

# ISEを使用したAristaスイッチでのTACACS+認証の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ISEでのTACACS+の設定](#)

[Aristaスイッチの設定](#)

[ステップ 1: TACACS+認証の有効化](#)

[ステップ 2: 設定の保存](#)

[確認](#)

[ISEのレビュー](#)

[トラブルシューティング](#)

[問題 1](#)

[考えられる原因](#)

[問題 2](#)

[考えられる原因](#)

[解決方法](#)

---

## はじめに

このドキュメントでは、Cisco ISE TACACS+をAristaスイッチと統合して、管理者アクセスのAAAを一元化する方法について説明します。

## 前提条件

次の項目に関する知識があることが推奨されます。

- Cisco ISEおよびTACACS+プロトコル。
- Aristaスイッチ

## 使用するコンポーネント

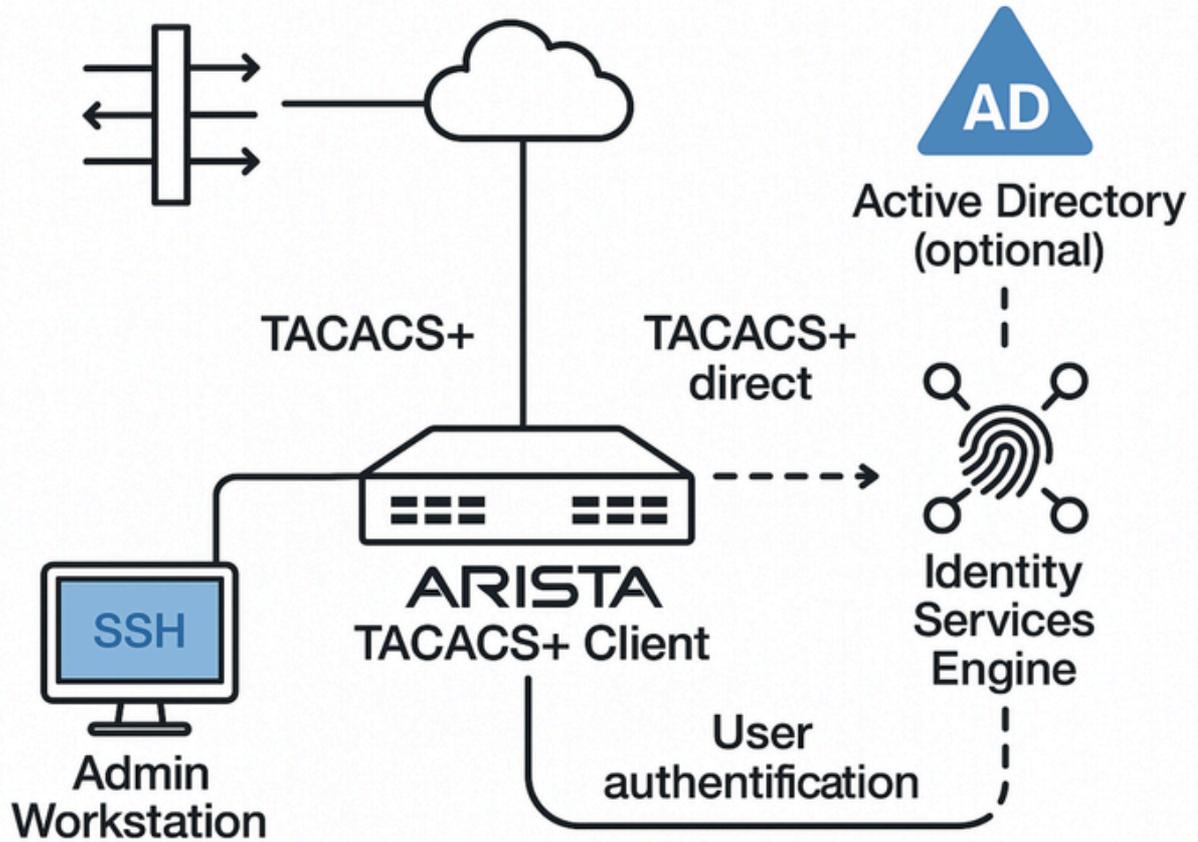
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Aristaスイッチソフトウェアイメージバージョン：4.33.2F
- Cisco Identity Services Engine(ISE)バージョン3.3パッチ4

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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください

