

# ISEおよびTACACS+によるデバイス管理用 APICの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[認証手順](#)

[APICの設定](#)

[ISE 設定](#)

[確認](#)

[トラブルシューティング](#)

---

## はじめに

このドキュメントでは、TACACS+プロトコルを使用した管理者ユーザ認証のためにAPICをISEと統合する手順について説明します。

## 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。

- Application Policy Infrastructure Controller ( APIC )
- Identity Services Engine ( ISE )
- TACACSプロトコル

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- APICバージョン4.2(7u)
- ISEバージョン3.2パッチ1

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。

# 設定

## ネットワーク図



統合図


## 認証手順

ステップ1:管理者ユーザクレデンシャルでAPICアプリケーションにログインします。

ステップ 2 : 認証プロセスがトリガーされ、ISEはローカルまたはActive Directoryを介してクレデンシャルを検証します。

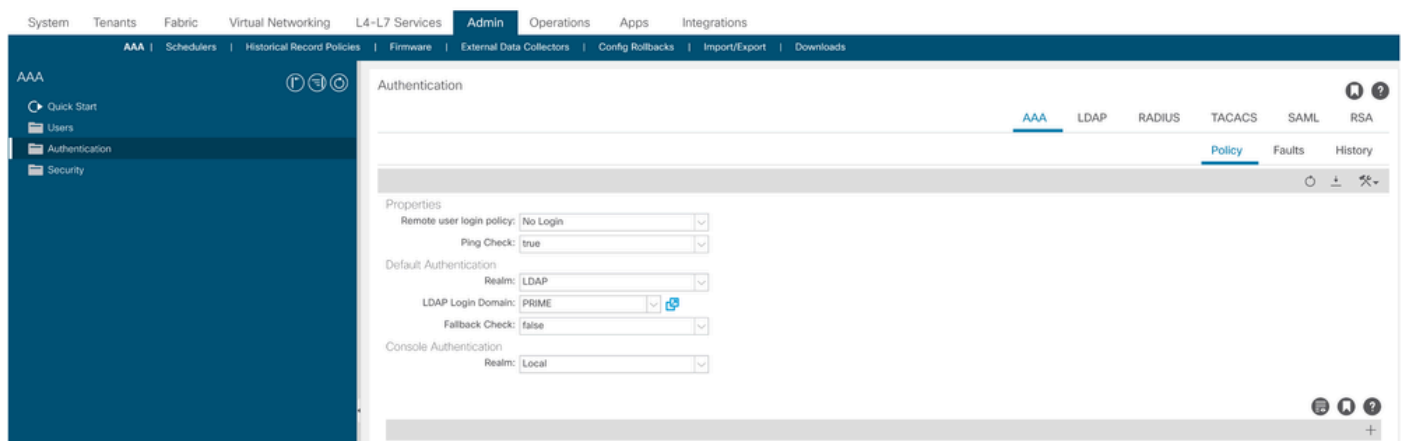
ステップ 3 : 認証が成功すると、ISEはpermitパケットを送信してAPICへのアクセスを許可します。

ステップ 4 : ISEに正常な認証ライブログが表示されます。

 注:APICは、TACACS+の設定をファブリックの一部であるリーフスイッチに複製します。

## APICの設定

ステップ 1 : 新しいログインドメインを作成するには、Admin > AAA > Authentication > AAAに移動して+ iconを選択します。



APICログイン管理の設定

ステップ 2 : 新しいログインドメインの名前とレルムを定義し、Providersの下の+をクリックして新しいプロバイダーを作成します。

## Create Login Domain



Name:

Realm:

Description:

Providers: 

Name	Priority	Description
------	----------	-------------

APICログイン管理者

Providers: 

Name	Priority	Description
<input type="text" value="select an option"/>	<input type="text"/>	<input type="text"/>

Create TACACS+ Provider

APIC TACACSプロバイダー

ステップ 3 : ISEのIPアドレスまたはホスト名を定義し、共有秘密を定義して、管理エンドポイントポリシーグループ(EPG)を選択します。 **Submit** をクリックして、TACACS+プロバイダーをlogin adminに追加します。

## 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

APIC TACACS+プロバイダーの設定値

## Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	

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

TACACSプロバイダービュー

## ISE 設定

ステップ 1 : ≡ > Administration > Network Resources > Network Device Groupsの順に移動します。すべてのデバイスタイプの下にネットワークデバイスグループを作成します。

### ≡ Cisco ISE

Network Devices **Network Device Groups** Network Device Profiles External

## 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ネットワークデバイスグループ

ステップ 2 : **APIC** に移動します。 Administration > Network Resources > Network DevicesAdd define APIC Name and IP addressを選択し、Device Type and TACACS+チェックボックスでAPICを選択し、APIC TACACS+プロバイダー設定で使用するパスワードを定義します。をクリックします。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](#) ⓘ

