ISEを使用したPalo AltoでのTACACS+デバイス管理の設定

内容

はじめに

このドキュメントでは、Palo AltoでのCisco ISEを使用したTACACS+の設定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。
- パロアルトファイアウォール。

使用するコンポーネント

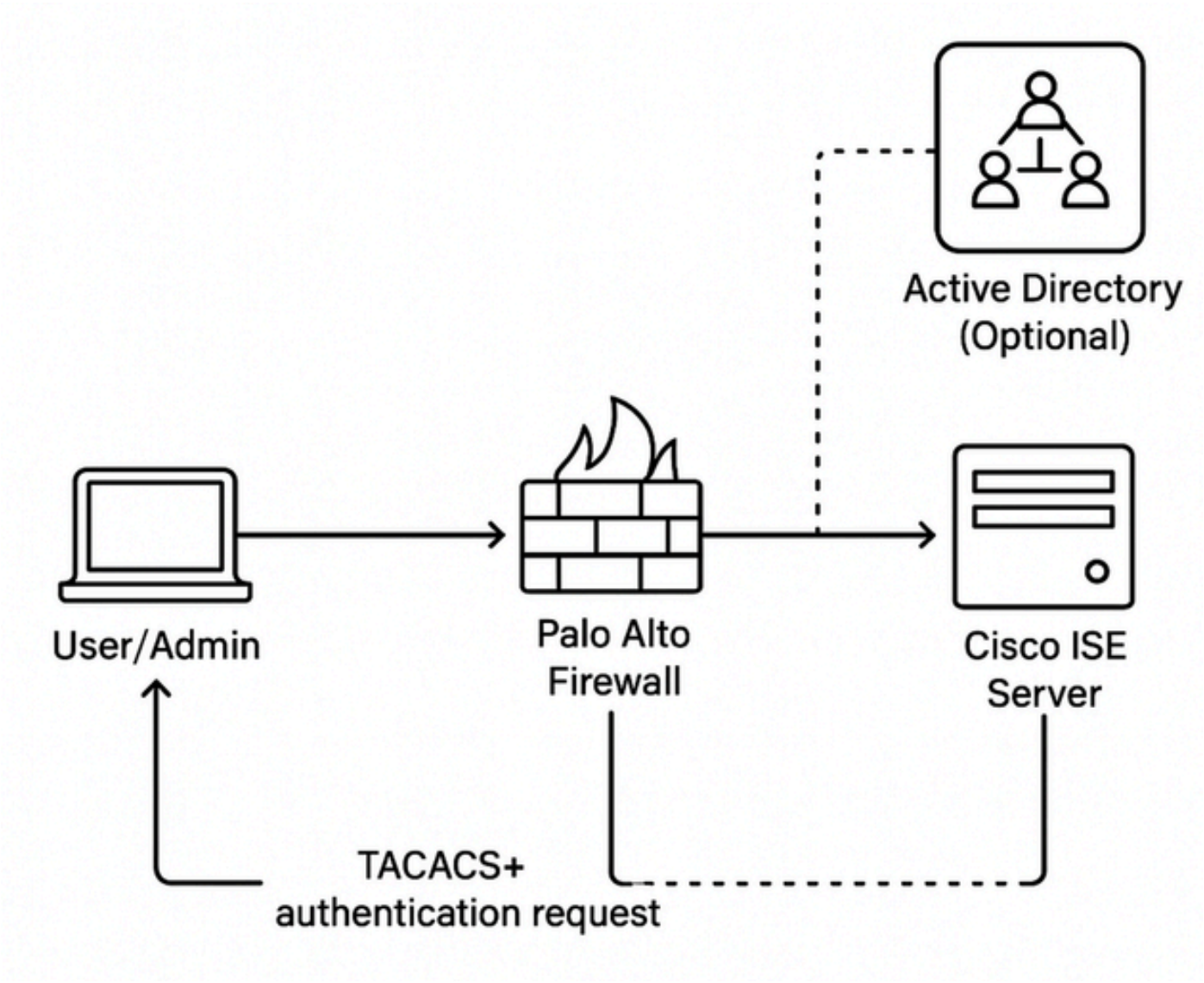
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Palo Alto Firewallバージョン10.1.0
- 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。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。

ネットワーク図



認証フロー

1. 管理者がPalo Altoファイアウォールにログインします。

2. Palo AltoがTACACS+認証要求をCisco ISEに送信します。

3. Cisco ISE:

- ADが統合されている場合、ADに対して認証と認可のクエリーが実行されます。
- ADが存在しない場合、ローカルIDストアまたはポリシーが使用されます。
- Cisco ISEは、設定されたポリシーに基づいてPalo Altoに認可応答を送信します。
- 管理者は、適切な特権レベルでアクセスできます。

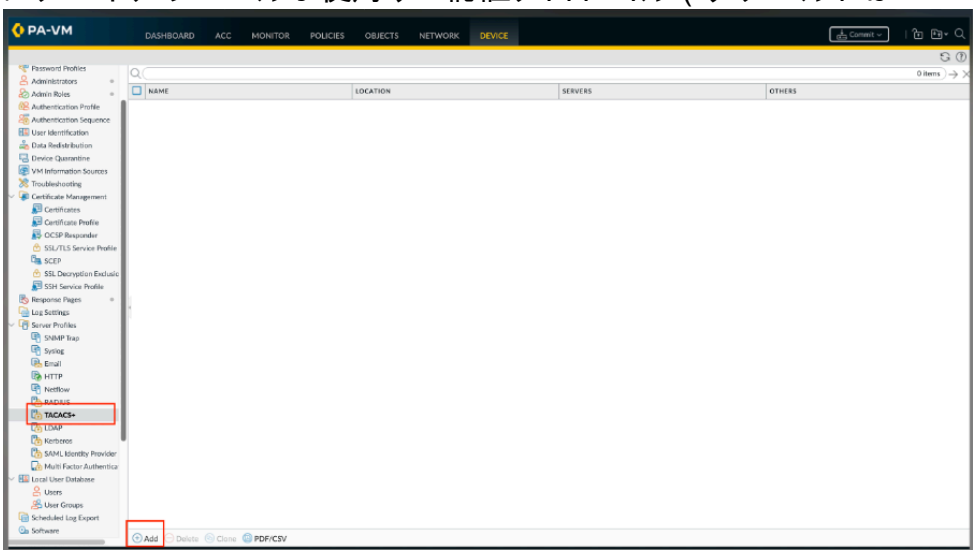
設定

セクション1:TACACS+用のPalo Altoファイアウォールの設定

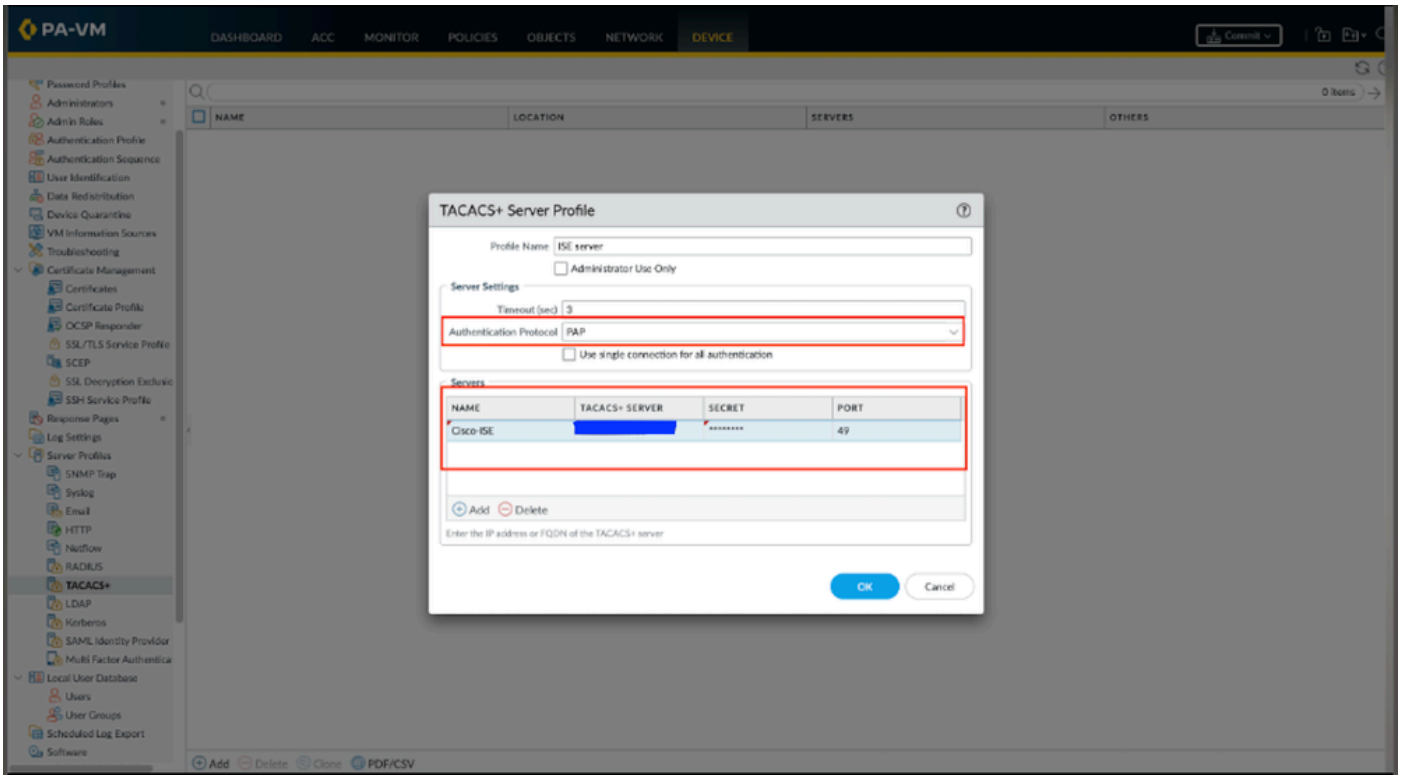
ステップ 1：TACACS+サーバプロファイルを追加します。

このプロファイルは、ファイアウォールをTACACS+サーバに接続する方法を定義します。

1. パノラマでDevice > Server Profiles > TACACS+またはPanorama > Server Profiles > TACACS+の順に選択し、Add a profileを選択します。
2. サーバプロファイルを識別するプロファイル名を入力します。
3. （オプション）管理者にアクセスを制限するには、Administrator Use Onlyを選択します。
4. 認証要求がタイムアウトするまでのタイムアウト間隔を秒単位で入力します（デフォルトは3、範囲は1 ~ 20）。
5. TACACS+サーバの認証にファイアウォールが使用する認証プロトコル（デフォルトはCHAP）を選択します。



