File"
xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="This NAD was added via ERS API" name="TESTNAD1">
<authenticationSettings> <dtlsRequired>true</dtlsRequired> <enableKeyWrap>true</enableKeyWrap>
<keyEncryptionKey>1234567890123456</keyEncryptionKey> <keyInputFormat>ASCII</keyInputFormat>
<messageAuthenticatorCodeKey>12345678901234567890</messageAuthenticatorCodeKey>
<radiusSharedSecret>cisco123</radiusSharedSecret> </authenticationSettings> <coaPort>1700</coaPort>
<dtlsDnsName>Domain</dtlsDnsName> <NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>NAD IP Address</ipaddress>
<mask>32</mask> </NetworkDeviceIP> </NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All
Locations#LAB</NetworkDeviceGroup> <NetworkDeviceGroup>Device Type#All Device Types#Access-Layer</NetworkDeviceGroup>
</NetworkDeviceGroupList> <profileName>Cisco</profileName> <snmpsettings> <linkTrapQuery>true</linkTrapQuery>
<macTrapQuery>true</macTrapQuery> <originatingPolicyServicesNode>Auto</originatingPolicyServicesNode>
<pollingInterval>3600</pollingInterval> <roCommunity>aaa</roCommunity> <version>ONE</version> </snmpsettings> <tacacsSettings>
<connectModeOptions>ON_LEGACY</connectModeOptions> <sharedSecret>cisco123</sharedSecret> </tacacsSettings> <trustsecsettings>
<deviceAuthenticationSettings> <sgaDeviceId>TESTNAD1</sgaDeviceId> <sgaDevicePassword>cisco123</sgaDevicePassword>
</deviceAuthenticationSettings> <deviceConfigurationDeployment> <enableModePassword>cisco123</enableModePassword>
<execModePassword>cisco123</execModePassword> <execModeUsername>Admin</execModeUsername>
<includeWhenDeployingSGTUpdates>true</includeWhenDeployingSGTUpdates> </deviceConfigurationDeployment>
<pushIdSupport>false</pushIdSupport> <sgaNotificationAndUpdates> <coaSourceHost>ise3-1test</coaSourceHost>
<downloadEnvironmentDataEveryXSeconds>86400</downloadEnvironmentDataEveryXSeconds>
<downloadPeerAuthorizationPolicyEveryXSeconds>86400</downloadPeerAuthorizationPolicyEveryXSeconds>
<downloadSGACLListsEveryXSeconds>86400</downloadSGACLListsEveryXSeconds>
<otherSGADevicesToTrustThisDevice>false</otherSGADevicesToTrustThisDevice>
<reAuthenticationEveryXSeconds>86400</reAuthenticationEveryXSeconds>
<sendConfigurationToDevice>false</sendConfigurationToDevice>
<sendConfigurationToDeviceUsing>ENABLE_USING_COA</sendConfigurationToDeviceUsing> </sgaNotificationAndUpdates>
</trustsecsettings> </ns0:networkdevice>
```



**Hinweis:** Beachten Sie, dass die nächsten Zeilen nur erforderlich sind, wenn `<enableKeyWrap>{false|true}</enableKeyWrap>` auf **true** festgelegt ist. Andernfalls kann dasselbe aus der XML-Vorlage gelöscht werden:

```
<keyEncryptionKey>1234567890123456</keyEncryptionKey> <keyInputFormat>ASCII</keyInputFormat>
<messageAuthenticatorCodeKey>12345678901234567890</messageAuthenticatorCodeKey>
```

Sie können die Konfiguration, die Sie nicht benötigen, aus der Vorlage entfernen und die Daten, die Sie tatsächlich während der Erstellung der NAD hinzufügen müssen, belassen. Als Beispiel wird hier dieselbe Vorlage verwendet, jedoch nur für die TACACS-Konfiguration. Stellen Sie unabhängig von der erforderlichen Konfiguration sicher, dass die Vorlage mit `</ns0:networkdevice>` endet.