## ネットワーク図

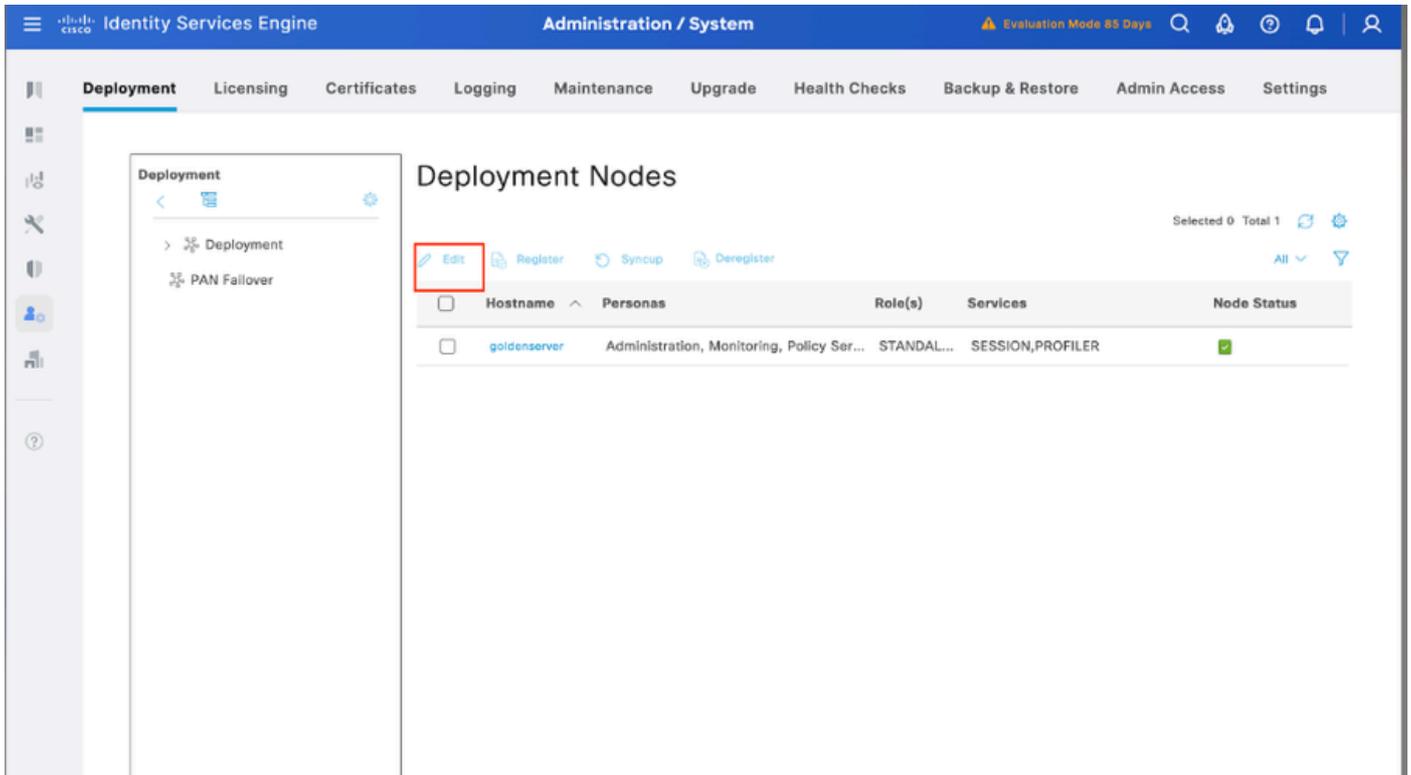


## コンフィギュレーション

### ISEでのTACACS+の設定

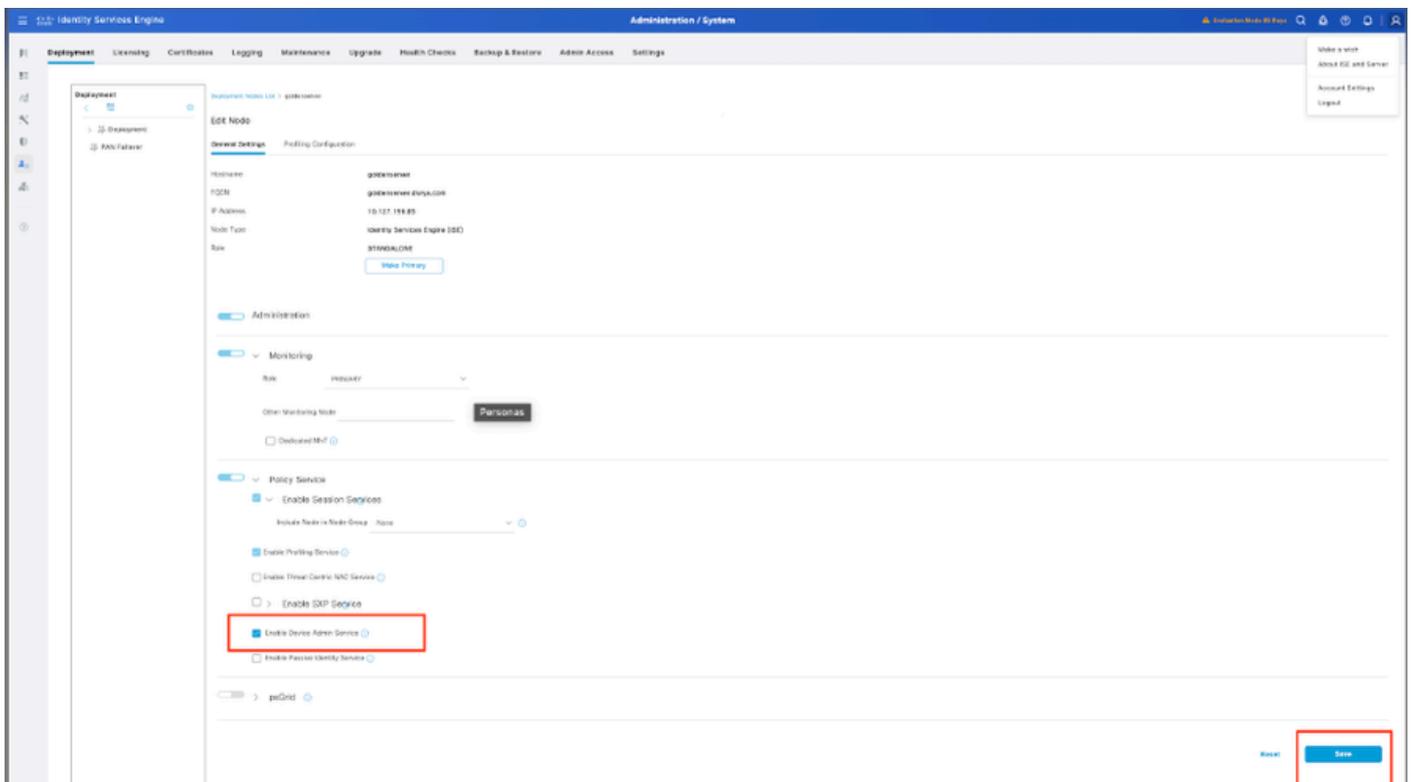
ステップ 1：最初に、Cisco ISEにTACACS+認証を処理するために必要な機能があるかどうかを確認します。これを行うには、目的のポリシーサービスノード(PSN)でデバイス管理サービス機能が有効になっていることを確認します。

Administration > System > Deploymentの順に移動し、ISEがTACACS+認証を処理する適切なノードを選択し、Editをクリックして設定を確認します。



ステップ 2 : 下にスクロールして、Device Administration Service機能を見つけます。この機能を有効にするには、ポリシーサービスのペルソナがノード上でアクティブであり、展開内で使用可能なTACACS+ライセンスが存在している必要があります。