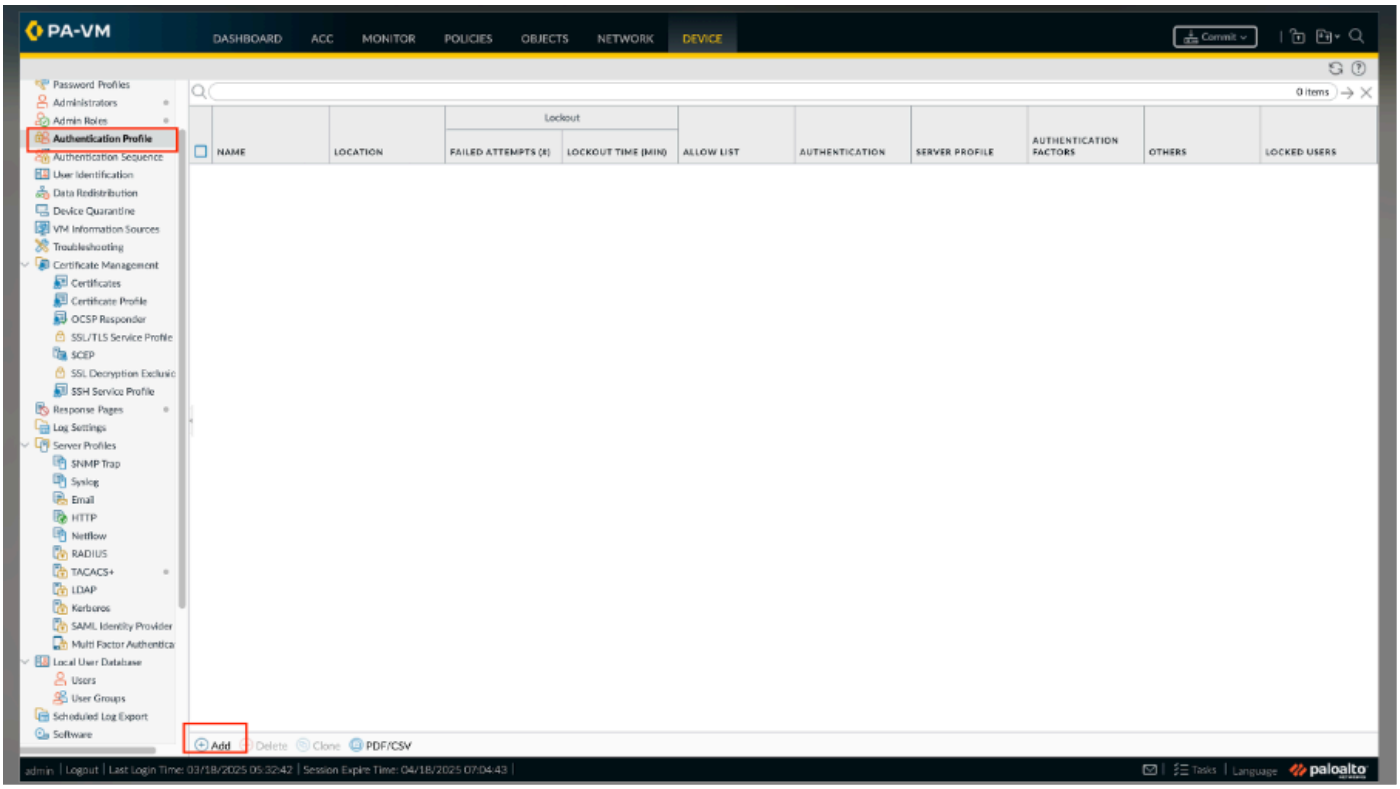
6. 各TACACS+サーバを追加して、次の手順を実行します。
    1. サーバを識別する名前。
    2. TACACS+サーバのIPアドレスまたはFQDN。FQDNアドレスオブジェクトを使用してサーバーを識別し、その後アドレスを変更した場合は、新しいサーバーアドレスの変更をコミットする必要があります。
    3. ユーザ名とパスワードを暗号化するためのシークレットとシークレットの確認。
    4. 認証要求のサーバポート（デフォルトは49）。 OKをクリックして、サーバプロファイルを保存します。
7. 「OK」をクリックして、サーバー・プロファイルを保存します。

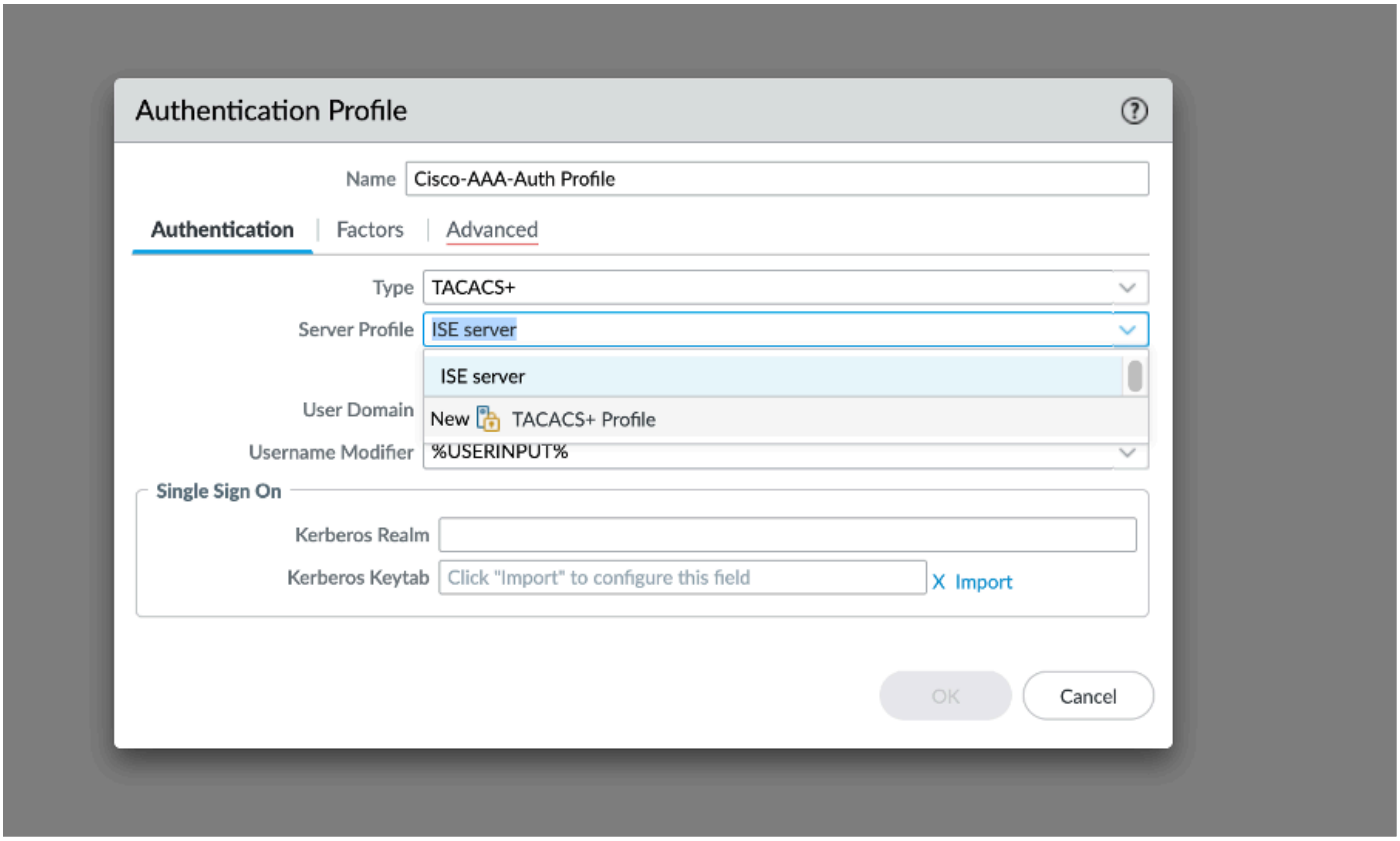


ステップ 2：TACACS+サーバプロファイルを認証プロファイルに割り当てます。

認証プロファイルは、一連のユーザに共通の認証設定を定義します。

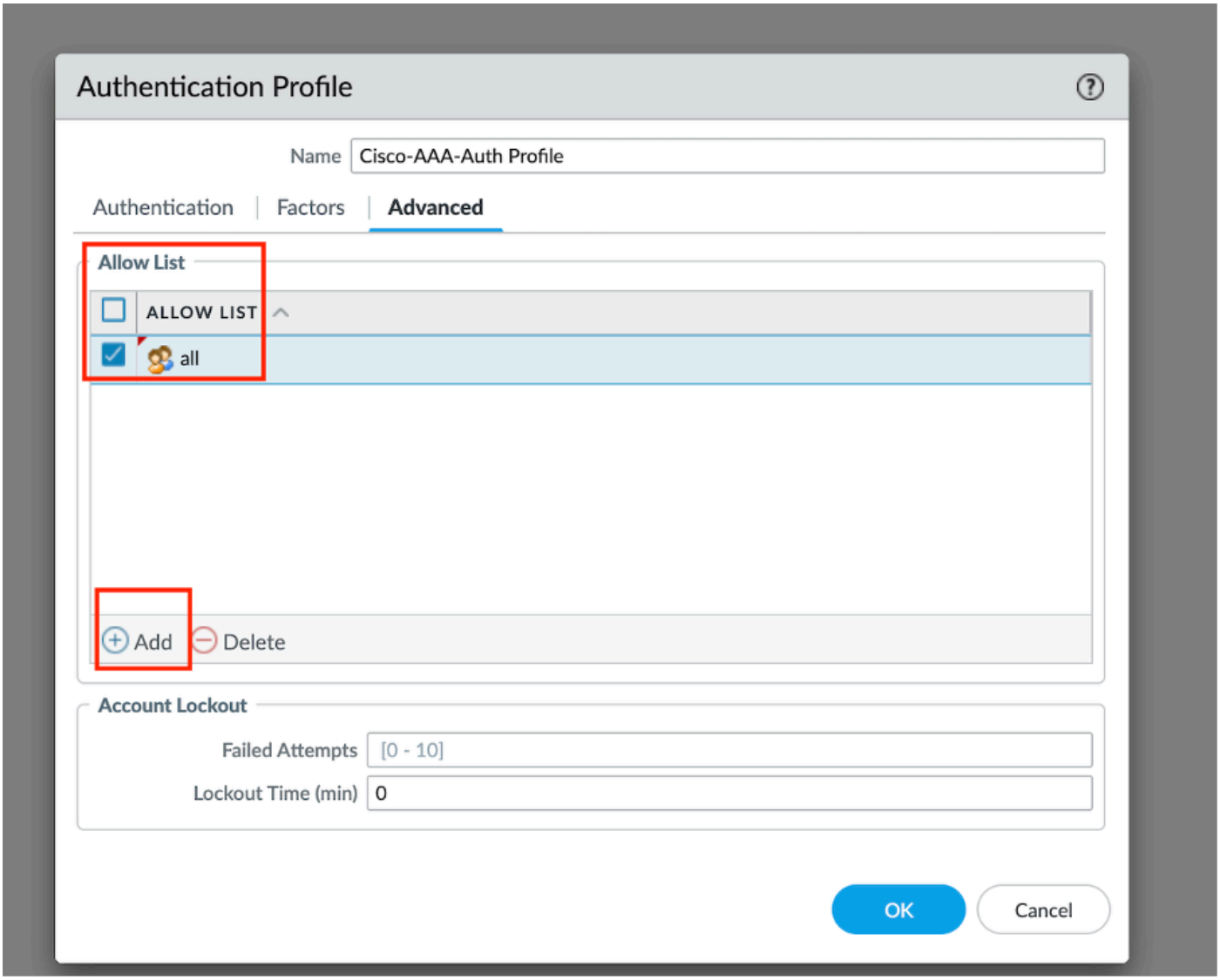
1. Device > Authentication Profile の順に選択し、プロファイルをAdd します。
    1. プロファイルを識別する名前を入力します
    2. TypeをTACACS+に設定します。
    3. 設定したサーバプロファイルを選択します。
    4. Retrieve user group from TACACS+を選択して、TACACS+サーバで定義されたVSAからユーザグループ情報を収集します。