```
<?xml version="1.0" encoding="UTF-8"?> <ns0:networkdevice xmlns:ns0="network.ers.ise.cisco.com" xmlns:xs="Schema XML File"
xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="This NAD was added via ERS API" name="TESTNAD1">
```

```
<NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>NAD IP Address</ipaddress> <mask>32</mask> </NetworkDeviceIP>
</NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All Locations#LAB</NetworkDeviceGroup>
<NetworkDeviceGroup>Device Type#All Device Types#Access-Layer</NetworkDeviceGroup> </NetworkDeviceGroupList>
<profileName>Cisco</profileName> <tacacsSettings> <connectModeOptions>ON_LEGACY</connectModeOptions>
<sharedSecret>cisco123</sharedSecret> </tacacsSettings> </ns0:networkdevice>
```

5. Fügen Sie die XML-Vorlage für **raw** unter den **Body**-Header ein.

6. Wählen Sie **POST** als Methode, fügen Sie [https://\[ISE-ip\]/ers/config/network-device](https://[ISE-ip]/ers/config/network-device) ein, und klicken Sie auf **Senden**. Wenn alles korrekt konfiguriert wurde, müssen Sie eine Meldung **201 Erstellt** sehen und das Ergebnis leer lassen.

The screenshot shows a REST client interface with the following details:

- URL: `https://10.201.230.99/ers/config/networkdevice`
- Method: **POST**
- Body type: **raw**
- Body content (XML):

```
50 <downloadEnvironmentDataEveryXSeconds>86400</downloadEnvironmentDataEveryXSeconds>
51 <downloadPeerAuthorizationPolicyEveryXSeconds>86400</downloadPeerAuthorizationPolicyEveryXSeconds>
52 <downloadSGACLListsEveryXSeconds>86400</downloadSGACLListsEveryXSeconds>
53 <otherSGADevicesToTrustThisDevice>false</otherSGADevicesToTrustThisDevice>