チェックボックスをオンにして機能を有効にし、設定を保存します。

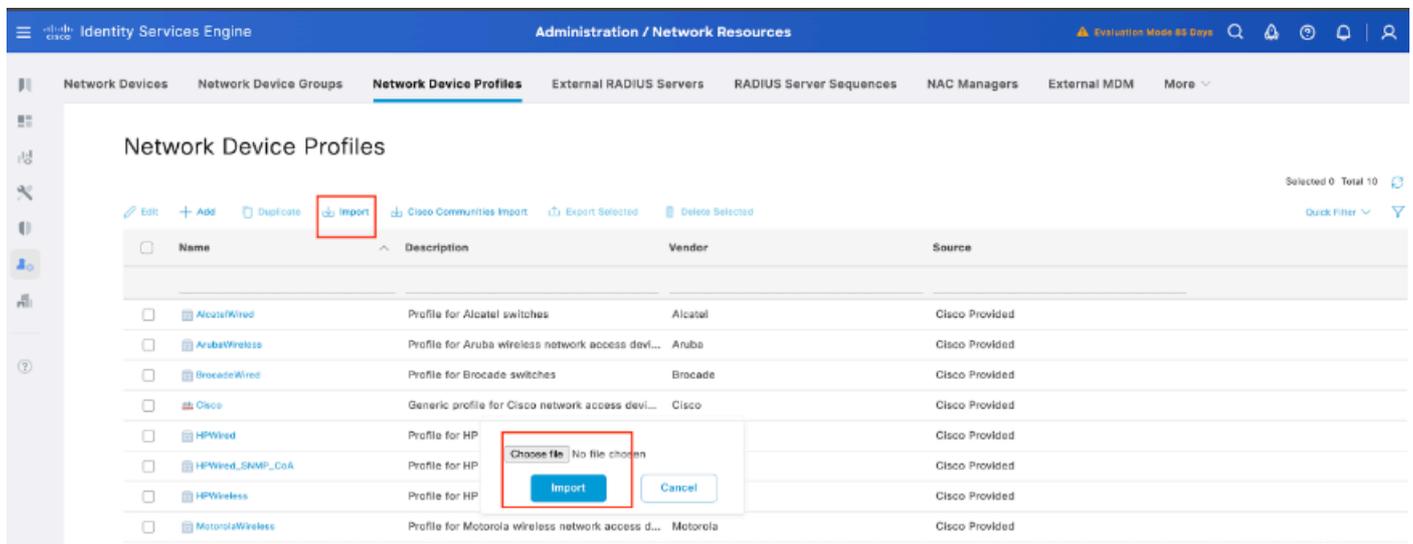


ステップ 3 : Cisco ISEのAristaネットワークデバイスプロファイルの取得

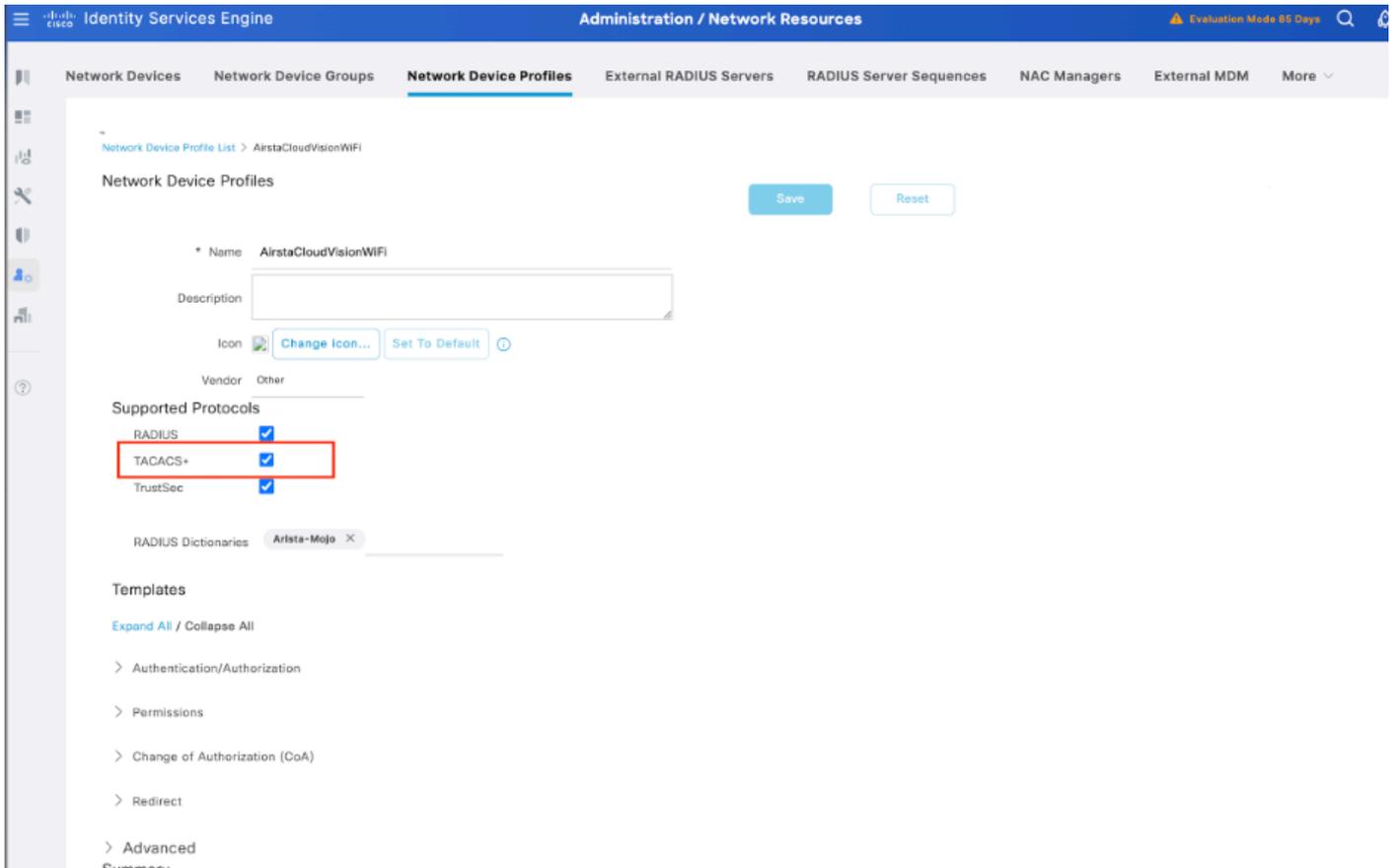
シスココミュニティは、Aristaデバイス専用のNADプロファイルを共有しています。このプロファイルと必要な辞書ファイルについては、『[Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration](#)』を参照してください。このプロファイルをダウンロードしてISE設定にインポートすると、統合が円滑になります

Arista NADプロファイルをCisco ISEにインポートする手順：

1. プロファイルをダウンロードします。
  - Arista NADプロファイルは、上記のシスココミュニティリンクから取得します。[シスココミュニティ](#)
2. Cisco ISEへのアクセス：
  - Cisco ISE管理コンソールにログインします
3. NADプロファイルをインポートします。
  - Administration > Network Resources > Network Device Profilesの順に選択します
  - [インポート]ボタンをクリックします。
  - ダウンロードしたArista NADプロファイルファイルをアップロードします。