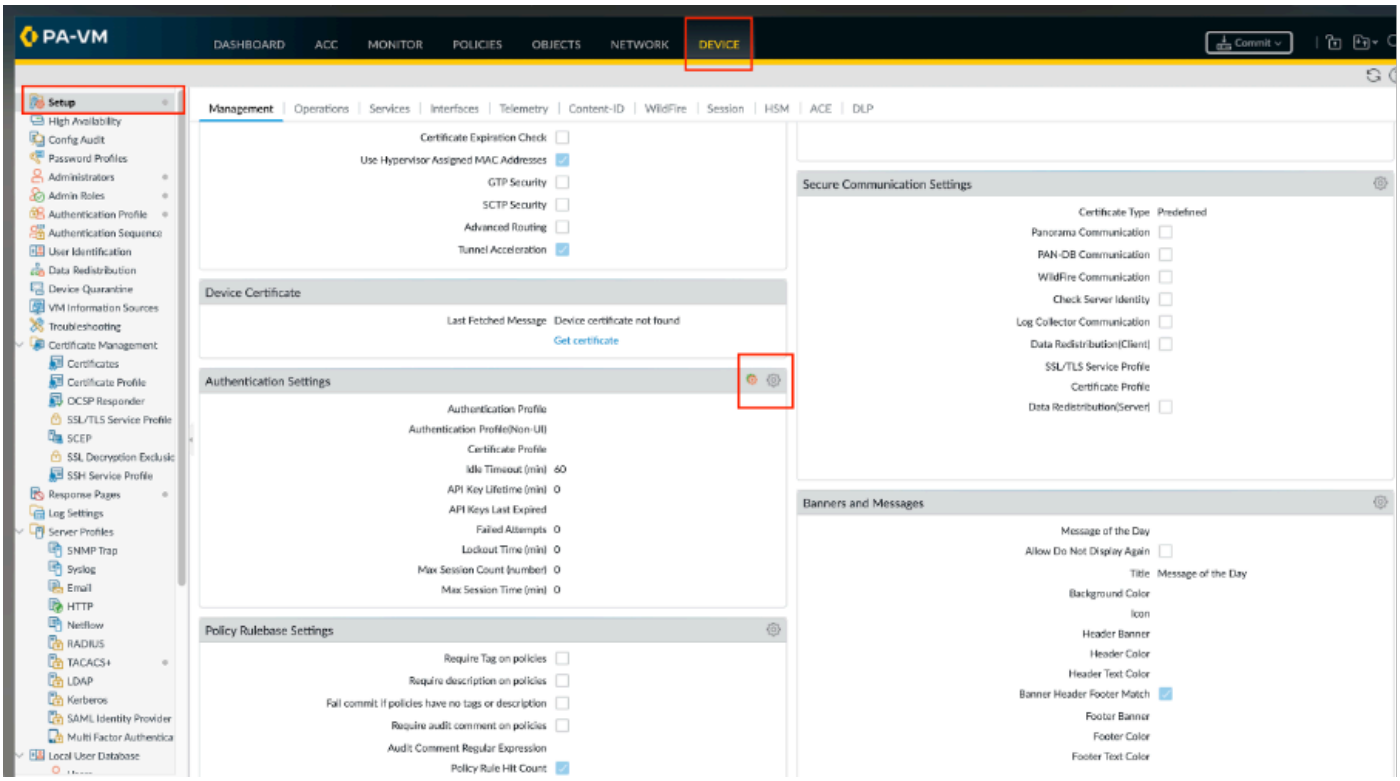
ファイアウォールは、認証プロファイルの許可リストで指定したグループを使用して、グループ情報を照合します。

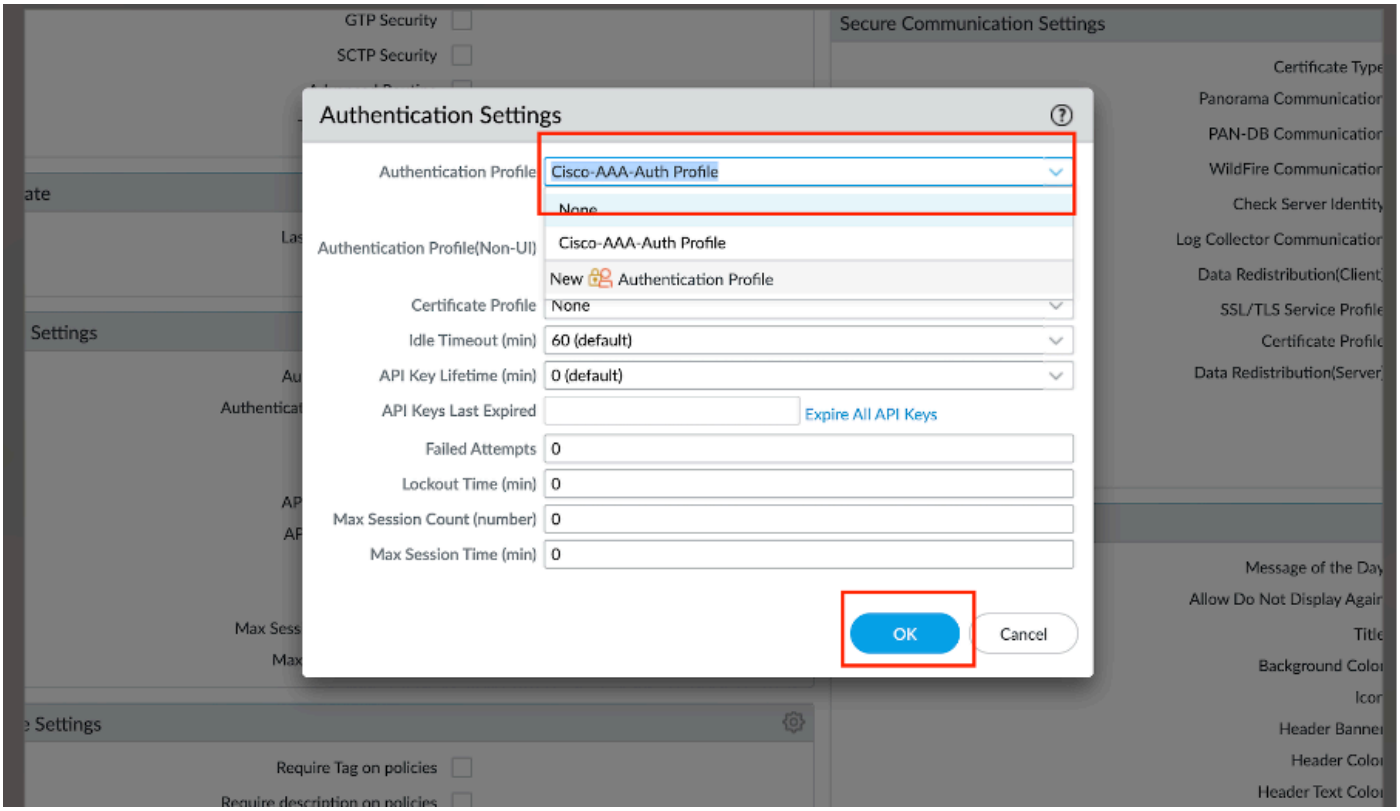
1. Advancedを選択し、Allow Listで、この認証プロファイルで認証できるユーザとグループを追加します。
2. OKをクリックして、認証プロファイルを保存します。



ステップ 3：すべての管理者に認証プロファイルを使用するようにファイアウォールを設定します。

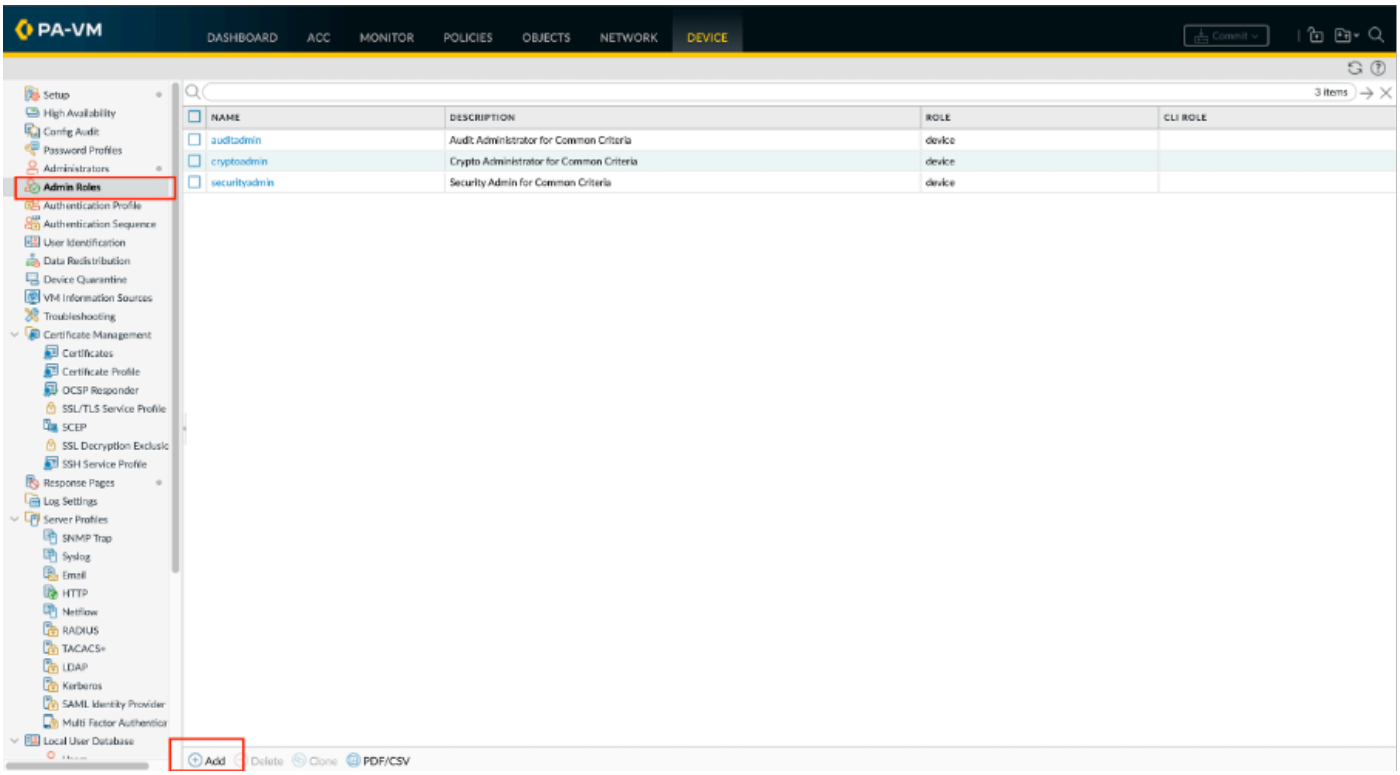
1. Device > Setup > Managementの順に選択し、Authentication Settingsを編集します。
2. 設定した認証プロファイルを選択し、OKをクリックします。