54 <reAuthenticationEveryXSeconds>86400</reAuthenticationEveryXSeconds>
55 <sendConfigurationToDevice>false</sendConfigurationToDevice>
56 <sendConfigurationToDeviceUsing>ENABLE_USING_COA</sendConfigurationToDeviceUsing>
57 </sgaNotificationAndUpdates>
58 </trustsecsettings>
59 </ns0:networkdevice>
```
- Status: **201 Created**
- Time: 791 ms
- Size: 1.22 KB

7. Bestätigen Sie, ob die NAD erstellt wurde, indem Sie einen **GET**-Aufruf für die NAD durchführen oder die ISE-NAD-Liste überprüfen.



Workspace / <https://10.201.230.99:9060/ers/config/networkdevice/name/Test> Save Send

POST Enter URL or paste text

Params Authorization Headers (12) Body Pre-request Script Tests Settings Cookies

Headers 9 hidden

Key	Value	Description	Bulk Edit	Presets
<input checked="" type="checkbox"/> Content-Type	application/json			
<input checked="" type="checkbox"/> Accept	application/json			
<input checked="" type="checkbox"/> ERS-Media-Type	network.networkdevice.1.1			
Key	Value	Description		

3. Navigieren Sie zur Kopfzeile des **Hauptteils**, und wählen Sie **unformatiert** aus. Auf diese Weise können Sie die JSON-Vorlage einfügen, die zum Erstellen der NAD erforderlich ist.

Workspace / <https://10.201.230.99:9060/ers/config/networkdevice/name/Test Copy> Save Send

POST Enter URL or paste text

Params Authorization Headers (11) **Body** Pre-request Script Tests Settings Cookies

none
  form-data
  x-www-form-urlencoded
  raw
  binary
  GraphQL
 XML

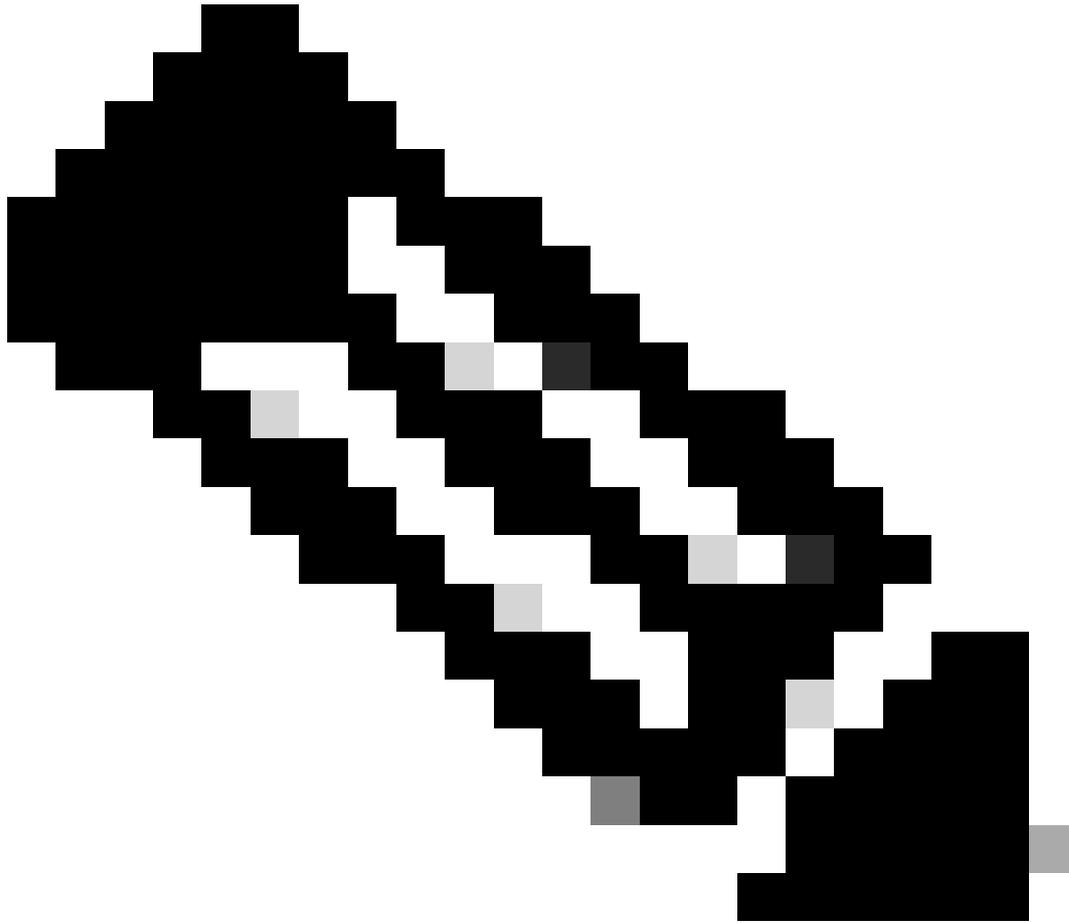
1

Response



4. Die JSON-Vorlage muss wie folgt aussehen (ändern Sie die Werte nach Bedarf):

