

# Konfigurieren des APIC für die Geräteadministration mit ISE und TACACS+

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Authentifizierungsverfahren](#)

[APIC-Konfiguration](#)

[ISE-Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

---

## Einleitung

In diesem Dokument wird das Verfahren zur Integration des APIC in die ISE für die Benutzerauthentifizierung durch den Administrator mit dem TACACS+-Protokoll beschrieben.

## Voraussetzungen

### Anforderungen

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

- Application Policy Infrastructure Controller (APIC)
- Identity Services Engine (ISE)
- TACACS-Protokoll

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- APIC Version 4.2(7u)
- ISE Version 3.2 Patch 1

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



Integrationsdiagramm

### Authentifizierungsverfahren

Schritt 1: Melden Sie sich mit Administratoranmeldeinformationen bei der APIC-Anwendung an.

Schritt 2: Der Authentifizierungsprozess wird ausgelöst, und die ISE überprüft die Anmeldeinformationen lokal oder über Active Directory.

Schritt 3: Nach erfolgreicher Authentifizierung sendet die ISE ein Erlaubnispaket, um den Zugriff auf den APIC zu autorisieren.

Schritt 4: Die ISE zeigt ein erfolgreiches Authentifizierungs-Liveprotokoll an.

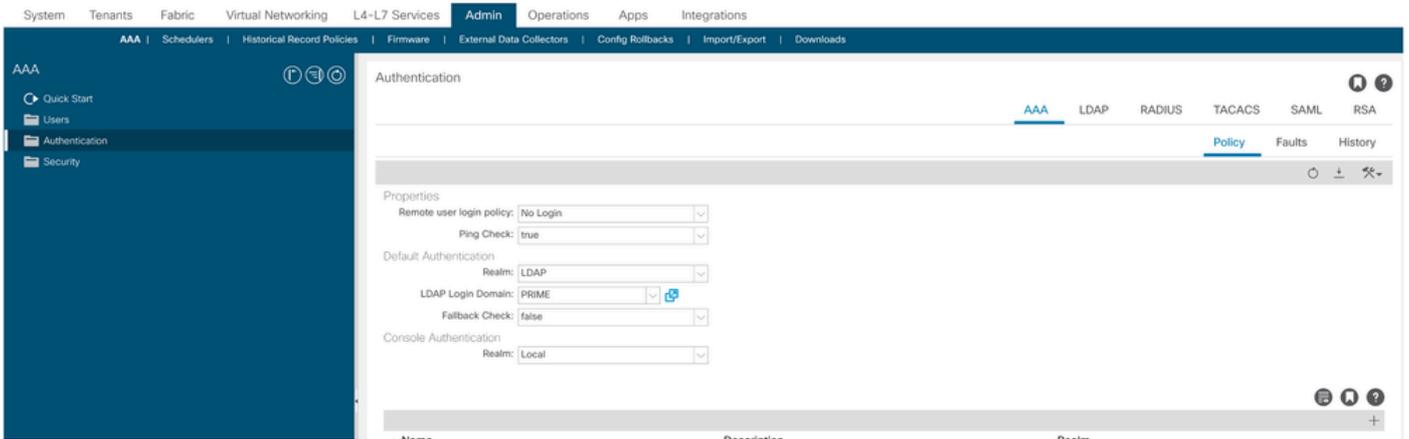
---

 Anmerkung: Der APIC repliziert die TACACS+-Konfiguration auf Leaf-Switches, die Teil der Fabric sind.

---

### APIC-Konfiguration

Schritt 1: Navigieren Sie zu `Admin > AAA > Authentication > AAA+`, und wählen Sie das Symbol aus, um eine neue Anmelde-Domäne zu erstellen.



Administratorkonfiguration für APIC-Anmeldung

Schritt 2. Definieren Sie einen Namen und einen Bereich für die neue Anmeldungsdomäne und klicken Sie unter Anbieter auf , um einen neuen Anbieter zu erstellen. Klicken Sie auf  Anbieter.