リーフスイッチに対して、手順1.と手順2.を繰り返します。

ステップ 3 : ISEをActive Directoryと統合するには、このリンクの手順を使用してください。

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html> にアクセスしてください。



注：このドキュメントには、アイデンティティソースとして内部ユーザとAD管理者グループの両方が含まれていますが、テストは内部ユーザのアイデンティティソースを使用して実行されます。結果はADグループでも同じです。

---

ステップ4: ( オプション ) ≡ >Administration > Identity Management > Groups に移動します。を選択しUser Identity Groups で、Addをクリックします。読み取り専用の管理ユーザと管理ユーザ用に1つのグループを作成します。

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	
<input type="checkbox"/> APIC_RW	

IDグループ

ステップ5: ( オプション ) ☰ > Administration > Identity Management > Identity. をクリックし、AddユーザとAdminユーザを1つ作成Read Only Adminします。ステップ4で作成した各グループに各ユーザを割り当てます。

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

手順 6 : ☰ > Administration > Identity Management > Identity Source Sequenceに移動します。Addを選択し、名前を定義して、リストからAD Join PointsとInternal UsersIdentity Sourceを選択します。Treat as if the user was not found and proceed to the next store in the sequenceを選択し、Advanced Search List SettingsSave をクリックします。



∨ Identity Source Sequence

\* Name

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		
	<input type="button" value="&gt;"/> <input type="button" value="&lt;"/> <input type="button" value="&gt;&gt;"/> <input type="button" value="&lt;&lt;"/>	<input type="button" value="↑"/> <input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="↓"/>

∨ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

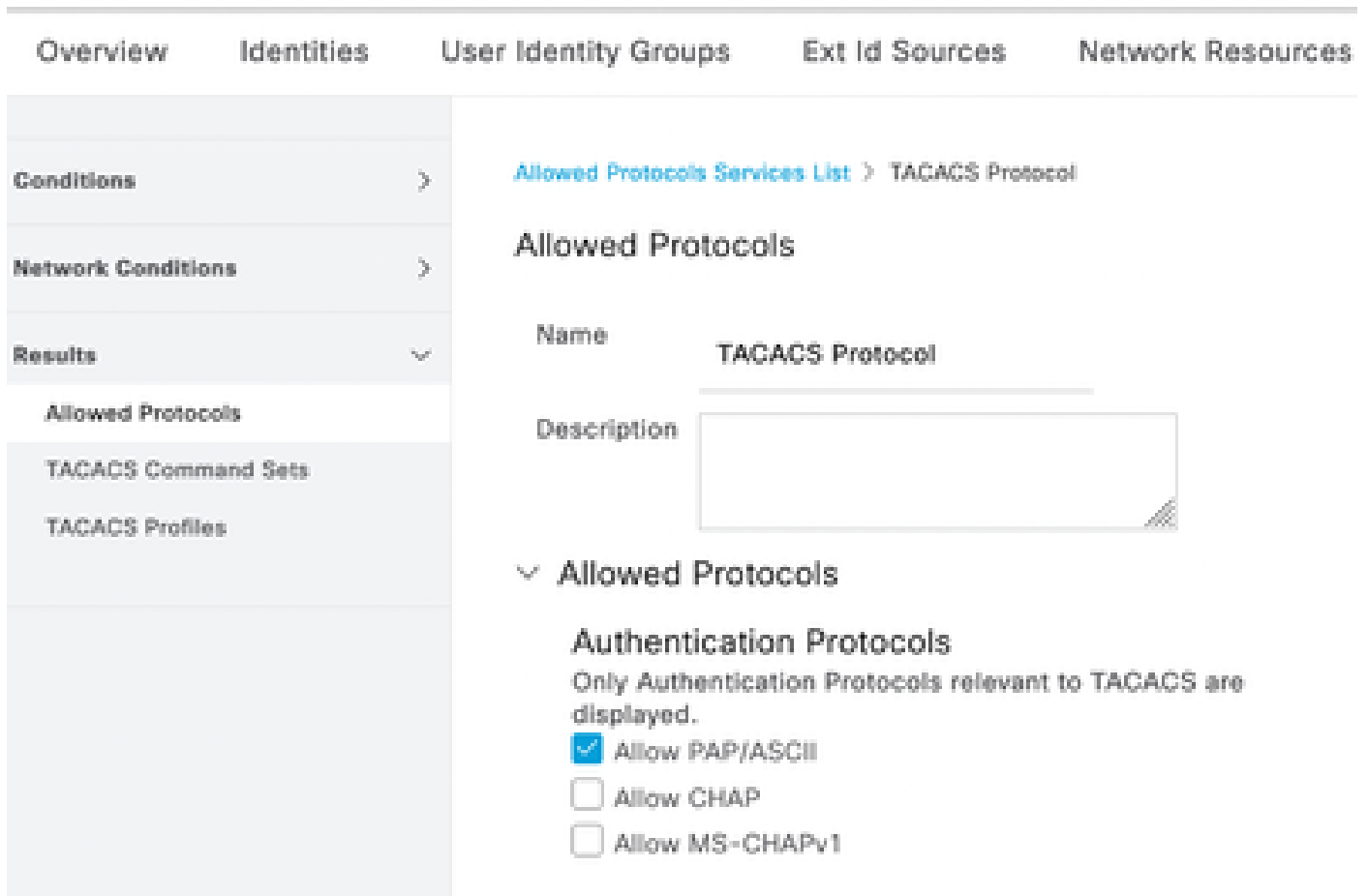
- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