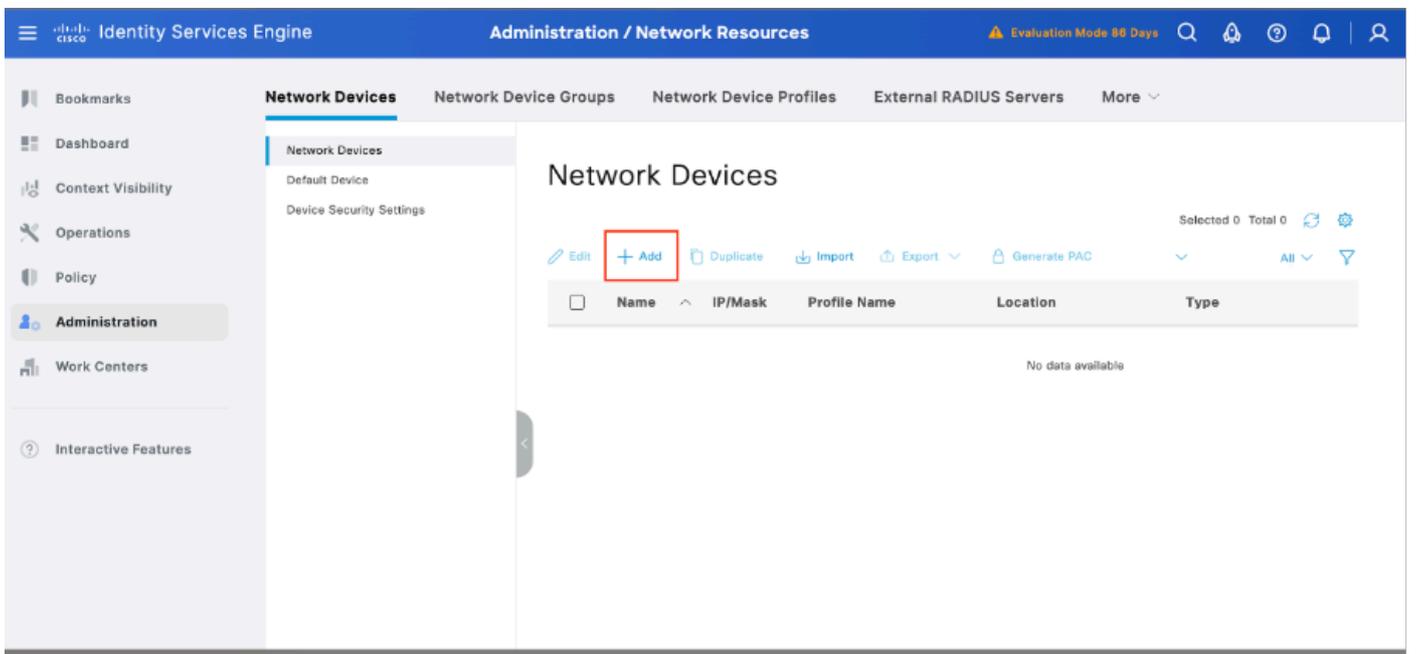


アップロードが完了したら、Editオプションに移動し、サポートされているプロトコルとしてTACACS+を有効にします。



ステップ2：ネットワークデバイスとしてAristaスイッチを追加します。

1. Administration > Network Resources > Network Devices> +Addの順に移動します。

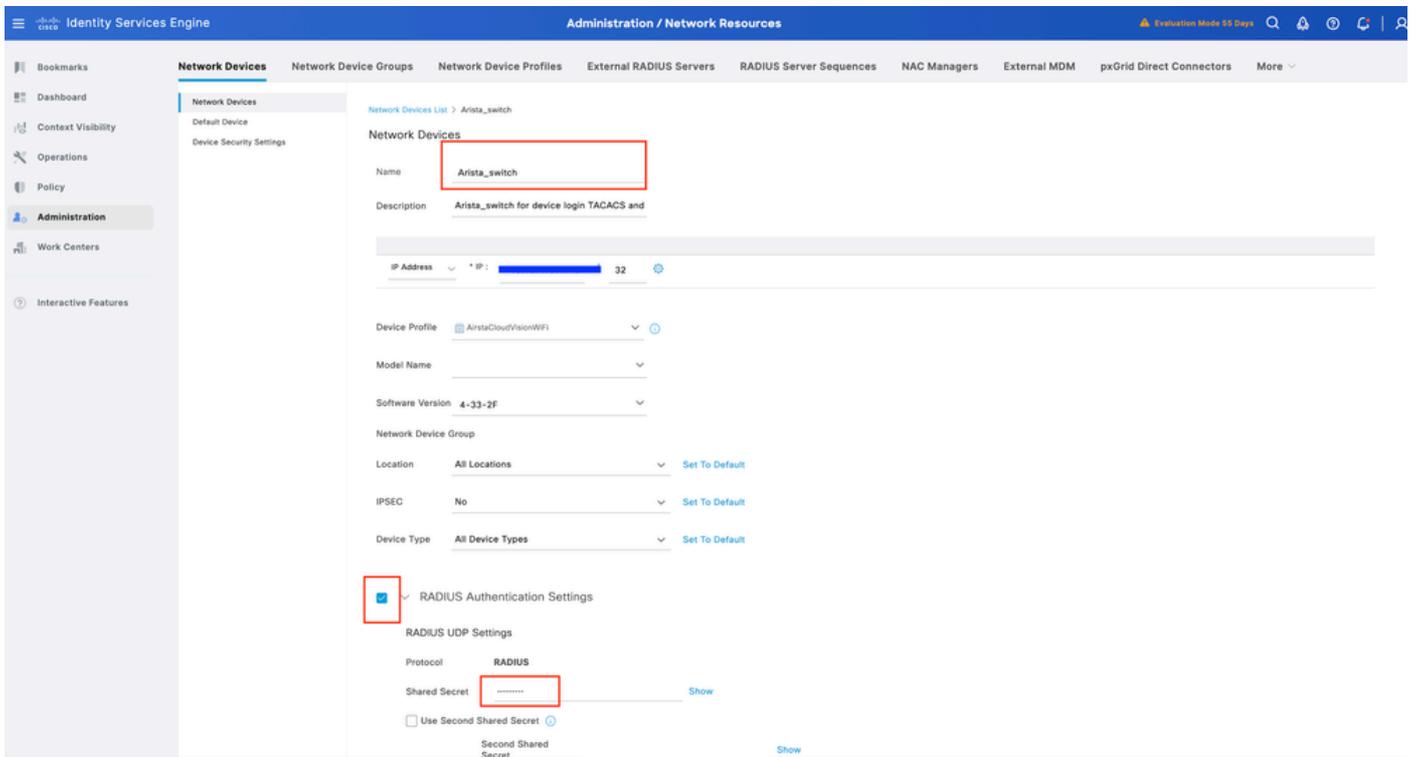


2. Addをクリックして、次の詳細情報を入力します。

- IPアドレス: <Switch-IP>
- デバイスタイプ：他の有線を選択
- Network Device Profile:AirstaCloudVisionWiFiを選択します。