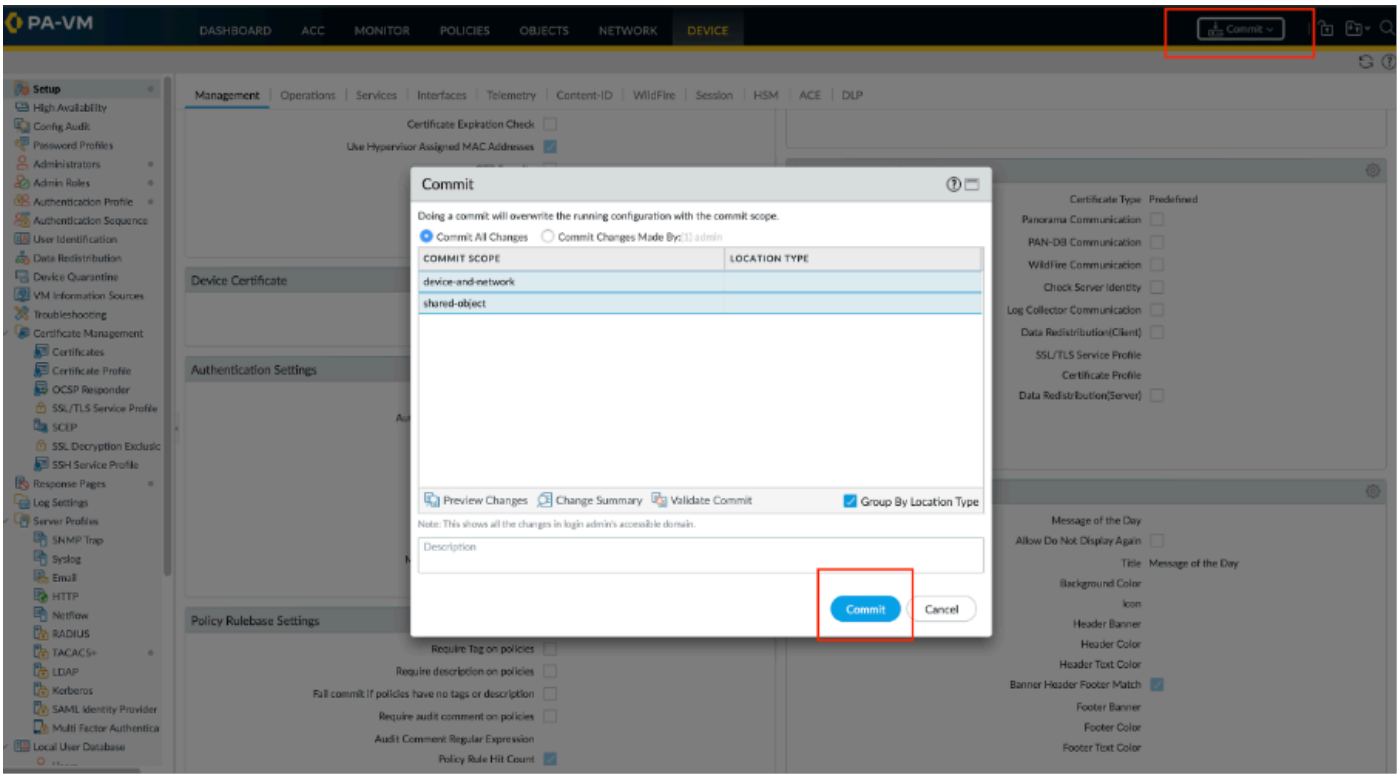


ステップ 4：管理者ロールプロファイルを設定します。

Device > Admin Rolesの順に選択し、Addをクリックします。ロールを識別する名前を入力します。

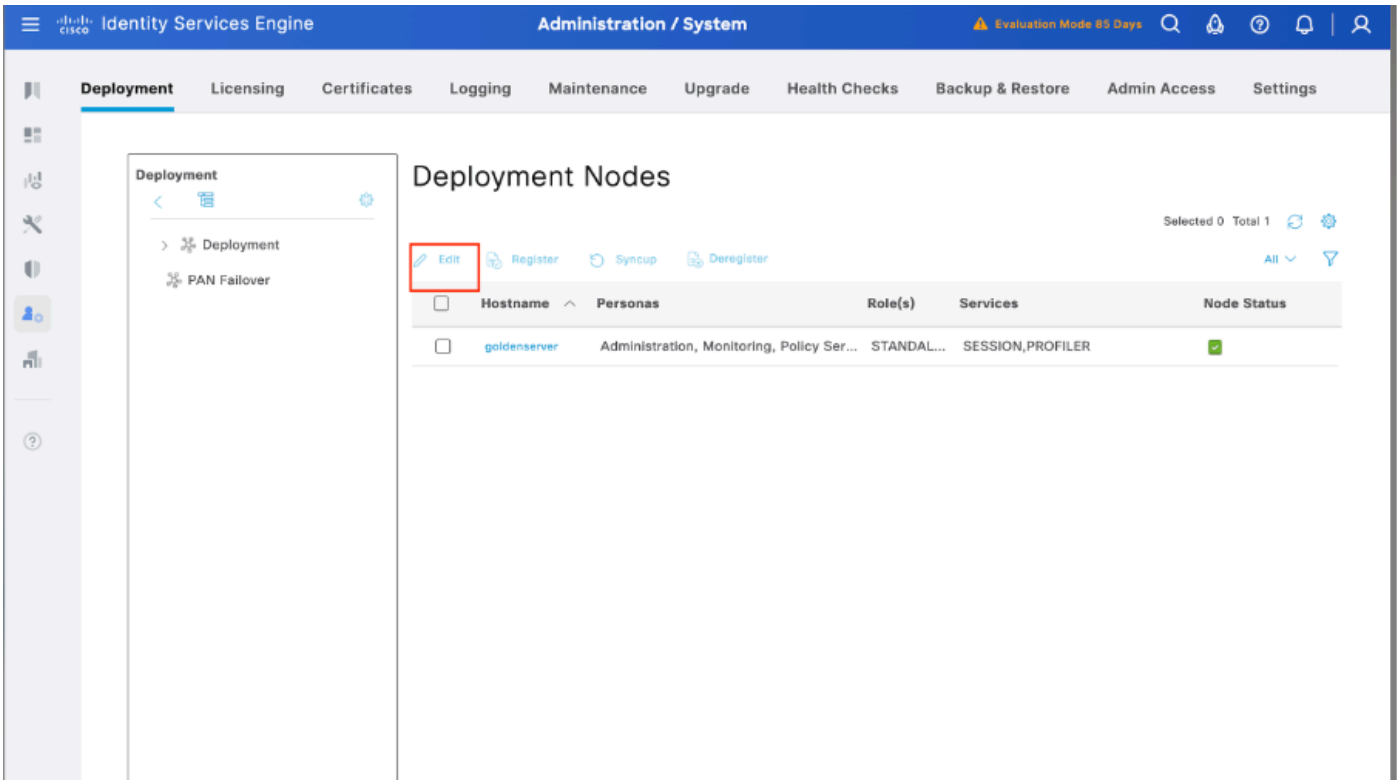


ステップ 5：変更を確定して、ファイアウォールで有効にします。

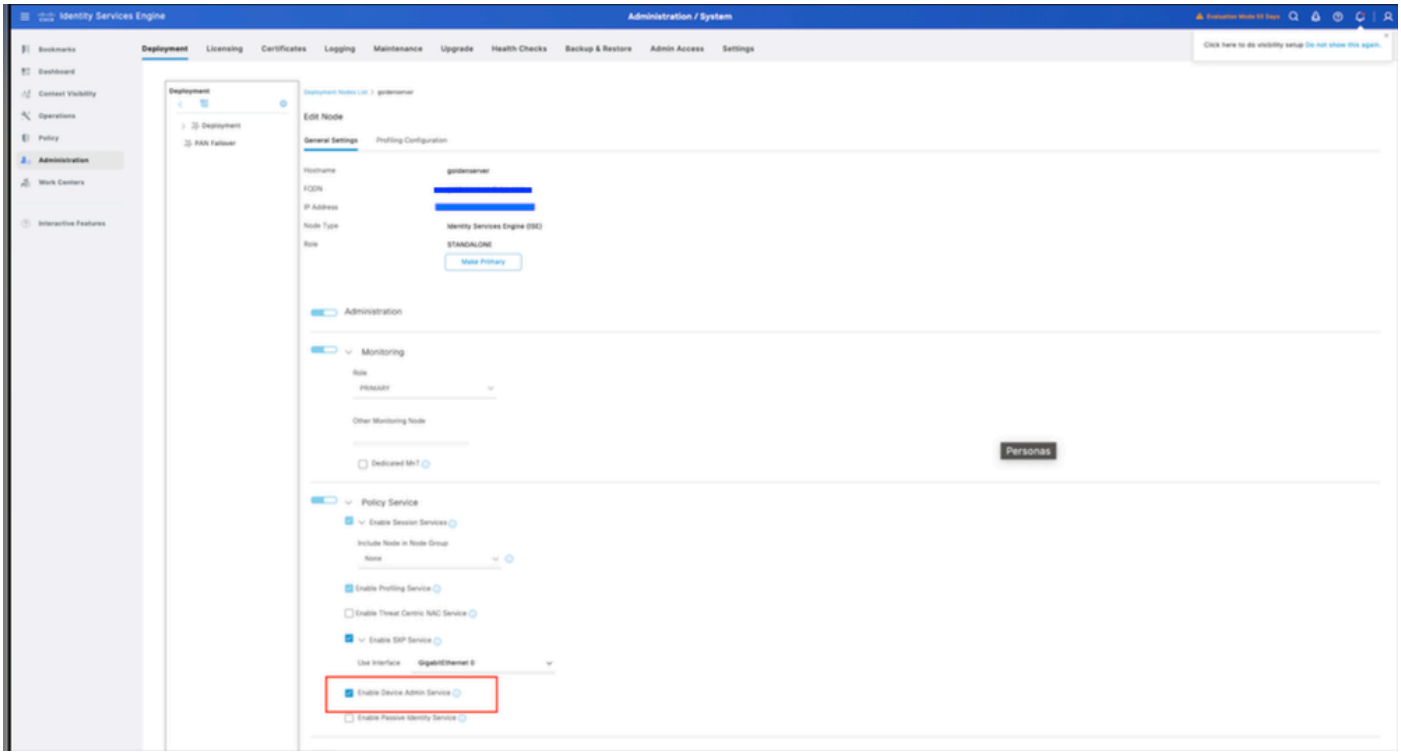


セクション2:ISEでのTACACS+の設定

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。

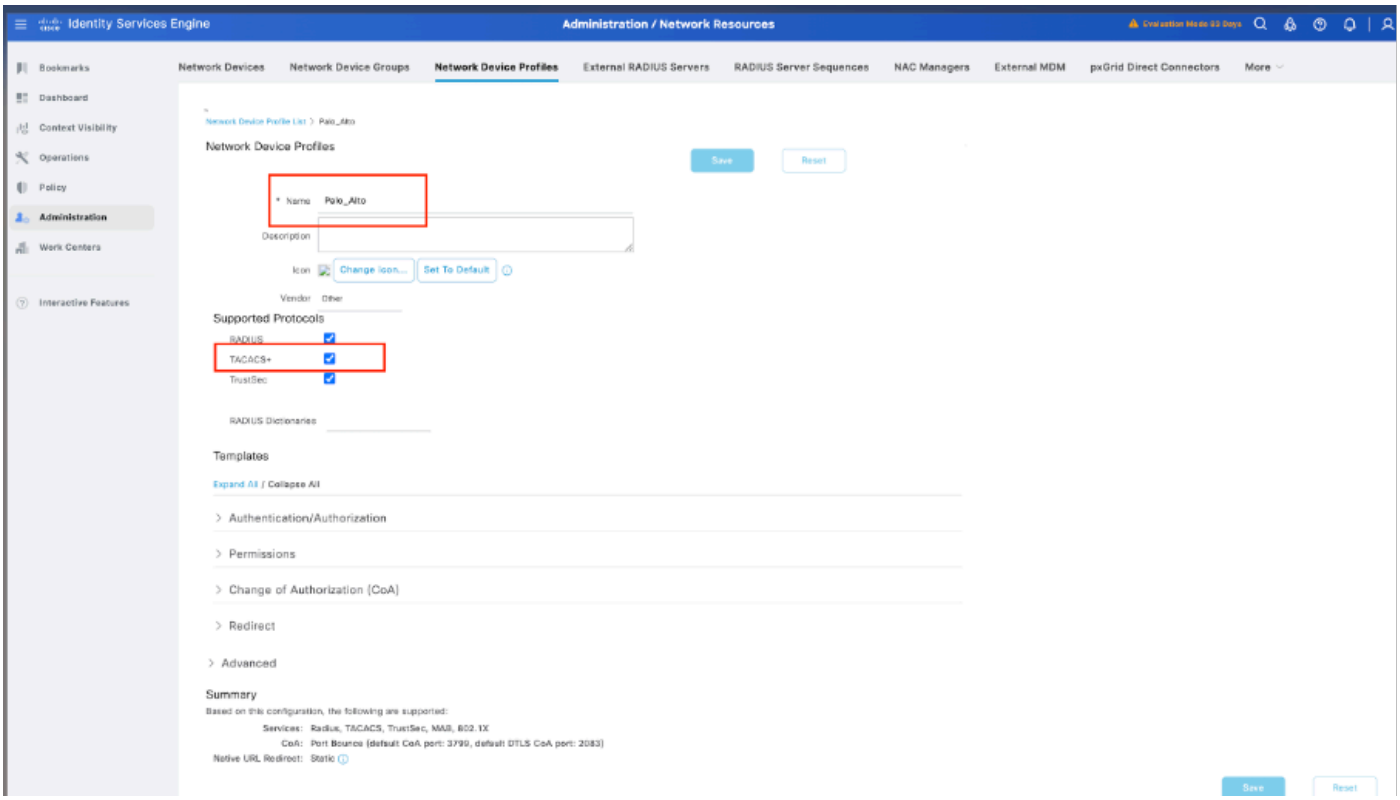


ステップ 2：下にスクロールして、Device Administration Service機能を見つけます。この機能を有効にするには、ポリシーサービスのペルソナがノード上でアクティブであり、展開内で使用可能なTACACS+ライセンスが存在している必要があります。チェックボックスをオンにして機能を有効にし、設定を保存します。



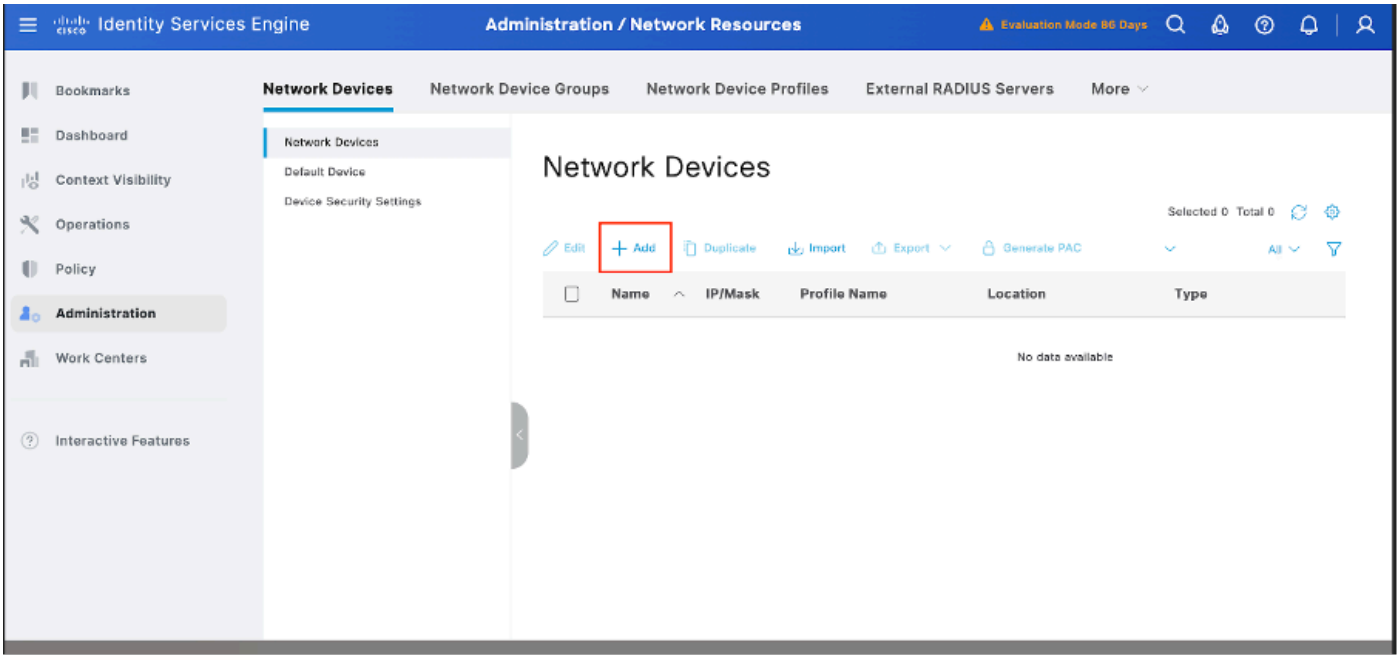