IDソースシーケンス

7. ☰>Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. に移動し、Select Addを選

択して、名前を定義し、Allow CHAPvとAllow MS-CHAPv1 from Authentication protocol listのチェックマークを外します。[Save] を選択します。

## ☰ Cisco ISE



Overview Identities User Identity Groups Ext Id Sources Network Resources

Conditions >

Network Conditions >

Results ▾

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Allowed Protocols Services List > TACACS Protocol

### Allowed Protocols

Name TACACS Protocol

Description

▾ Allowed Protocols

#### Authentication Protocols

Only Authentication Protocols relevant to TACACS are displayed.

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

TACACS許可プロトコル

8. ☰ > Work Centers > Device Administration > Policy Elements > Results > TACACS Profileに移動します。addをクリックし、Raw Viewの下のリストにある属性に基づいて2つのプロファイルを作成します。をクリックします。Save

- 管理者ユーザ : cisco-av-pair=shell:domains=all/admin/
- 読み取り専用管理ユーザ : cisco-av-pair=shell:domains=all/read-all



注：スペースまたは追加の文字が含まれている場合、認証フェーズは失敗します。

---

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Administration

Conditions > 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プロファイル

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

## TACACS Profiles

[Refresh](#) [Add](#) [Duplicate](#) [Trash](#) [Edit](#)

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

TACACS AdminおよびReadOnly Adminプロファイル

ステップ9: ≡ > Work Centers > Device Administration > Device Admin Policy Setに移動します。新しいポリシーセットを作成し、名前を定義して、手順1で作成しAPICなデバイスタイプを選択します。許可されたプロトコルとして、ステップ7で作成したTACACS Protocolを選択し、Saveをクリックします。

Policy Sets

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

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	APIC		DEVICE-Device Type EQUALS All Device Types#APIC	TACACS Protocol	55		