- RADIUS認証設定:
  - RADIUS認証を有効にします。
  - 共有秘密を入力します (スイッチ設定と一致している必要があります)。

3. Saveをクリックします。

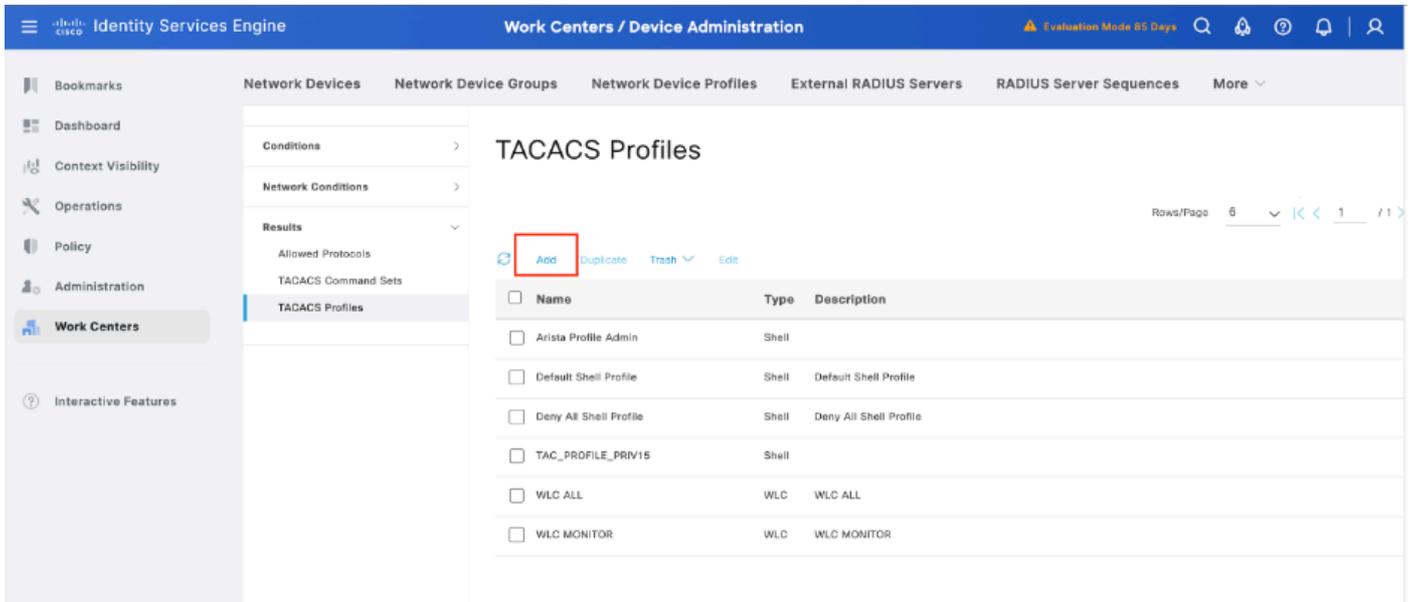


ステップ 3 : 新しいデバイスがNetwork Devicesの下に表示されていることを確認します。

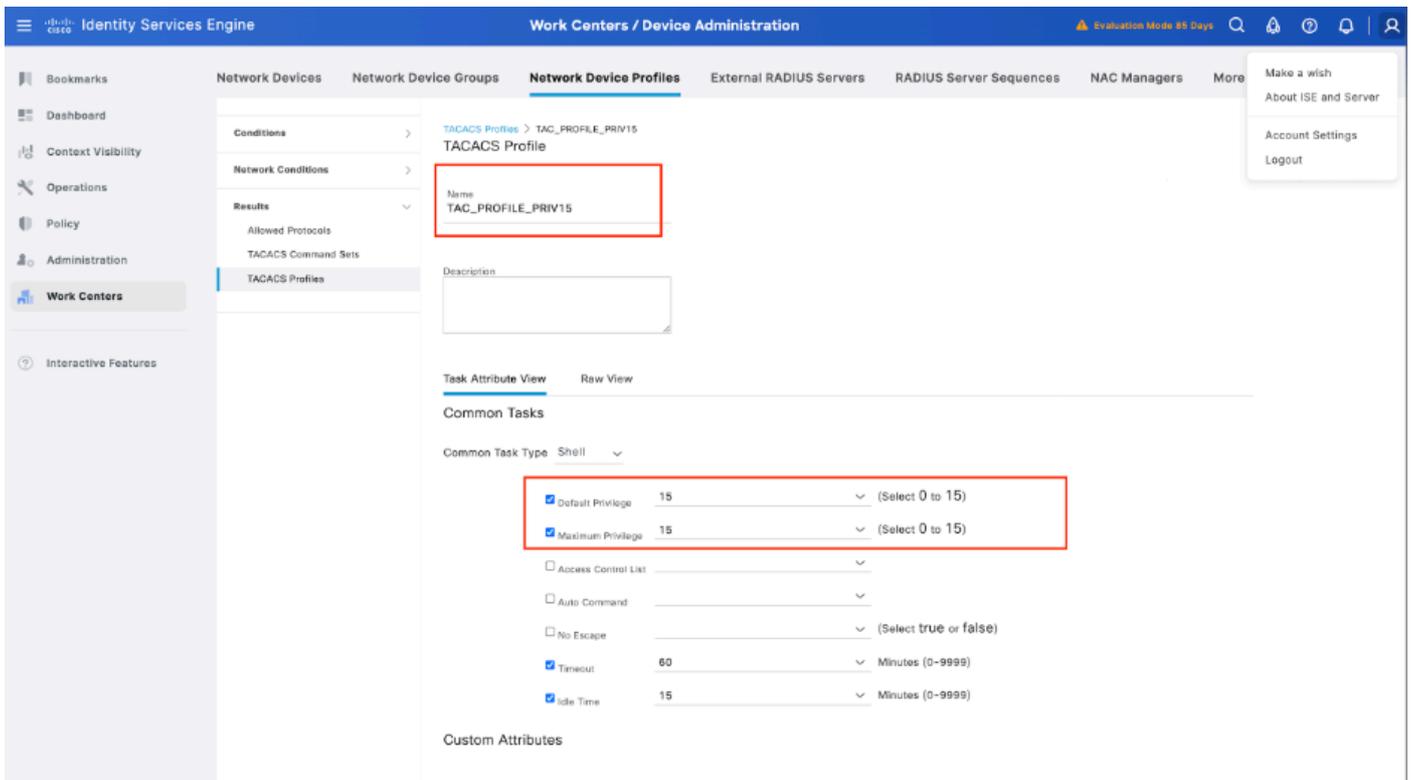


ステップ 4 : TACACSプロファイルを設定します。

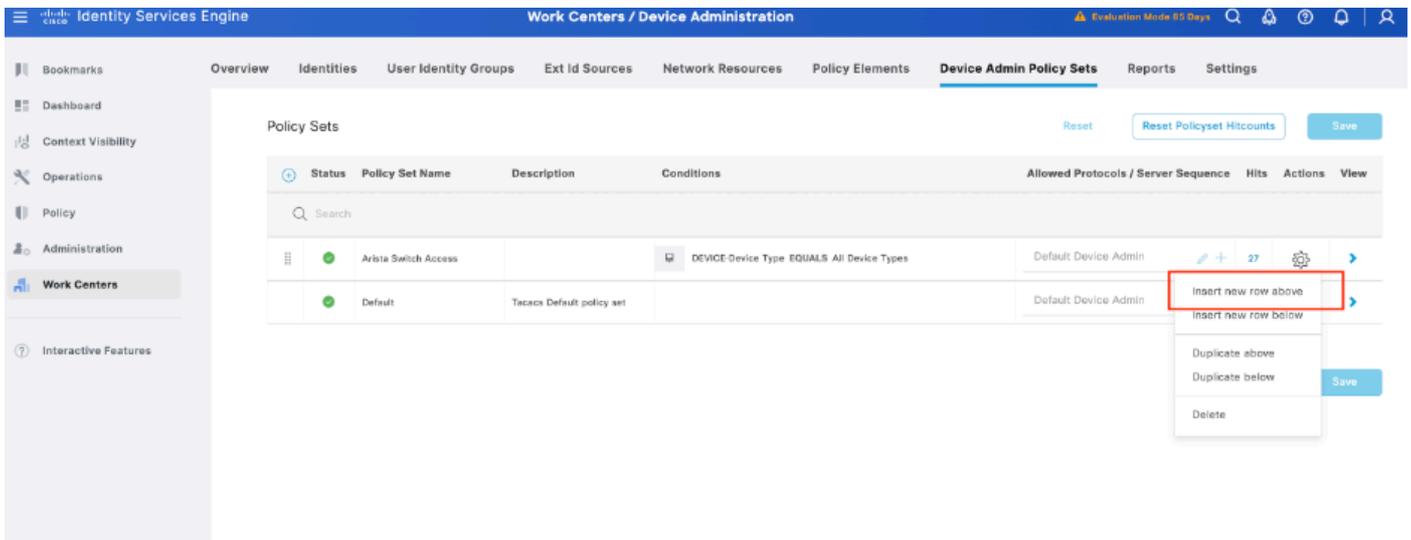
TACACSプロファイルを作成し、Work Centers > Device Administration > Policy Elements > Results > TACACS Profilesの順にメニューに移動して、Addを選択します。



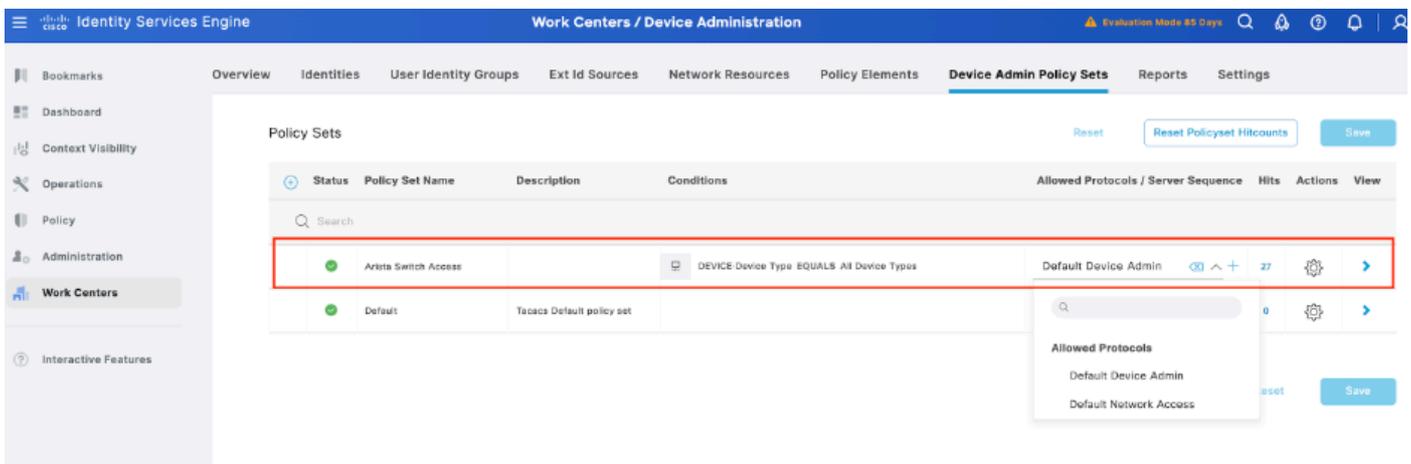
名前を入力し、「デフォルト権限」チェックボックスを選択し、値を15に設定します。さらに、Maximum Privilegeを選択し、その値を15に設定して、Submitをクリックします。



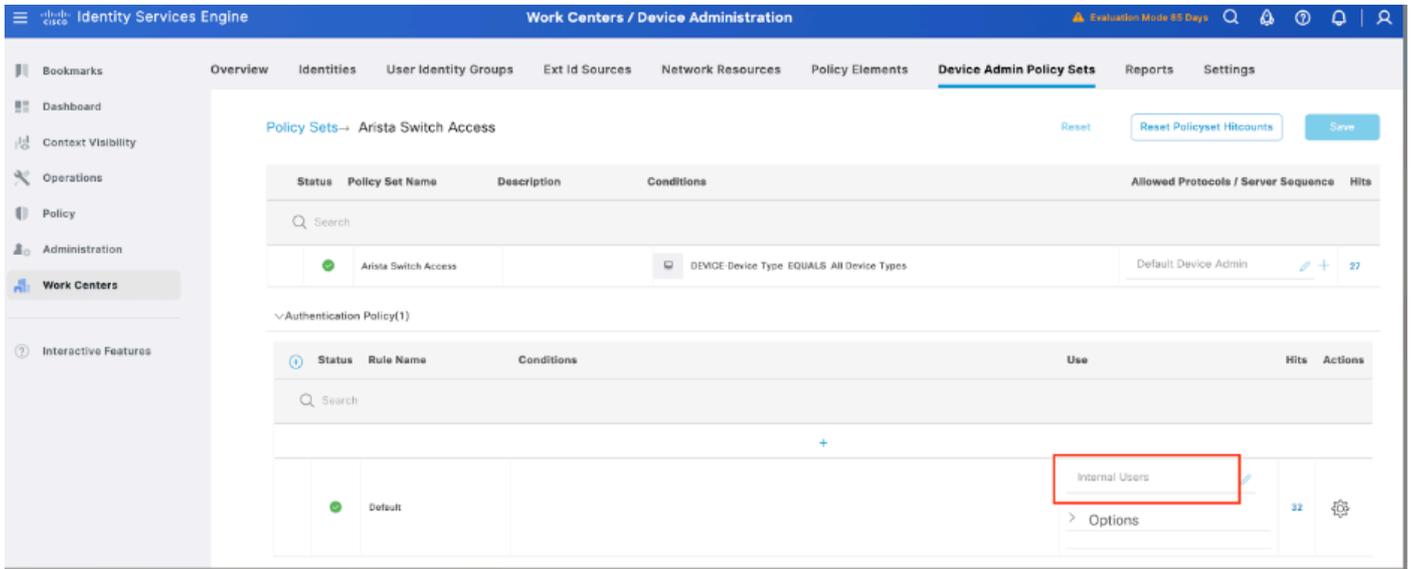
ステップ 5 : Aristaスイッチで使用するデバイス管理ポリシーセットを作成し、ワークセンター>デバイス管理>デバイス管理ポリシーセットの順にメニューに移動します。既存のポリシーセットから歯車のアイコンを選択し、上の新しい行を挿入を選択します。