ステップ 3：Cisco ISEのPalo Altoネットワークデバイスプロファイルを設定します。

Administration > Network Resources > Network device profileの順に移動します。Addをクリックし、名前(Palo Alto)を指定して、supported protocolsの下でTACACS+をイネーブルにします。



ステップ 4：Palo Altoをネットワークデバイスとして追加します。

1. Administration > Network Resources > Network Devices > +Addの順に選択します。



2. Addをクリックして、次の詳細情報を入力します。

名前：Palo-Alto

IPアドレス：<Palo-Alto IP>

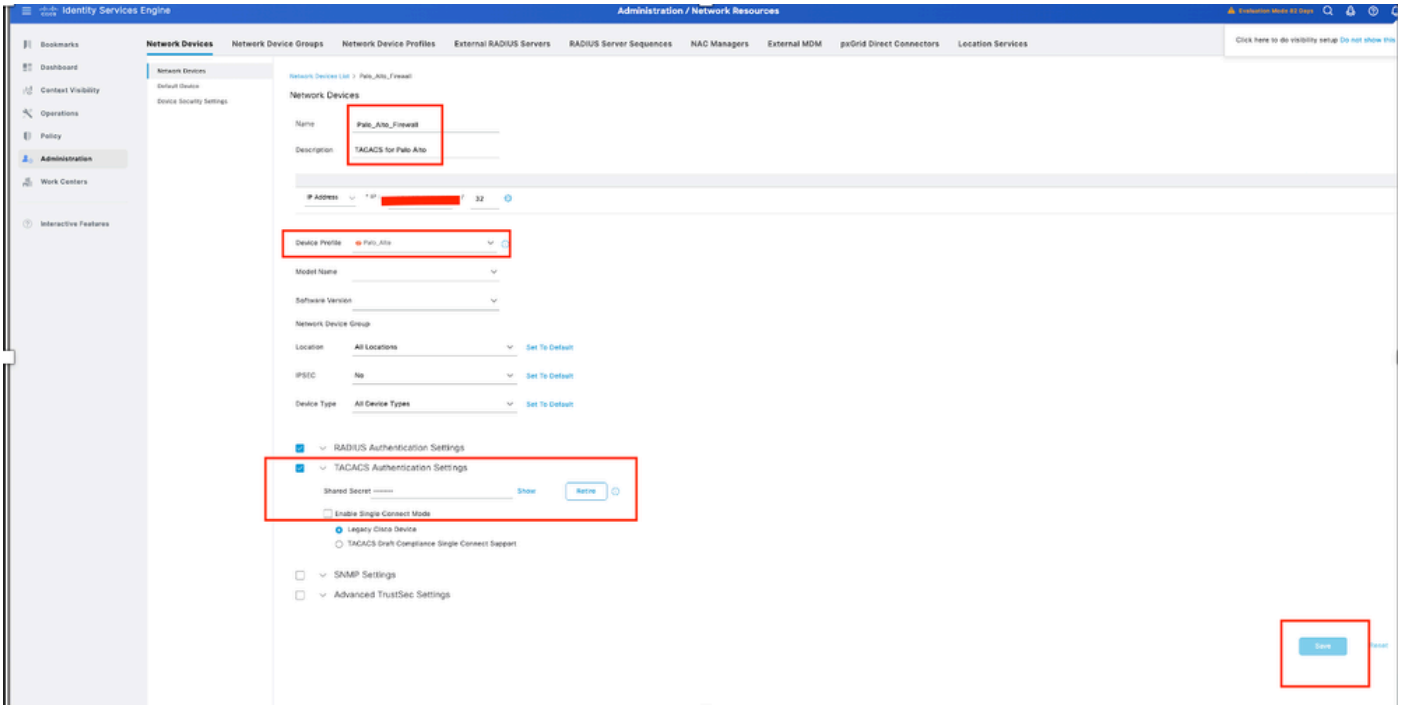
ネットワークデバイスプロファイル：Palo Altoを選択

TACACS認証設定：

TACACS+認証の有効化

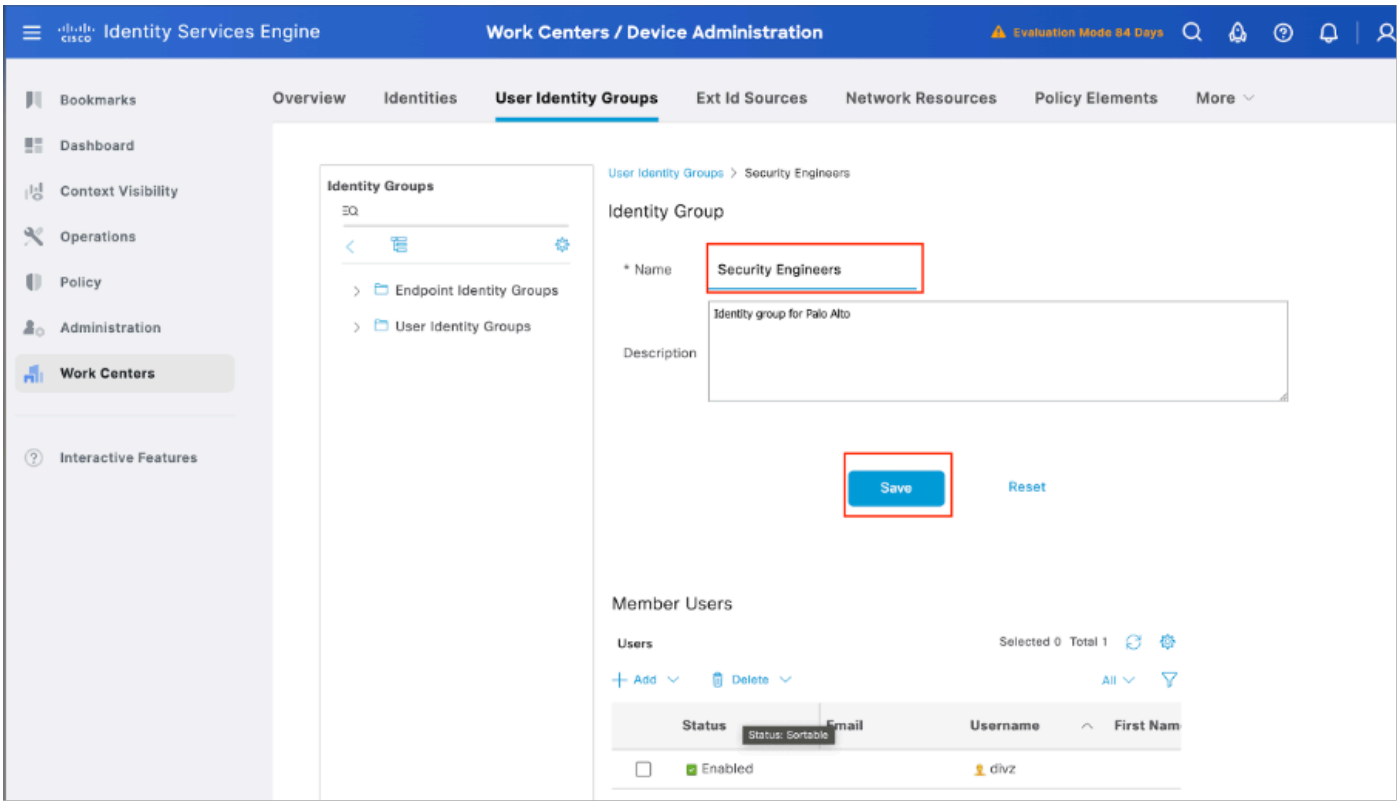
共有秘密鍵を入力します（Palo Altoの設定と一致している必要があります）。