## Create Login Domain

? ✕

Name:

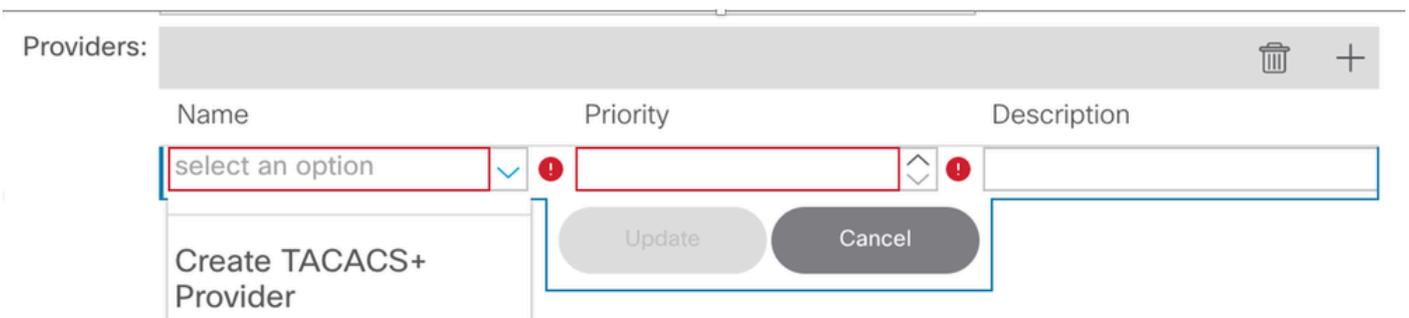
Realm:

Description:

Providers:  

Name	Priority	Description

APIC-Anmeldeadministrator



APIC TACACS-Anbieter

Schritt 3: Definieren Sie die ISE-IP-Adresse oder den Hostnamen, definieren Sie einen

gemeinsamen geheimen Schlüssel, und wählen Sie die Management Endpoint Policy Group (EPG) aus. Klicken Sie, **Submit** um den TACACS+-Anbieter für die Anmeldung als Administrator hinzuzufügen.

## Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol:  CHAP  MS-CHAP  PAP

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring:  Disabled  Enabled

Cancel

Submit

## Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	

### Authentication



AAA   LDAP   RADIUS   **TACACS**   SAML   RSA

Host Name	Description	Port	Timeout (sec)	Retries
52.13.89		49	5	1

TACACS-Anbieteransicht

## ISE-Konfiguration

Schritt 1: Navigieren Sie zu Administration > Network Resources > Network Device Groups. Erstellen Sie unter "Alle Gerätetypen" eine Netzwerk-Gerätegruppe.

# Network Device Groups

[All Groups](#) **Choose group** ▾

[↻](#) **Add**   [Duplicate](#)   [Edit](#)   [🗑️ Trash](#)   [👁️ Show group members](#)   [⬇️ Import](#)   [⬆️ Export](#) ▾   ☰

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▾ All Device Types	All Device Types
<input type="checkbox"/>	APIC	

ISE-Netzwerk-Gerätegruppen

Schritt 2. Navigieren Sie zu Administration > Network Resources > Network Devices. Add Wählen Sie Definieren des APIC-Namens und der IP-Adresse, wählen Sie APIC unter Device Type (Gerätetyp) und TACACS+ (TACACS+) aus, und definieren Sie das Kennwort für die APIC TACACS+ Provider-Konfiguration. Klicken Sie auf .Submit

Network Devices   Network Device Groups   Network Device Profiles   External RADIUS Servers   RADIUS Server

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > APIC-LAB

### Network Devices

Name

Description

IP Address  \* IP :

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location   [Set To Default](#)

IPSEC   [Set To Default](#)

Device Type   [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret  [Show](#) [Retire](#)

Wiederholen Sie die Schritte 1 und 2 für Leaf-Switches.

Schritt 3: Verwenden Sie die Anweisungen auf diesem Link, um die ISE in Active Directory zu integrieren.

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html>



Anmerkung: In diesem Dokument sind interne Benutzer und AD-Administratorgruppen als Identitätsquellen enthalten. Der Test wird jedoch mit der Identitätsquelle der internen Benutzer durchgeführt. Das Ergebnis ist für AD-Gruppen identisch.

---

Schritt 4. (Optional) Navigieren Sie zu **☰** >Administration > Identity Management > Groups. Wählen Sie **User Identity Groups** und klicken Sie auf **Add**. Erstellen Sie eine Gruppe für schreibgeschützte Admin-Benutzer und Admin-Benutzer.