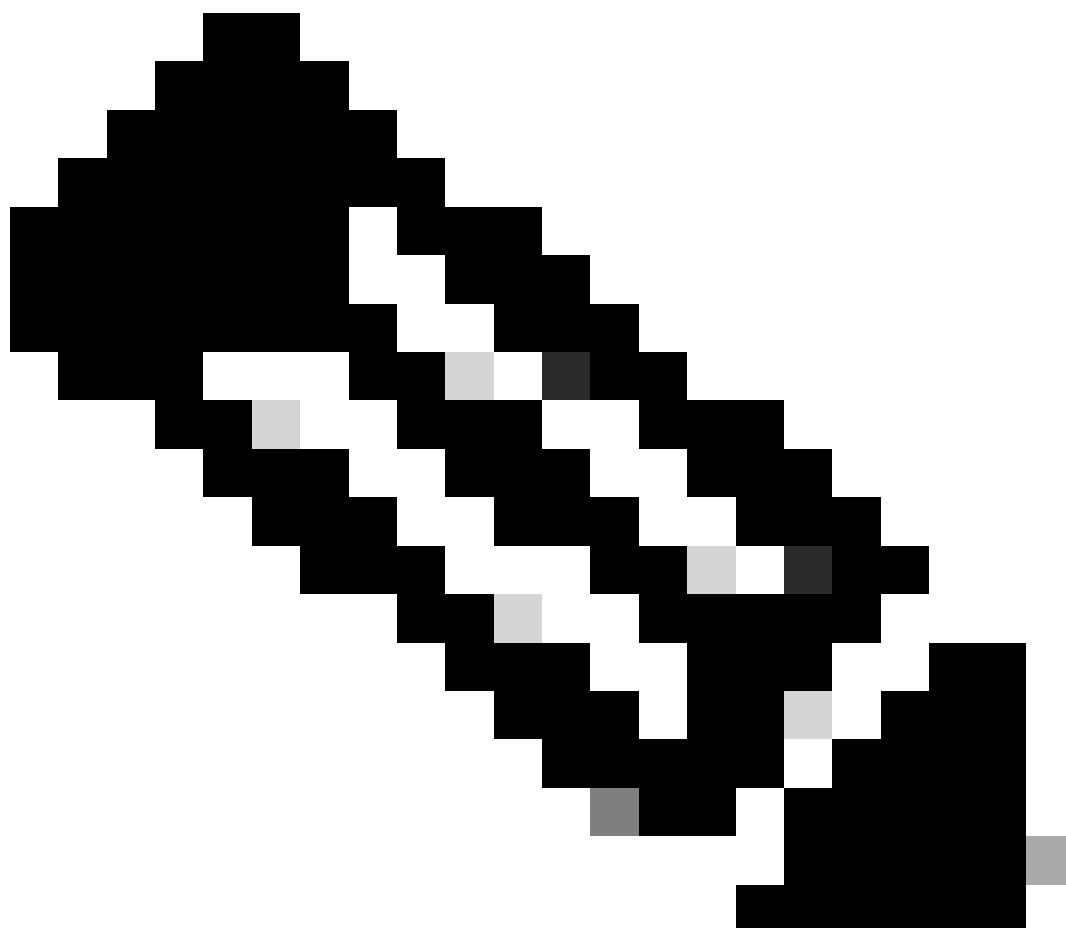
## TACACSポリシーセット

ステップ 10 : [new Policy Set]で右矢印をクリックし、認証ポリシーを作成します。名前を定義し、条件としてデバイスのIPアドレスを選択します。次に、ステップ6で作成したアイデンティティソースシーケンスを選択します。

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	APIC Authentication Policy	Network Access Device IP Address EQUALS 188.21	APIC_ISS	55	Options

## 認証ポリシー





注:Locationまたはその他の属性は認証条件として使用できます。

ステップ 11各管理者ユーザタイプの認可プロファイルを作成し、名前を定義し、条件として内部ユーザまたはADユーザグループ (あるいはその両方) を選択します。APICなどの追加条件を使用できます。各認可ポリシーで適切なシェルプロファイルを選択し、Saveをクリックします。

Authorization Policy (3)

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles	Hits	Actions
●	APIC Admin RO	AND Network Access Device IP Address EQUALS .188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO			APIC ReadOnly Profile		
●	APIC Admin User	AND Network Access Device IP Address EQUALS .188.21 OR IdentityGroup-Name EQUALS User Identity Groups:APIC_RW IsLab-ExternalGroups EQUALS ciscoise.lab/Bulltin/Administrators			APIC ReadWrite Profile	18	
●	Default			DenyAllCommands	Deny All Shell Profile		

TACACS許可プロファイル

## 確認

ステップ 1 : ユーザ管理者クレデンシャルを使用してAPIC UIにログインします。リストからTACACSオプションを選択します。

APIC  
Version 4.2(7u)  
CISCO

User ID  
APIC\_ROUser

Password  
.....

Domain  
S\_TACACS

Login

APICログイン

ステップ 2 : APIC UIでアクセスを確認し、TACACSライブログに適切なポリシーが適用されていることを確認します。

# 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ウェルカムメッセージ

読み取り専用管理ユーザに対して手順1と2を繰り返します。

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To ▾

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
×	▾		Identity	▾	Authentication Policy	Authorization Policy	Ise Node	Network Device N...
Apr 20, 2023 10:14:42.4...	✔	🔒	APIC_ROUser	Authorizat...		APIC >> APIC Admin RO	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+ライブログ

## トラブルシューティング

ステップ 1 : ☰ > Operations > Troubleshoot > Debug Wizardに移動します。TACACSを選択し、Debug Nodesをクリックします。

# 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

プロファイル設定のデバッグ

ステップ 2 : トラフィックを受信するノードを選択し、Save をクリックします。



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](#)

デバッグノードの選択

ステップ 3 : 新しいテストを実行し、次の Operations > Troubleshoot > Download logs の下のログをダウンロードします。

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

デバッグで認証と認可の情報が表示されない場合は、次を検証します。

1. Devices Administration サービスが ISE ノードで有効になっている。
2. 正しい ISE IP アドレスが APIC 設定に追加されました。
3. ファイアウォールが中央にある場合は、ポート 49 (TACACS) が許可されていることを確認します。

## 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。