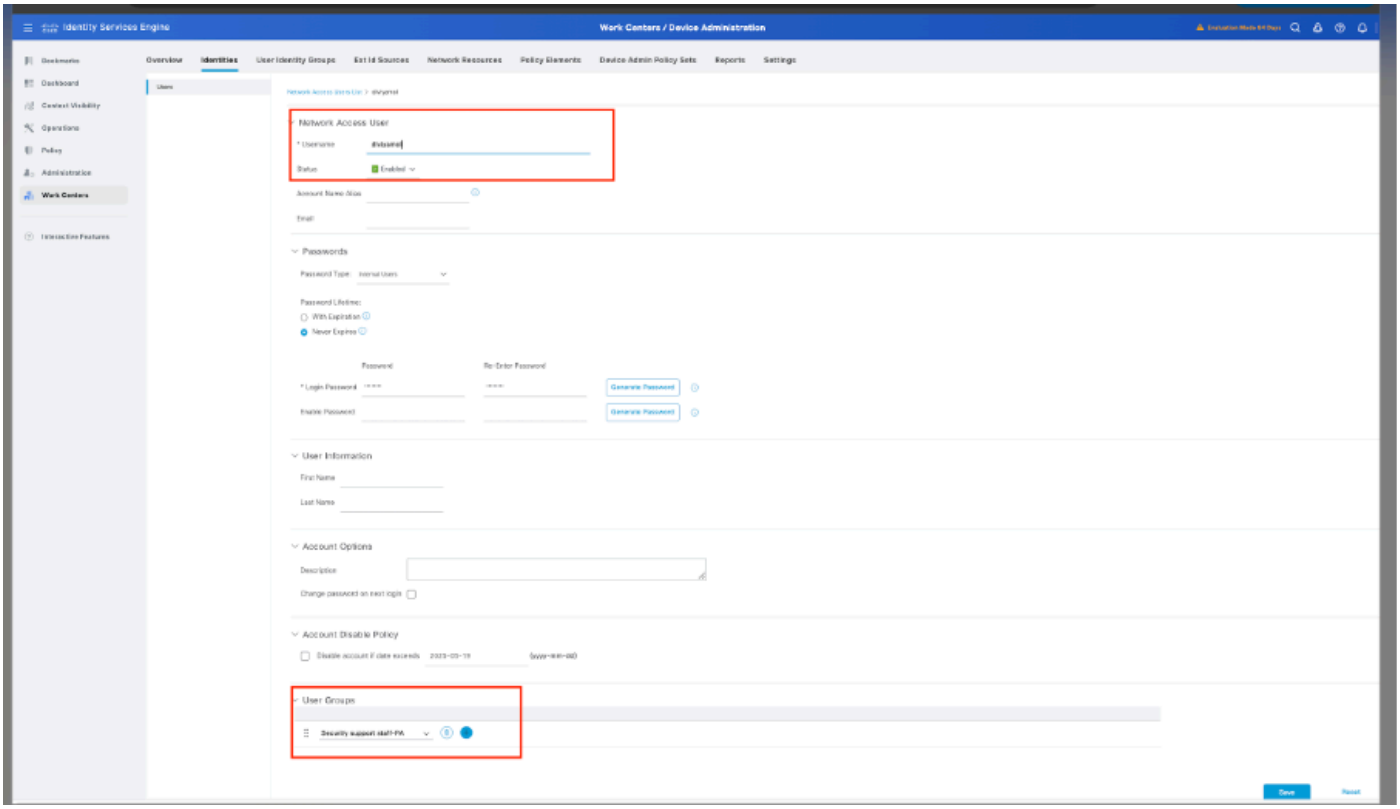
[Save] をクリックします。

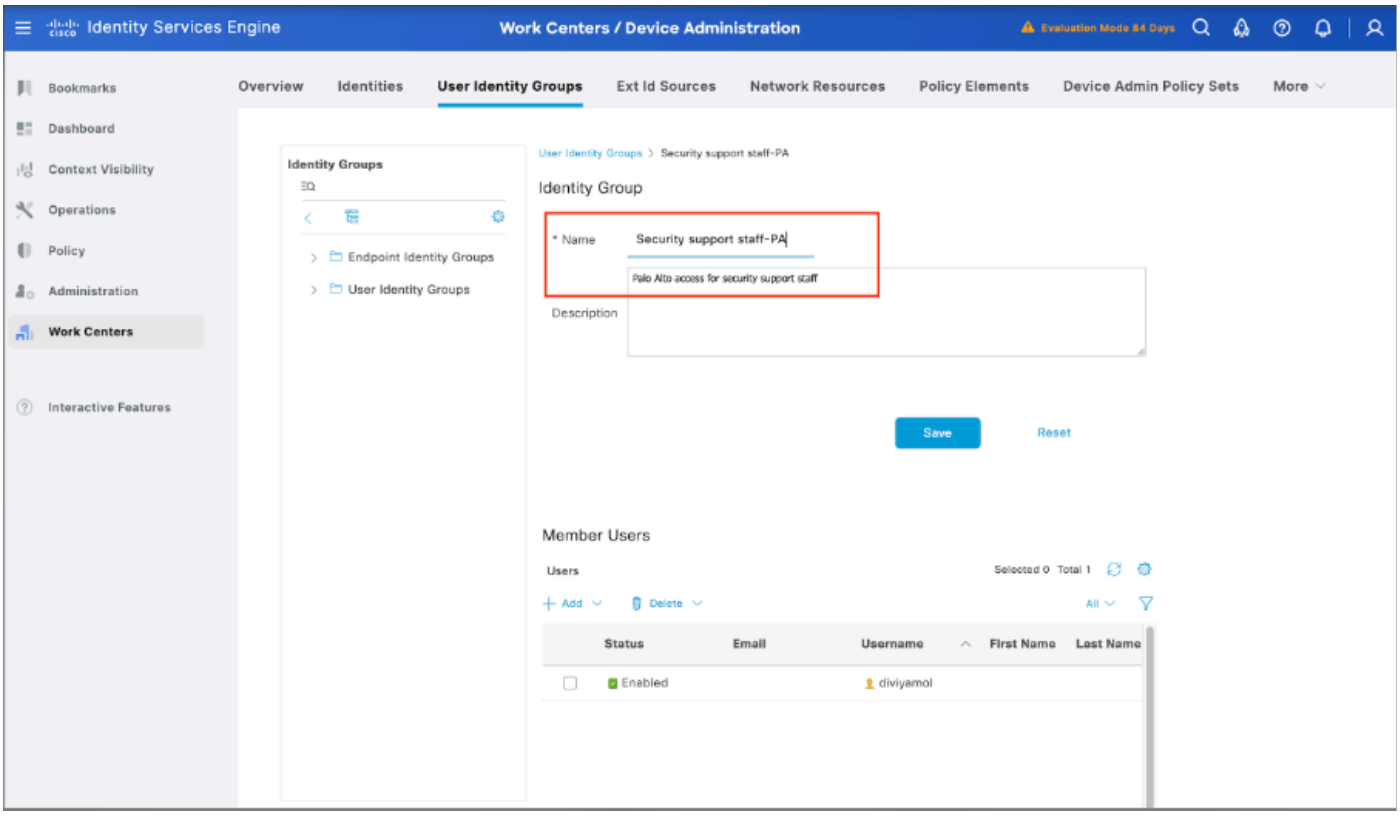


ステップ 5：ユーザIDグループを作成します。

Work Centers > Device Administration > User Identity Groupsの順に移動し、Addをクリックして、ユーザグループの名前を指定します。