Identity Groups

EQ

< [List Icon] [Settings Icon]

- > Endpoint Identity Groups
- > **User Identity Groups**

# User Identity Groups

[Edit](#) [+ Add](#) [Delete](#) [Import](#) [Export](#)

	Name	Description
<input type="checkbox"/>	ALL_ACCOUNTS (default)	Default ALL_
<input type="checkbox"/>	APIC_RO	<a href="#">i</a>
<input type="checkbox"/>	APIC_RW	

Identitätsgruppe

Schritt 5. (Optional) Navigieren Sie zu ☰ > Klicken Sie auf Administration > Identity Management > Identity., Add und erstellen Sie einen Read Only Admin Benutzer und einen Admin Benutzer. Weisen Sie jeden Benutzer jeder in Schritt 4 erstellten Gruppe zu.

Users

Latest Manual Network Scan Res...

## Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#) [Duplicate](#)

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/>	Enabled	APIC_ROUser				APIC_RO
<input type="checkbox"/>	Enabled	APIC_RWUser				APIC_RW

Schritt 6: Navigieren Sie zu ☰ > Administration > Identity Management > Identity Source Sequence. Wählen Sie Add, definieren Sie einen Namen, und wählen Sie in der Liste AD Join Points und Internal Users Identitätsquelle aus. Wählen Sie Treat as if the user was not found and proceed to the next store in the sequence unter Advanced Search List Settings aus, und klicken Sie auf Save.

∨ Identity Source Sequence

\* Name **APIC\_ISS**

Description

∨ Certificate Based Authentication

Select Certificate Authentication Profile

∨ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints		iselab
Guest Users		Internal Users
All_AD_Join_Points		

Navigation buttons: > < >> << (between columns) and ^ v (within columns)

∨ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Identitätsquellensequenz

>7. Navigieren Sie zu ☰ Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. Wählen

Sie Hinzufügen aus, definieren Sie einen Namen, und deaktivieren Sie CHAP zulassen und MS-CHAPv1 aus der Liste der Authentifizierungsprotokolle zulassen. Wählen Sie Speichern aus.

**Cisco ISE**

Overview Identities User Identity Groups Ext Id Sources Network Resources

Conditions >

Network Conditions >

Results v

Allowed Protocols

TACACS Command Sets

TACACS Profiles

[Allowed Protocols Services List](#) > TACACS Protocol

### Allowed Protocols

Name TACACS Protocol

Description

v Allowed Protocols

#### Authentication Protocols

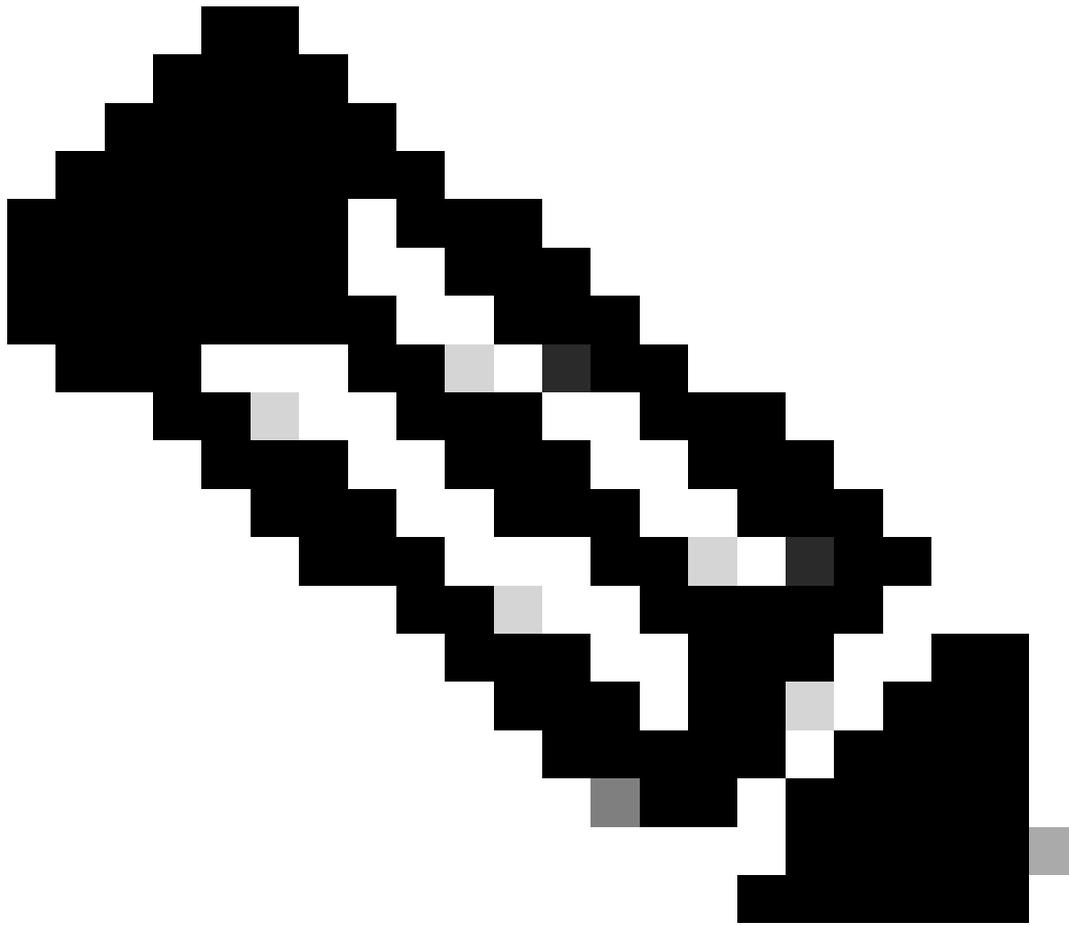
Only Authentication Protocols relevant to TACACS are displayed.

- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1

TACACS-Zulässigkeitsprotokoll

8. Navigieren Sie zu **≡** >Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Klicken Sie auf „add“ und erstellen Sie zwei Profile basierend auf den Attributen in der Liste unter Raw View. Klicken Sie auf „Save“

- Administrator: cisco-av-pair=shell:domains=all/admin/
- Schreibgeschützter Administratorbenutzer: cisco-av-pair=shell:domains=all/read-all



Anmerkung: Bei Leerzeichen oder zusätzlichen Zeichen schlägt die Autorisierungsphase fehl.

---

- Conditions >
- Network Conditions >
- Results ▾
  - Allowed Protocols
  - TACACS Command Sets
  - TACACS Profiles**

[TACACS Profiles](#) > APIC ReadWrite Profile

### TACACS Profile

Name  
**APIC ReadWrite Profile**

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:domains=all/admin/

Cancel
Save

TACACS-Profil

- Overview
- Identities
- User Identity Groups
- Ext Id Sources
- Network Resources**

## TACACS Profiles

Add
Duplicate
Trash ▾
Edit

	Name	Type	Description
<input type="checkbox"/>	APIC ReadOnly Profile	Shell	
<input type="checkbox"/>	APIC ReadWrite Profile	Shell	

TACACS-Admin- und schreibgeschützte Admin-Profile

**Schritt 9:** Navigieren Sie zu **≡ > Work Centers > Device Administration > Device Admin Policy Set**. Erstellen Sie einen neuen Richtlinienatz, definieren Sie einen Namen, und wählen Sie den in Schritt 1 erstellten Gerätetyp **APICaus**. Wählen Sie in Schritt 7. erstellt als zulässiges Protokoll **TACACS Protocolaus**, und klicken Sie auf **Save**.

Policy Sets Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	APIC		DEVICE Device Type EQUALS All Device Types#APIC	TACACS Protocol	55		