手順 6 : この新しいポリシーセットに名前を付け、Aristaスイッチから実行されている TACACS+認証の特性に応じて条件を追加し、Allowed Protocols > Default Device Adminの順に選択して、設定を保存します。

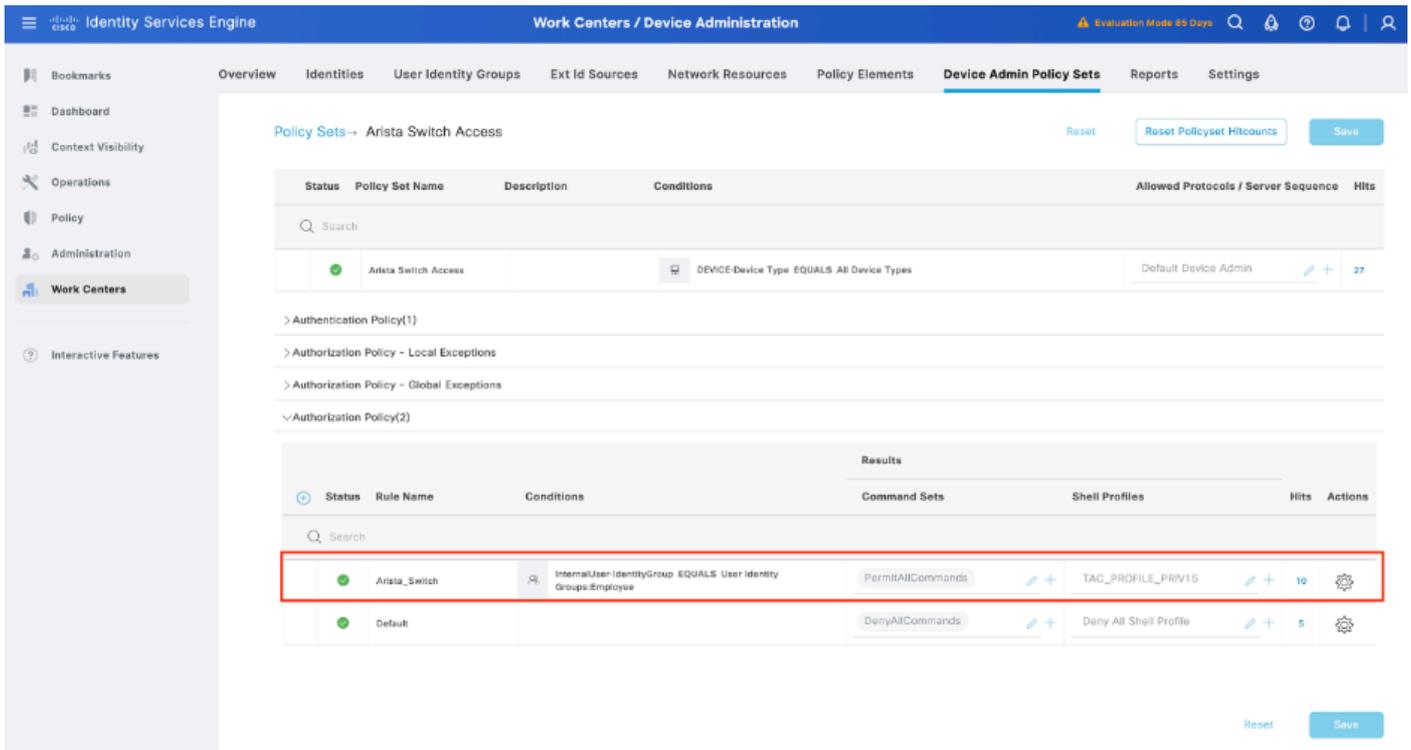


手順 7 : > viewオプションを選択してから、Authentication Policyセクションで、Aristaスイッチの認証用のユーザ名とクレデンシャルを照会するためにCisco ISEが使用する外部アイデンティティソースを選択します。この例では、クレデンシャルはISE内に保存された内部ユーザに対応します。



ステップ 8： Authorization PolicyというセクションがDefault policyになるまでスクロールダウンして、歯車のアイコンを選択し、上にルールを1つ挿入します。

ステップ 9： 新しい認可ルールに名前を付け、グループメンバーシップとして認証済みのユーザーに関する条件を追加します。次に、Shell Profilesセクションで、以前に設定したTACACSプロファイルを追加し、設定を保存します。