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

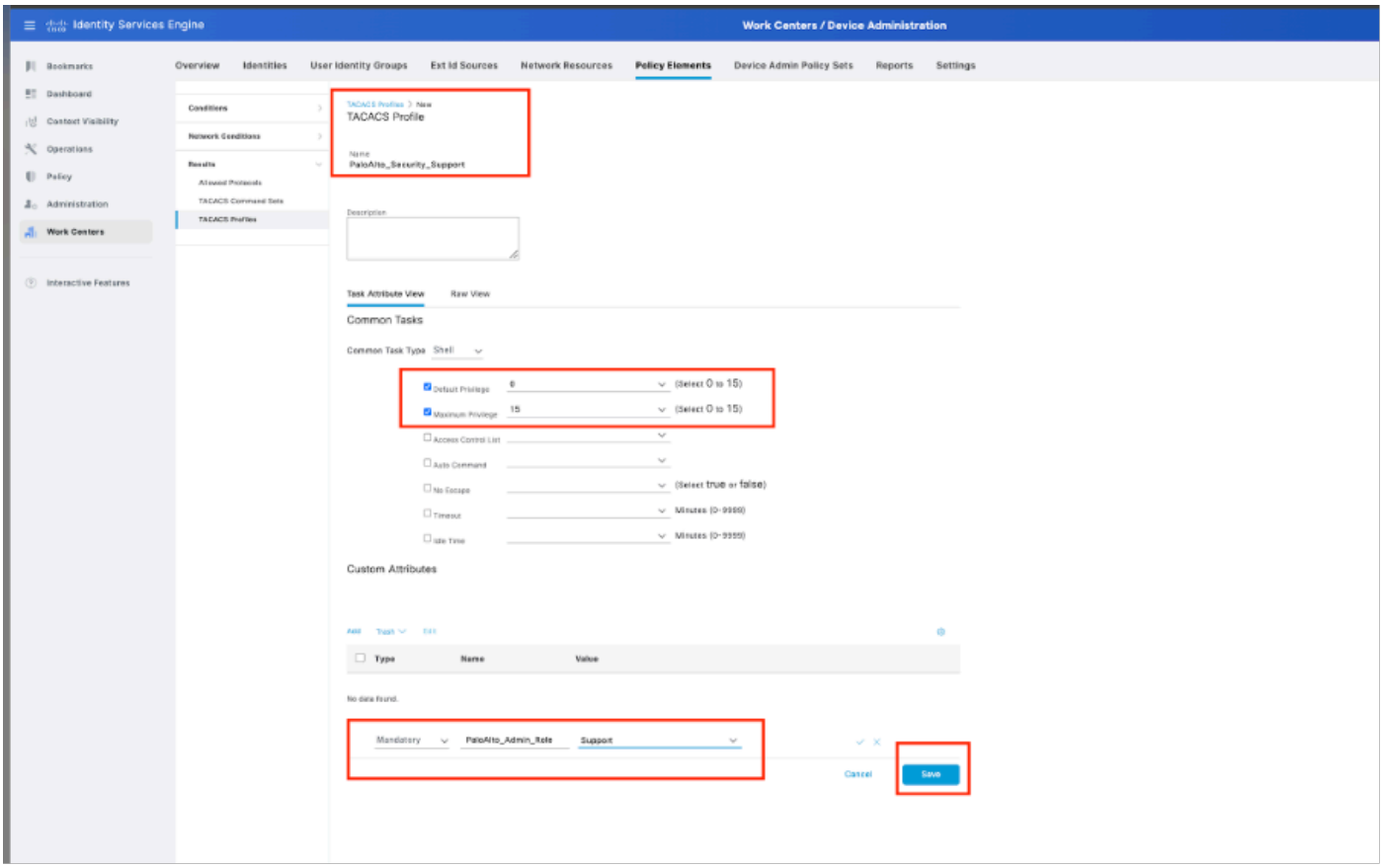

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

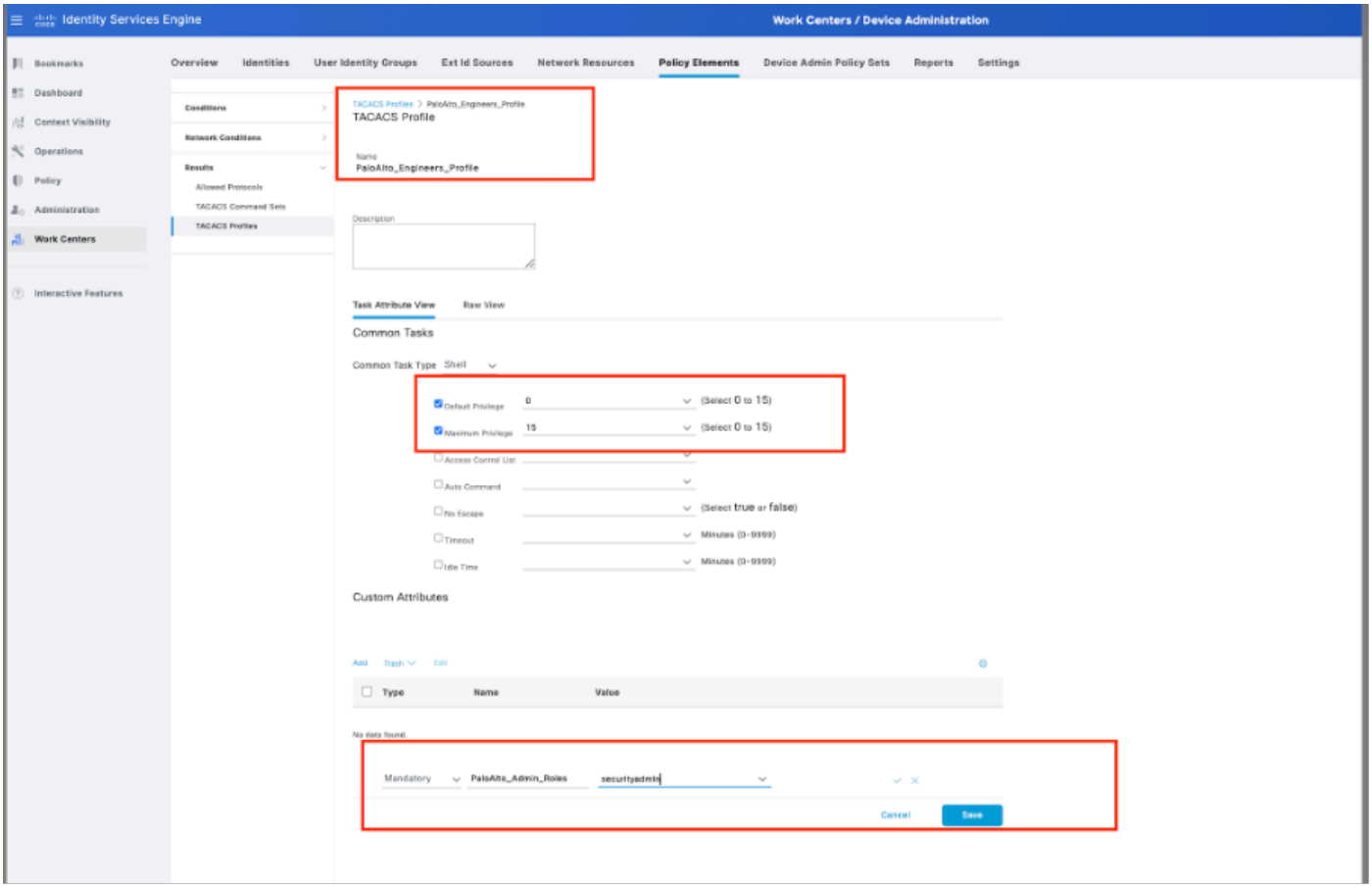


手順 6：TACACSプロファイルを設定します。

次は、特権レベルやタイムアウトの設定などの設定を行うことができるTACACSプロファイルの設定です。Work Centers > Device Administration -> Policy Elements -> Results -> TACACS Profilesの順に移動します。

Addをクリックして、新しいTACACS Profileを作成します。プロファイルに適切な名前を付けます。





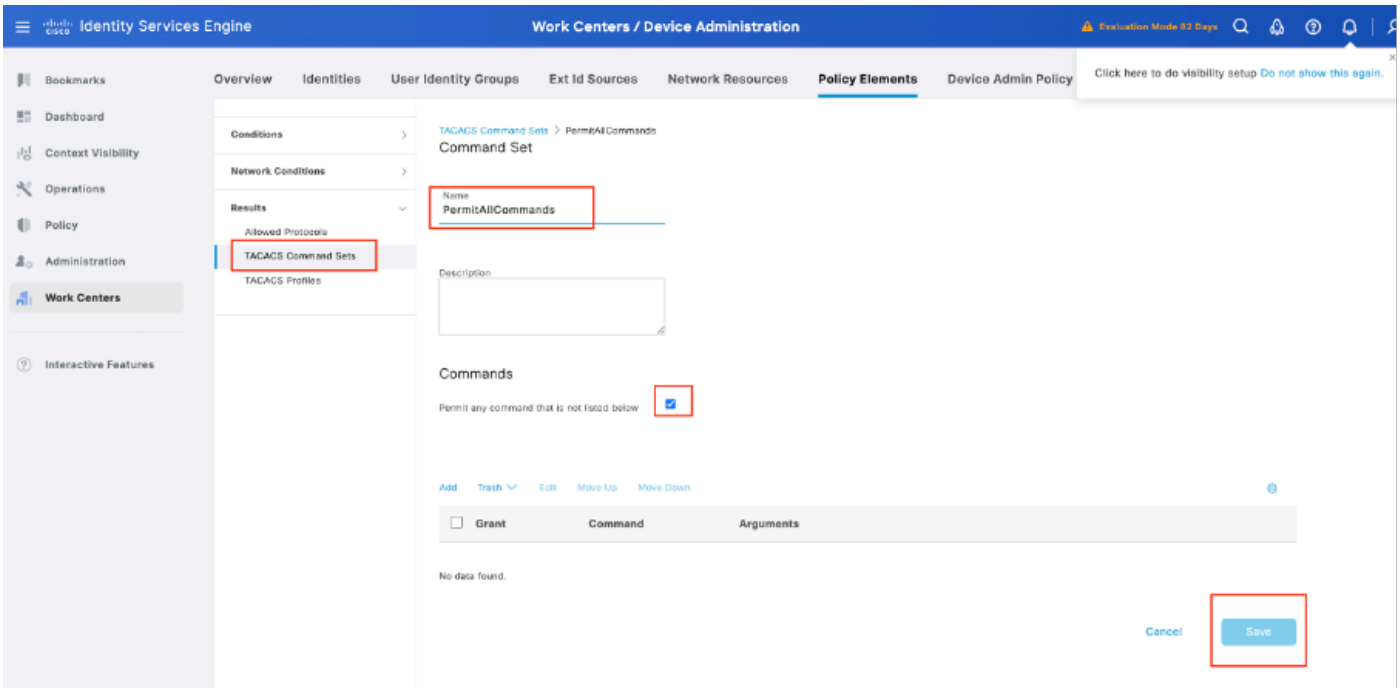
手順 6：TACACSコマンドセットを設定します。

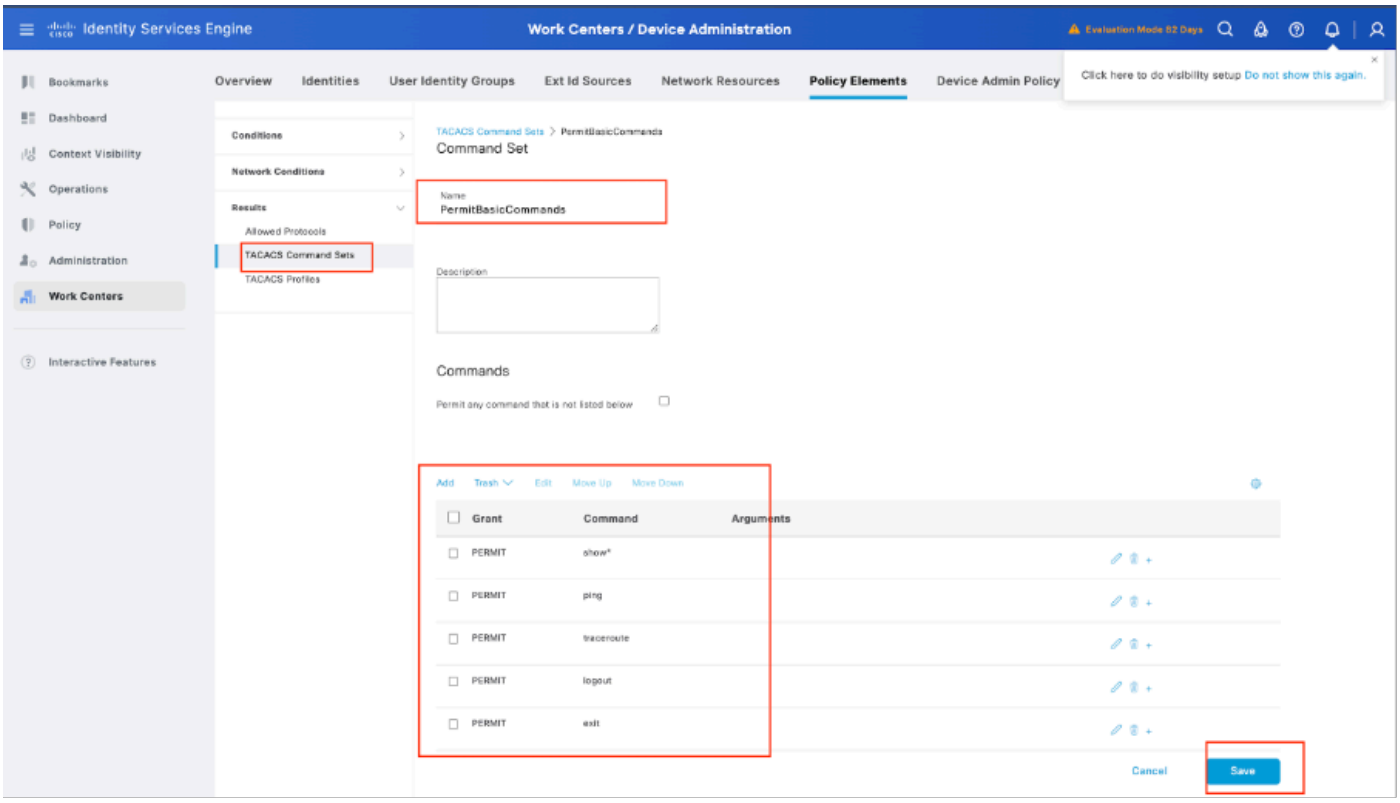
次に、ユーザが使用できるコマンドを設定します。両方の使用例に特権レベル15を付与して、利