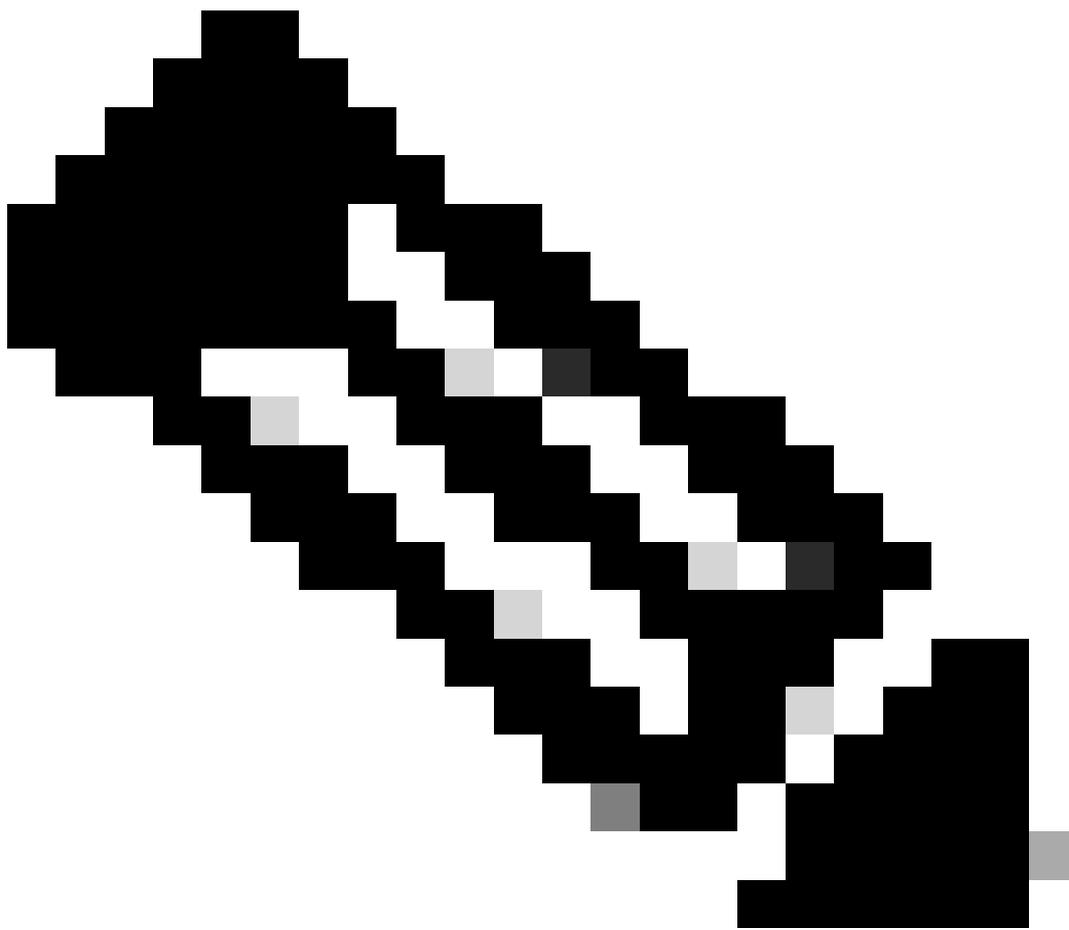
### TACACS-Richtliniensatz

Schritt 10: Klicken Sie unter "NeuPolicy Set" auf den Pfeil nach rechts>, und erstellen Sie eine Authentifizierungsrichtlinie. Definieren Sie einen Namen, und wählen Sie die IP-Adresse des Geräts als Bedingung aus. Wählen Sie dann die in Schritt 6 erstellte Identitätsquellensequenz aus.

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
<span style="color: green;">●</span>	APIC Authentication Policy	Network Access Device IP Address EQUALS 188.21	APIC_ISS	55	Options

### Authentifizierungsrichtlinie



Anmerkung: Location oder andere Attribute können als Authentifizierungsbedingung verwendet werden.

Schritt 11: Erstellen Sie ein Autorisierungsprofil für jeden Admin-Benutzertyp, definieren Sie einen Namen, und wählen Sie einen internen Benutzer und/oder eine AD-Benutzergruppe als Bedingung aus. Es können zusätzliche Bedingungen wie der APIC verwendet werden. Wählen Sie für jede Autorisierungsrichtlinie das passende Shell-Profil aus, und klicken Sie auf **Save**.

Authorization Policy (3)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
ON	APIC Admin RO	AND Network Access Device IP Address EQUALS .188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO		APIC ReadOnly Profile	34	
ON	APIC Admin User	AND OR Network Access Device IP Address EQUALS .188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RW Iselab-ExternalGroups EQUALS cisco:lab/bullfin/Administrators		APIC ReadWrite Profile	16	
ON	Default		DenyAllCommands	Deny All Shell Profile	0	

TACACS-Autorisierungsprofil

## Überprüfung

Schritt 1: Melden Sie sich auf der APIC-Benutzeroberfläche mit den Anmeldeinformationen für den Benutzeradministrator an. Wählen Sie in der Liste die Option TACACS aus.

APIC  
Version 4.2(7u)  
CISCO

User ID  
APIC\_ROUser

Password  
.....