## Aristaスイッチの設定

ステップ 1： TACACS+認証の有効化

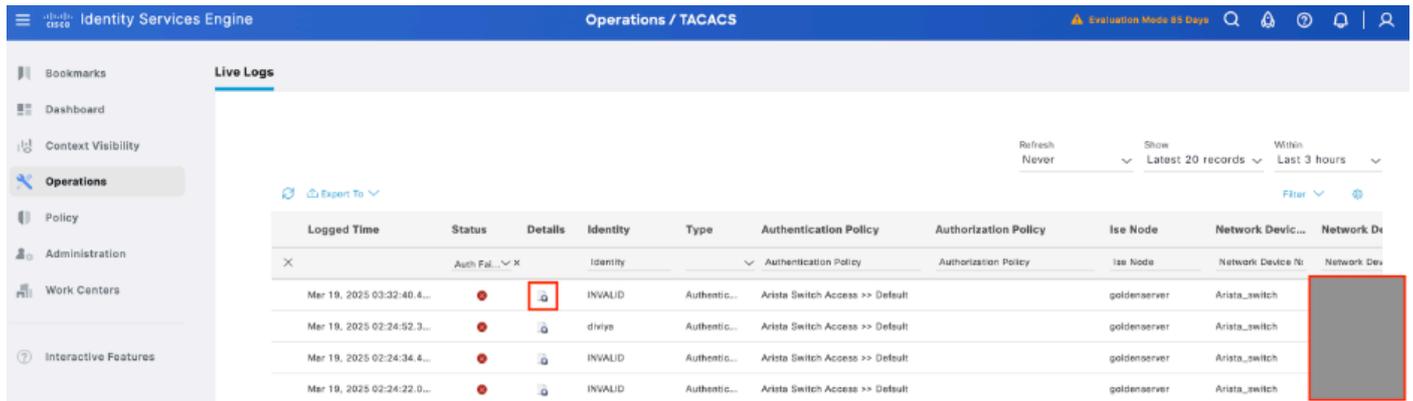
Aristaスイッチにログインし、設定モードに入ります。

設定



Operations > TACACS > Live logsのメニューで確認できます。

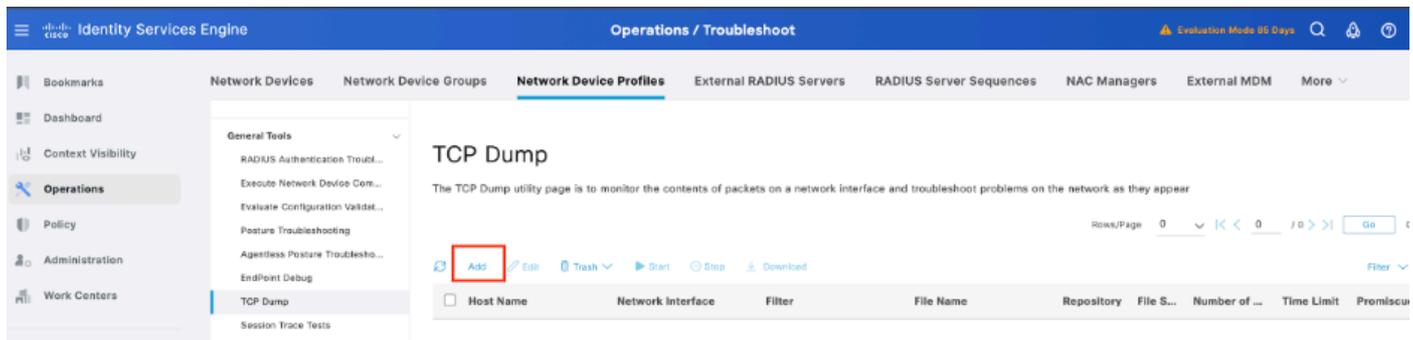
障害の原因に応じて、設定を調整したり、障害の原因に対処したりできます。



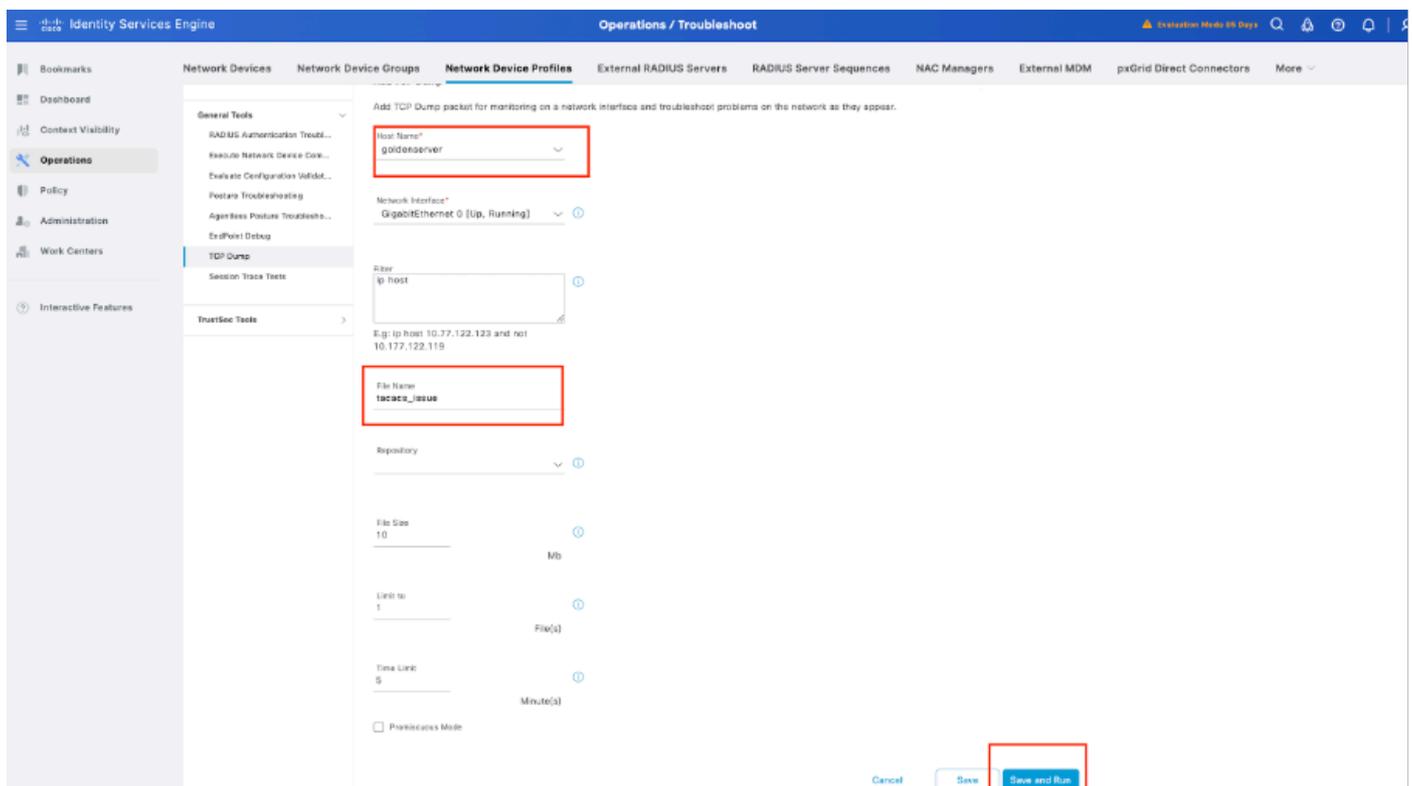
The screenshot shows the 'Live Logs' page in the Identity Services Engine. The table displays log entries with columns for Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, and Network Device. A red box highlights the 'Details' column for the first entry, which shows a lock icon and the text 'Auth Fail... X'. Another red box highlights the 'Network Device' column for the same entry, which shows 'Arista\_switch'.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network De
Mar 19, 2025 03:32:40.4...	●	Auth Fail... X	INVALID	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	
Mar 19, 2025 02:24:52.3...	●		diviya	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:24:34.4...	●		INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:24:22.0...	●		INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	

手順 3：ライブログが表示されない場合は、パケットキャプチャに進みます。Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dumpの順にメニューに移動し、Addを選択します。

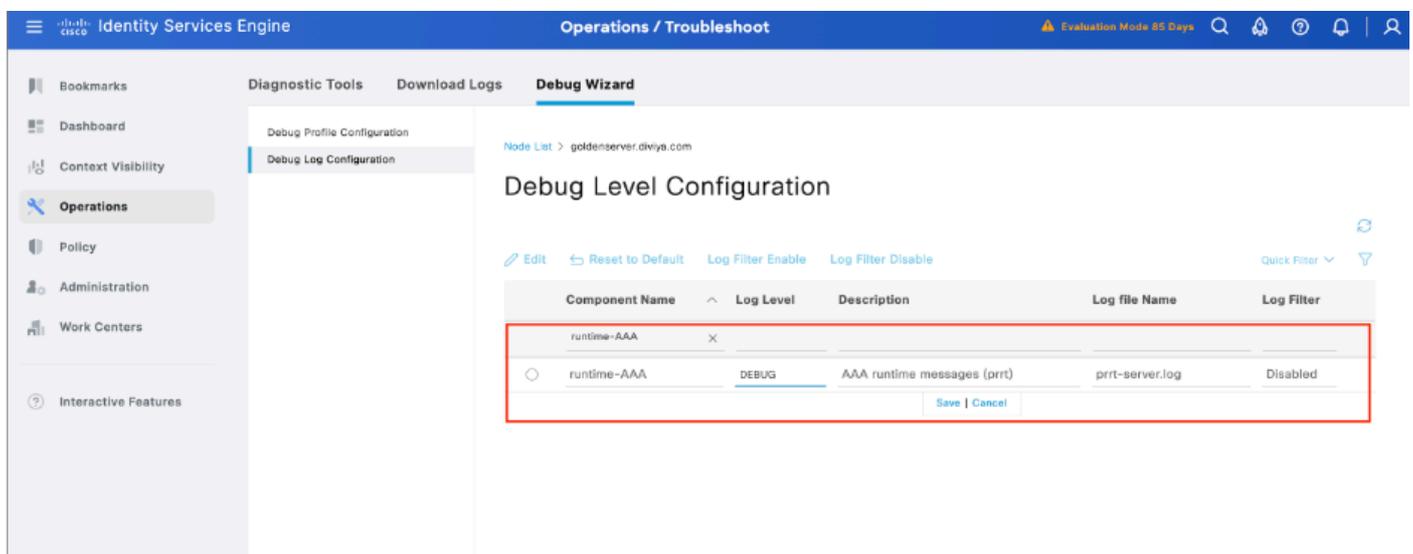
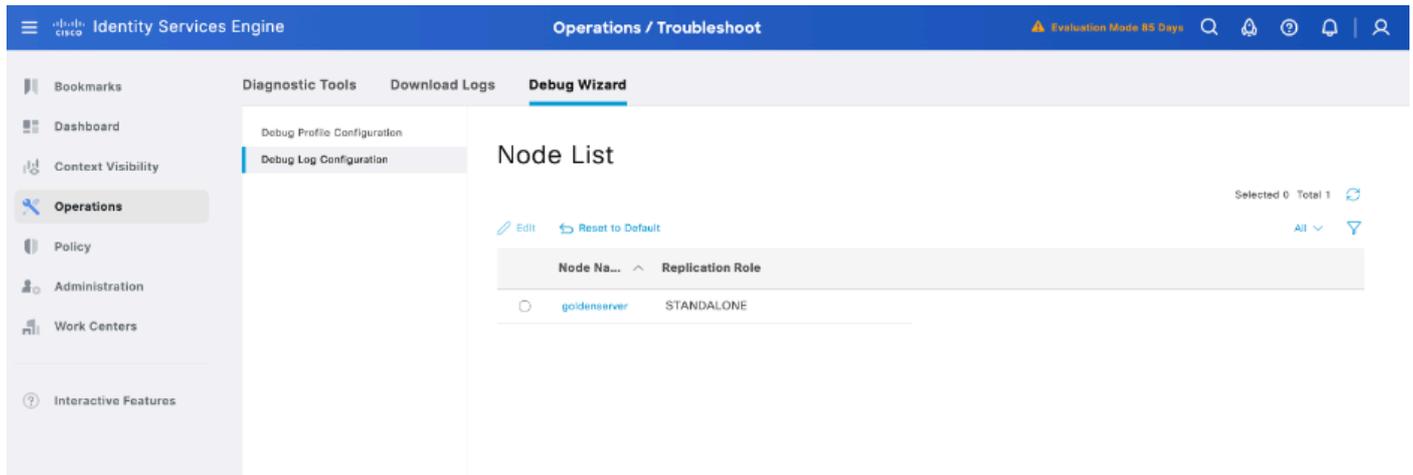