```
{ "NetworkDevice": { "name": "TESTNAD2", "description": "This NAD was added via ERS API", "authenticationSettings": {
"radiusSharedSecret": "cisco123", "enableKeyWrap": true, "dtlsRequired": true, "keyEncryptionKey": "1234567890123456",
"messageAuthenticatorCodeKey": "12345678901234567890", "keyInputFormat": "ASCII" }, "snmpsettings": { "version": "ONE",
"roCommunity": "aaa", "pollingInterval": 3600, "linkTrapQuery": true, "macTrapQuery": true, "originatingPolicyServicesNode": "Auto" },
"trustsecsettings": { "deviceAuthenticationSettings": { "sgaDeviceId": "TESTNAD2", "sgaDevicePassword": "cisco123" },
"sgaNotificationAndUpdates": { "downloadEnvironmentDataEveryXSeconds": 86400, "downloadPeerAuthorizationPolicyEveryXSeconds":
86400, "reAuthenticationEveryXSeconds": 86400, "downloadSGACLListsEveryXSeconds": 86400, "otherSGADevicesToTrustThisDevice":
false, "sendConfigurationToDevice": false, "sendConfigurationToDeviceUsing": "ENABLE_USING_COA", "coaSourceHost": "ise3-1test" },
"deviceConfigurationDeployment": { "includeWhenDeployingSGTUpdates": true, "enableModePassword": "cisco123", "execModePassword":
"cisco123", "execModeUsername": "Admin" }, "pushIdSupport": "false" }, "tacacsSettings": { "sharedSecret": "cisco123",
"connectModeOptions": "ON_LEGACY" }, "profileName": "Cisco", "coaPort": 1700, "dtlsDnsName": "Domain", "NetworkDeviceIPList": [ {
"ipaddress": "NAD IP Adress", "mask": 32 } ], "NetworkDeviceGroupList": [ "Location#All Locations", "Device Type#All Device Types" ] } }
```



**Hinweis:** Beachten Sie, dass die nächsten Zeilen nur erforderlich sind, wenn "**enableKeyWrap**":{**false|true**} auf "**true**" festgelegt ist. Andernfalls kann dasselbe aus der JSON-Vorlage gelöscht werden:

---

"keyEncryptionKey": "1234567890123456", "messageAuthenticatorCodeKey": "12345678901234567890", "keyInputFormat": "ASCII" Sie können auch die Konfiguration, die Sie nicht benötigen, aus der Vorlage entfernen und die Daten, die Sie tatsächlich während der Erstellung der NAD hinzufügen müssen, belassen.

5. Fügen Sie die JSON-Vorlage für **raw** unter den **Body**-Header ein.

6. Wählen Sie **POST** als Methode, fügen Sie <https://{ISE-ip}/ers/config/network-device> ein, und klicken Sie auf **Senden**. Wenn alles korrekt konfiguriert wurde, müssen Sie eine Meldung **201 Erstellt** sehen und das Ergebnis leer lassen.

Workspace / <https://10.201.230.99:9060/ers/config/networkdevice/name/Test Copy> Save

POST <https://10.201.230.99/ers/config/networkdevice> Send

Params Authorization Headers (13) Body Pre-request Script Tests Settings Cookies Beautify

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 {
2   "NetworkDevice": {
3     "name": "TESTNAD2",
4     "description": "This NAD was added via ERS API",
5     "authenticationSettings": {
6       "radiusSharedSecret": "cisco123",
7       "enableKeyWrap": true,
8       "dtlsRequired": true,
9       "keyEncryptionKey": "1234567890123456",
10      "messageAuthenticatorCodeKey": "12345678901234567890",
11      "keyFormat": "ASCII"
12    }
13  }
14 }
```