Domain  
S\_TACACS

Login

APIC-Anmeldung

Schritt 2: Überprüfen, ob der Zugriff auf die APIC-Benutzeroberfläche und die Anwendung der richtigen Richtlinien auf die TACACS Live-Protokolle gewährleistet sind

# Welcome to APIC

What's new in version 4.2(7u)



## New Features

- Floating L3out
  - Docker EE (Kubernetes) container integration
  - L4-L7 Services support in vPod
  - Backup PBR destination
  - Support for 64 Remote Leaf pairs
- UI Enhancements:
    - User-defined UI banner
    - First Time Setup wizard
    - Simplified L3Out creation
    - EPG to leafs deployment view

[View Release Notes](#)

### Getting Started

[What's New in v4.2\(7u\)](#)

[Online Videos \(YouTube™\)](#)

[View All Tutorial Videos](#)

### Explore

[Configuration Guides](#)

[Knowledge Base Articles](#)

[APIC Communities](#)

### Support

[Online Help](#)

[Troubleshooting](#)

[Documentation](#)

Do not show on login

[Review First Time Setup](#)

[Get Started](#)

APIC-Willkommensmeldung

Wiederholen Sie die Schritte 1 und 2 für schreibgeschützte Administratorbenutzer.

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
Apr 20, 2023 10:14:42.4...	✓	🔒	APIC_ROUser	Authorizat...	Authentication Policy	Authorization Policy	PAN32	APIC-LAB
Apr 20, 2023 10:14:42.2...	✓	🔒	APIC_ROUser	Authentic...	APIC >> APIC Authentication Po...		PAN32	APIC-LAB

Last Updated: Fri Apr 21 2023 00:14:53 GMT+0200 (Central European Summer Time)

TACACS+ Live-Protokolle

## Fehlerbehebung

Schritt 1: Navigieren Sie zu ☰ > Operations > Troubleshoot > Debug Wizard. Wählen Sie TACACS und klicken Sie auf Debug Nodes.

# Debug Profile Configuration

Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISI

 [Add](#)  [Edit](#)  [Remove](#)  [Debug Nodes](#)

<input type="checkbox"/>	Name	Description	Status
<input type="checkbox"/>	802.1X/MAB	802.1X/MAB	DISABLED
<input type="checkbox"/>	Active Directory	Active Directory	DISABLED
<input type="checkbox"/>	Application Server Issues	Application Server Issues	DISABLED
<input type="checkbox"/>	BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED
<input type="checkbox"/>	Context Visibility	Context Visibility	DISABLED
<input type="checkbox"/>	Guest portal	Guest portal	DISABLED
<input type="checkbox"/>	Licensing	Licensing	DISABLED
<input type="checkbox"/>	MnT	MnT	DISABLED
<input type="checkbox"/>	Posture	Posture	DISABLED
<input type="checkbox"/>	Profiling	Profiling	DISABLED
<input type="checkbox"/>	Replication	Replication	DISABLED
<input checked="" type="checkbox"/>	TACACS	TACACS	DISABLED

Konfiguration des Debugprofils

Schritt 2. Wählen Sie den Knoten, der den Datenverkehr empfängt, und klicken Sie auf **Save**.

Diagnostic Tools   Download Logs   **Debug Wizard**

Debug Profile Configuration  
Debug Log Configuration

Debug Profile Configuration > Debug Nodes

## Debug Nodes

Selected profile TACACS

Choose on which ISE nodes you want to enable this profile.

 Filter  

<input type="checkbox"/>	Host Name	Persona	Role
<input checked="" type="checkbox"/>	PAN32.ciscoise.lab	Administration, Monitoring, Policy Service	PRI(A), PRI(M)
<input type="checkbox"/>	SPAN32.ciscoise.lab	Administration, Monitoring, Policy Service, ...	SEC(A), SEC(M)

[Cancel](#)   [Save](#)

Auswahl der Debug-Knoten

**Schritt 3:** Führen Sie einen neuen Test durch, und laden Sie die Protokolle herunter, Operations > Troubleshoot > Download logs wie folgt:

AcsLogs, 2023-04-20 22:17:16, 866, DEBUG, 0x7f93cab7700, cntx=0004699242, sesn=PAN32/469596415/70, CPMSession

Falls die Debugging-Informationen keine Authentifizierungs- und Autorisierungsinformationen enthalten, überprüfen Sie Folgendes:

1. Der Geräteverwaltungsdienst ist auf dem ISE-Knoten aktiviert.
2. Die richtige ISE-IP-Adresse wurde der APIC-Konfiguration hinzugefügt.
3. Falls sich eine Firewall in der Mitte befindet, stellen Sie sicher, dass Port 49 (TACACS) zulässig ist.

## 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.