The screenshot shows the 'TCP Dump' page in the Identity Services Engine. The page title is 'TCP Dump' and it includes a description: 'The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear'. There are controls for 'Rows/Page' (0) and 'Go'. A red box highlights the 'Add' button. Below the button is a table with columns: Host Name, Network interface, Filter, File Name, Repository, File S..., Number of ..., Time Limit, and Promiscu.



The screenshot shows the configuration page for the 'TCP Dump' utility. The page title is 'Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.' There are several input fields and dropdown menus. A red box highlights the 'Host Name' dropdown menu, which is set to 'goldenserver'. Another red box highlights the 'File Name' input field, which contains the text 'tacacs\_issue'. At the bottom right, there are buttons for 'Cancel', 'Save', and 'Save and Run'.

ステップ 4 : Operations > Troubleshoot > Debug Wizard > Debug log configurationの順に選択し、PSN nodeを選択してから、Editボタンを選択して、認証の実行元PSN内のデバッグでコンポーネントruntime-AAAを有効にします。



runtime-AAAコンポーネントを特定し、そのログレベルをdebugに設定し、問題を再現し、さらに調査するためにログを分析します。

## トラブルシューティング

### 問題 1

Cisco ISEとAristaスイッチ（または任意のネットワークデバイス）の間のTACACS+認証が失敗し、次のエラーメッセージが表示されます。

「選択13036たシェルプロファイルはDenyAccessです」

Overview		Steps	
Request Type	Authentication	13013	Received TACACS+ Authentication START Request
Status	Fail	15049	Evaluating Policy Group (🔴 Step latency=1ms)
Session Key	goldenserver/541265148/80	15008	Evaluating Service Selection Policy (🔴 Step latency=0ms)
Message Text	Failed-Attempt: Authentication failed	15048	Queried PIP - DEVICE.Device Type (🔴 Step latency=2ms)
Username	diviya	15041	Evaluating Identity Policy (🔴 Step latency=3ms)
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth	15048	Queried PIP - Network Access.Protocol (🔴 Step latency=2ms)
Selected Authorization Profile	Deny All Shell Profile	15013	Selected Identity Source - Internal Users (🔴 Step latency=2ms)
		24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
		24212	Found User in Internal Users IDStore (🔴 Step latency=37ms)
		13045	TACACS+ will use the password prompt from global TACACS+ configuration (🔴 Step latency=0ms)
		13015	Returned TACACS+ Authentication Reply (🔴 Step latency=0ms)
		13014	Received TACACS+ Authentication CONTINUE Request (🔴 Step latency=68ms)
		15041	Evaluating Identity Policy (🔴 Step latency=0ms)
		15013	Selected Identity Source - Internal Users (🔴 Step latency=4ms)
		24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
		24212	Found User in Internal Users IDStore (🔴 Step latency=7ms)
		22037	Authentication Passed (🔴 Step latency=0ms)
		15036	Evaluating Authorization Policy (🔴 Step latency=0ms)
		15048	Queried PIP - Network Access.UserName (🔴 Step latency=4ms)

Authentication Details	
Generated Time	2025-07-27 16:06:30.094000 +05:30
Logged Time	2025-07-27 16:06:30.094
Epoch Time (sec)	1753612590
ISE Node	goldenserver
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for this request
Username	diviya

Cisco ISEのエラー「13036 Selected Shell Profile is DenyAccess」は通常、TACACS+デバイス管理試行時に、認可ポリシーがDenyAccessに設定されたシェルプロファイルに一致したことを意味します。これは通常、シェルプロファイル自体の設定が誤っているのではなく、設定された認可ルールのいずれも着信ユーザ属性（グループメンバーシップ、デバイスタイプ、ロケーションなど）に一致しなかったことを示します。その結果、ISEはデフォルトルールまたは明示的な拒否ルールにフォールバックし、アクセスが拒否されます。

## 考えられる原因

- ISEの認可ポリシールールを確認します。ユーザまたはデバイスが、適切なアクセスを許可するルールなど、目的のシェルプロファイルを割り当てる正しいルールと一致していることを確認します。
- ADまたは内部ユーザグループマッピングが正しいこと、およびポリシー条件（ユーザグループメンバーシップ、デバイスタイプ、プロトコルなど）が正しく指定されていることを確認します。
- ISEライブログと失敗した試行の詳細を使用して、一致したルールとその理由を正確に確認します。

## 問題 2

Cisco ISEとAristaスイッチ（または任意のネットワークデバイス）の間のTACACS+認証が失敗し、次のエラーメッセージが表示されます。

## "13017 Received TACACS+ packet from unknown Network Device or AAA Client"

The screenshot displays the Cisco ISE GUI for an authentication failure event. The interface is divided into two main sections: Overview and Authentication Details.

**Overview**

Request Type	Authentication
Status	Fail
Session Key	
Message Text	Failed-Attempt: TACACS+ Request dropped
Username	
Authentication Policy	
Selected Authorization Profile	

**Steps**

13017 Received TACACS+ packet from unknown Network Device or AAA Client

**Authentication Details**

Generated Time	2025-07-27 17:50:17.705000 +05:30
Logged Time	2025-07-27 17:50:17.705
Epoch Time (sec)	1753618817
ISE Node	goldenserver
Message Text	Failed-Attempt: TACACS+ Request dropped
Failure Reason	13017 Received TACACS+ packet from unknown Network Device or AAA Client
Resolution	
Root Cause	
Username	

### 考えられる原因

- 最も一般的な理由は、スイッチのIPアドレスがISEのネットワークデバイスとして追加されていないことです ( Administration > Network Resources > Network Devicesの下 )。
- IPアドレスまたは範囲が、TACACS+パケットを送信するためにAristaスイッチによって使用されている送信元IPと正確に一致していることを確認します。
- スイッチが管理インターフェイスを使用している場合は、ISEにその正確なIP ( サブネット /範囲だけでなく ) が追加されていることを確認します。

### 解決方法

- ISE GUIで、Administration > Network Resources > Network Devicesの順に選択します。
- Aristaスイッチの正確な送信元IPアドレス ( 通常は管理インターフェイスIP ) が TACACS+通信に使用されているかどうかを確認します。
- 共有秘密を指定します ( これはAristaスイッチに設定されているものと一致する必要があります ) 。

## 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。