Body Cookies (2) Headers (17) Test Results Status: 201 Created Time: 678 ms Size: 1.03 KB Save as Example

Pretty Raw Preview Visualize JSON

1

7. Bestätigen Sie, ob die NAD erstellt wurde, indem Sie einen GET-Aufruf für die NAD durchführen oder die ISE-NAD-Liste überprüfen.

Workspace / <https://10.201.230.99:9060/ers/config/networkdevice/name/Test Copy> Save

GET <https://10.201.230.99/ers/config/networkdevice> Send

Params Authorization Headers (13) Body Pre-request Script Tests Settings Cookies Beautify

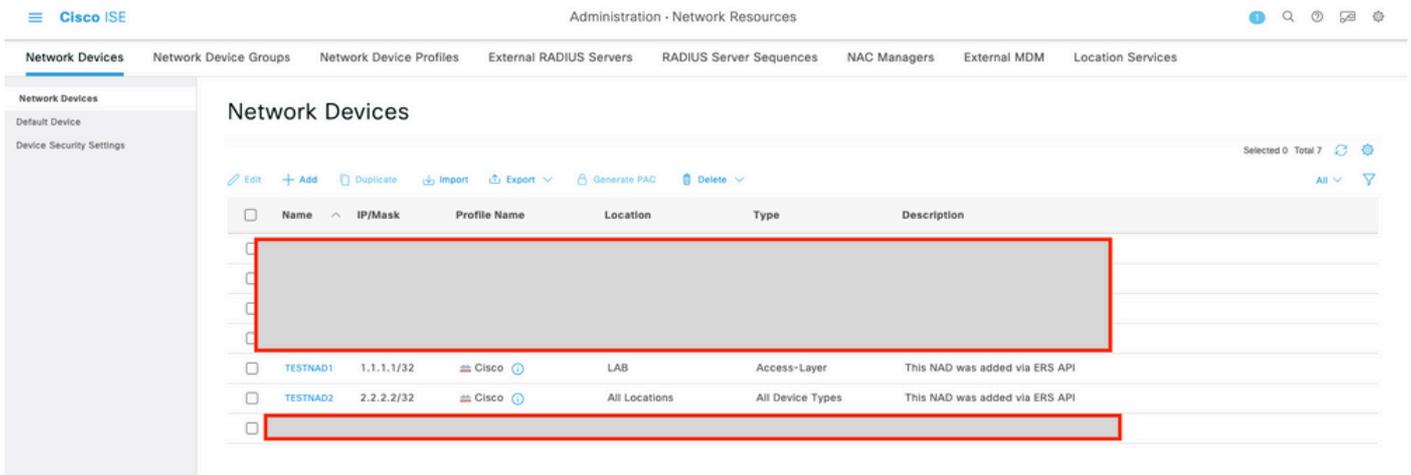
none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 {
2   "NetworkDevice": {
3     "name": "TESTNAD2",
4     "description": "This NAD was added via ERS API",
5     "authenticationSettings": {
6       "radiusSharedSecret": "cisco123",
7       "enableKeyWrap": true,
8       "dtlsRequired": true,
9       "keyEncryptionKey": "1234567890123456",
10      "messageAuthenticatorCodeKey": "12345678901234567890",
11      "keyFormat": "ASCII"
12    }
13  }
14 }
```

Body Cookies (2) Headers (18) Test Results Status: 200 OK Time: 659 ms Size: 3.74 KB Save as Example

Pretty Raw Preview Visualize JSON

```
57 {
58   "name": "TESTNAD1",
59   "description": "This NAD was added via ERS API",
60   "link": {
61     "rel": "self",
62     "href": "https://10.201.230.99/ers/config/networkdevice/afe572d0-5bcc-11ee-9ab7-9a446445bd4f",
63     "type": "application/json"
64   }
65 },
66 {
67   "id": "9dd45a60-5bd7-11ee-9ab7-9a446445bd4f",
68   "name": "TESTNAD2",
69   "description": "This NAD was added via ERS API",
70   "link": {
71     "rel": "self",
72     "href": "https://10.201.230.99/ers/config/networkdevice/9dd45a60-5bd7-11ee-9ab7-9a446445bd4f",
73     "type": "application/json"
74   }
75 }
```



## Überprüfung

Wenn Sie auf die GUI-Seite des API-Diensts zugreifen können, z. B. <https://{iseip}:{port}/api/swagger-ui/index.html> oder <https://{iseip}:9060/ers/sdk>, bedeutet dies, dass der API-Dienst wie erwartet funktioniert.

## Fehlerbehebung

- Alle REST-Vorgänge werden überwacht, und die Protokolle werden in den Systemprotokollen protokolliert.
- Um Probleme zu beheben, die sich auf die offenen APIs beziehen, legen Sie die **Protokollstufe** für die **apiservice**-Komponente im Fenster Konfiguration des **Debug-Protokolls** auf **DEBUG fest**.
- Um Probleme im Zusammenhang mit den ERS APIs zu beheben, legen Sie die **Protokollstufe** für die **ers**-Komponente im Fenster zur Konfiguration des **Debug-Protokolls** auf **DEBUG fest**. Um dieses Fenster anzuzeigen, navigieren Sie zur Cisco ISE-Benutzeroberfläche, klicken Sie auf das Menüsymbol und wählen Sie **Vorgänge > Fehlerbehebung > Debug-Assistent > Debug-Protokollkonfiguration aus**.
- Sie können die Protokolle aus dem Fenster **Download Logs** (Protokolle **herunterladen**) herunterladen. Um dieses Fenster anzuzeigen, navigieren Sie zur Cisco ISE-Benutzeroberfläche, klicken Sie auf das **Menü**-Symbol, und wählen Sie **Operations > Troubleshoot > Download Logs**.
- Sie können entweder ein Support-Paket von der Registerkarte Support Bundle herunterladen, indem Sie auf die Schaltfläche **Download** unter der Registerkarte klicken, oder Sie laden die **api-service**-Debug-Protokolle von der Registerkarte **Debug Logs herunter**, indem Sie auf den Wert **Log File (Protokolldatei)** für das api-service-Debug-Protokoll klicken.

## 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.