用可能なすべてのコマンドにアクセスできるようにすることができるため、TACACSコマンドセットを使用して、使用できるコマンドを制限してください。

Work Centers > Device Administration > Policy Elements >Results -> TACACS Command Setsの順に移動します。Addをクリックして新しいTACACSコマンドセットを作成し、PermitAllCommandsという名前を付けます。このTACACSコマンドセットをセキュリティサポートに適用します。

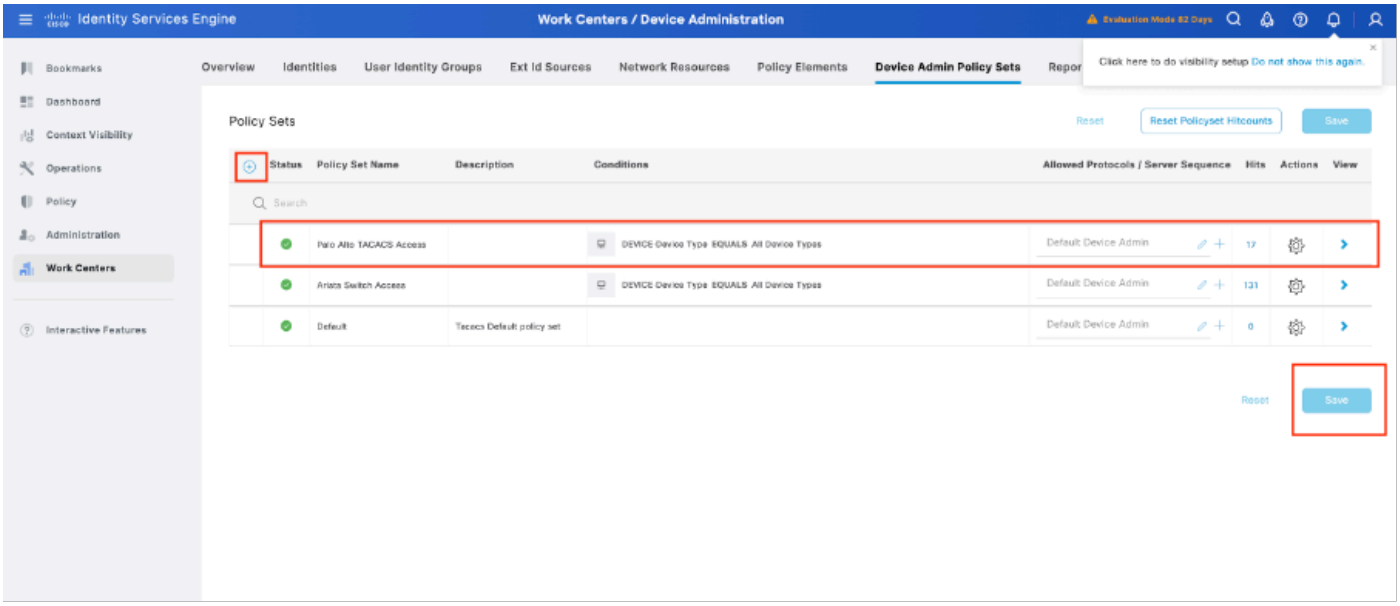
このTACACSコマンドセットで設定する必要があるのは、次にリストされていないコマンドをすべて許可するチェックボックスをオンにすることです。



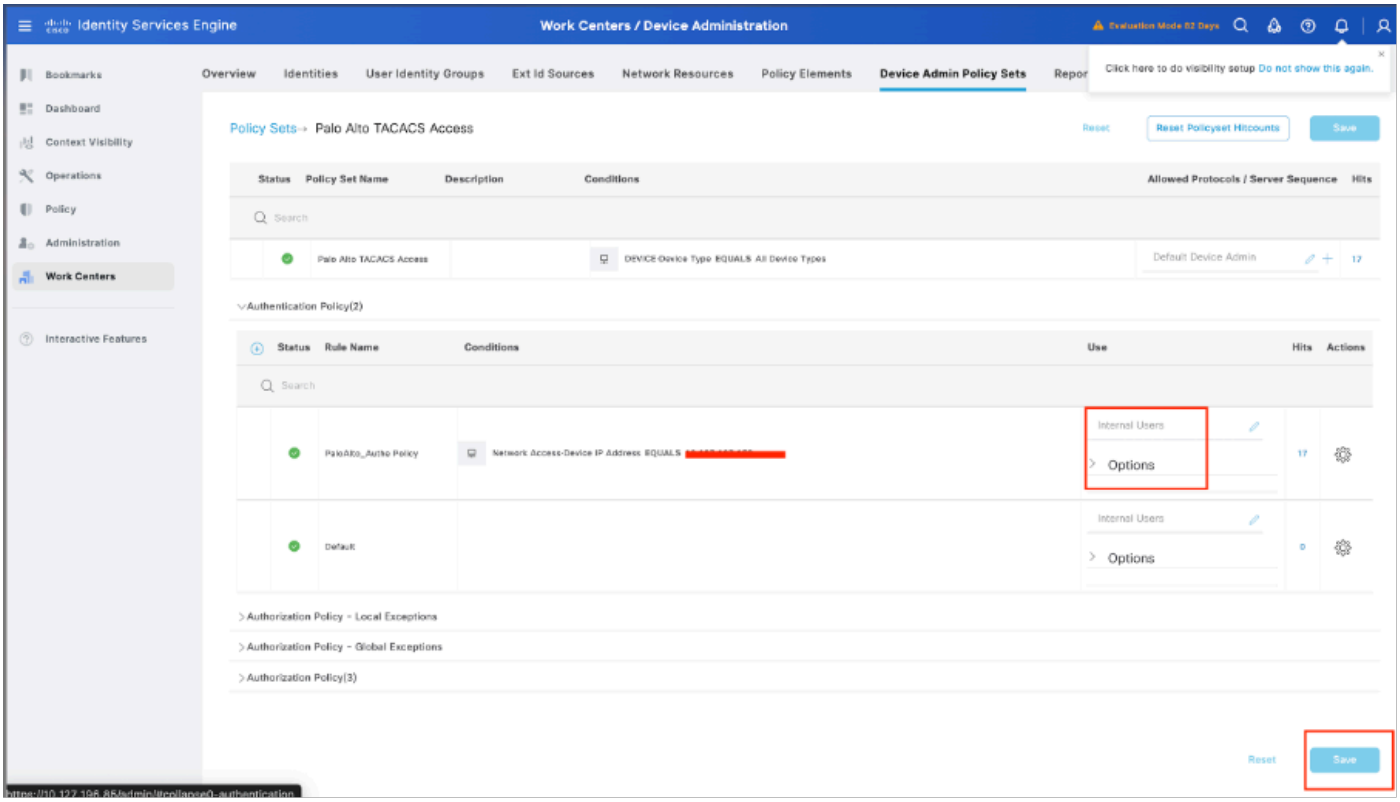


手順 7：Palo Altoで使用するデバイス管理ポリシーセットを作成し、ワークセンター>デバイス管理>デバイス管理ポリシーセットの順に選択し、追加 +アイコンをクリックします。

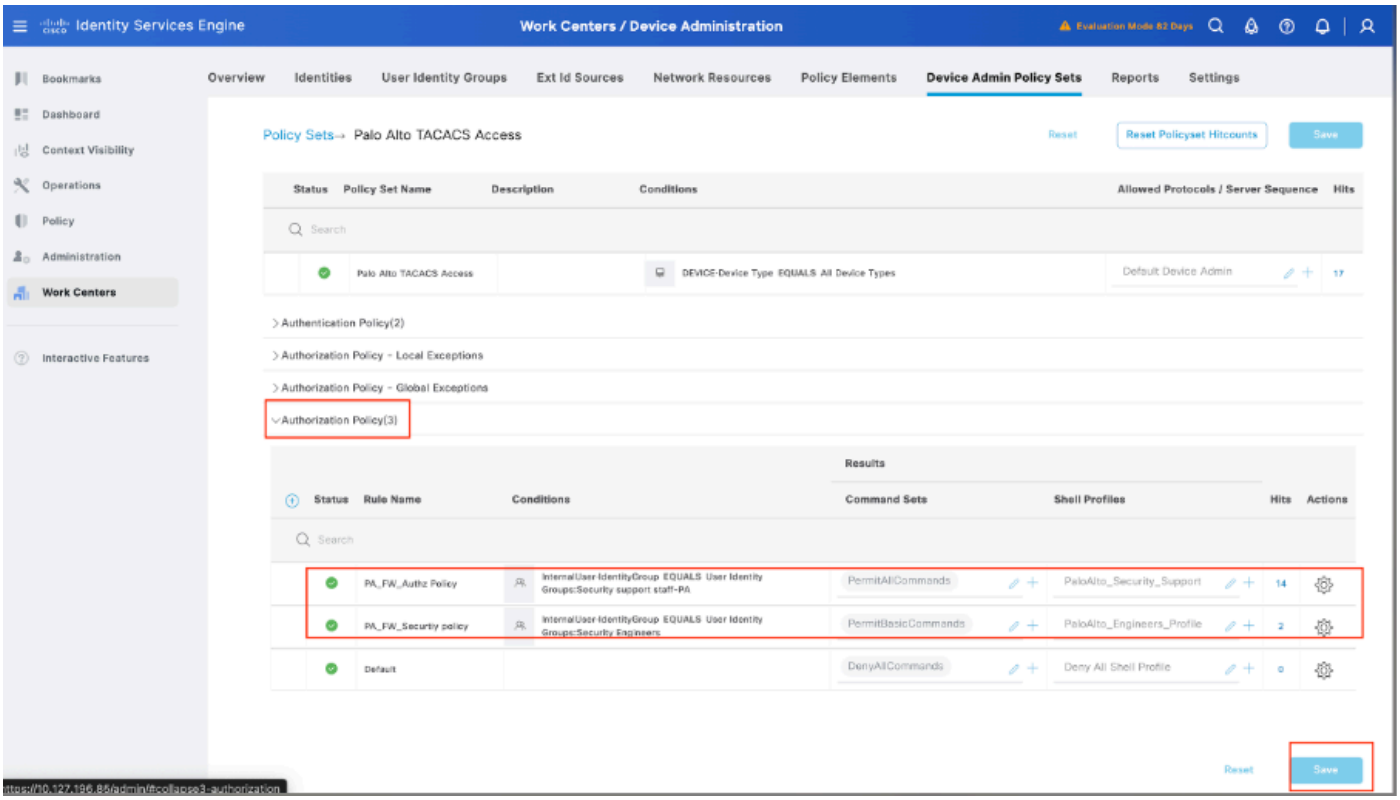
ステップ 8：この新しいポリシーセットに名前を付け、Palo Alto Firewallで実行中のTACACS+認証の特性に応じて条件を追加し、Allowed Protocols > Default Device Adminの順に選択します。設定を保存します。



ステップ 9：> viewオプションを選択してから、Authentication Policyセクションで、Palo Alto Firewallで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 10： DefaultポリシーまでAuthorization Policyというセクションまで下にスクロールし、gearアイコンを選択して、上にルールを1つ挿入します。



ステップ 11 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。

確認

ISEのレビュー

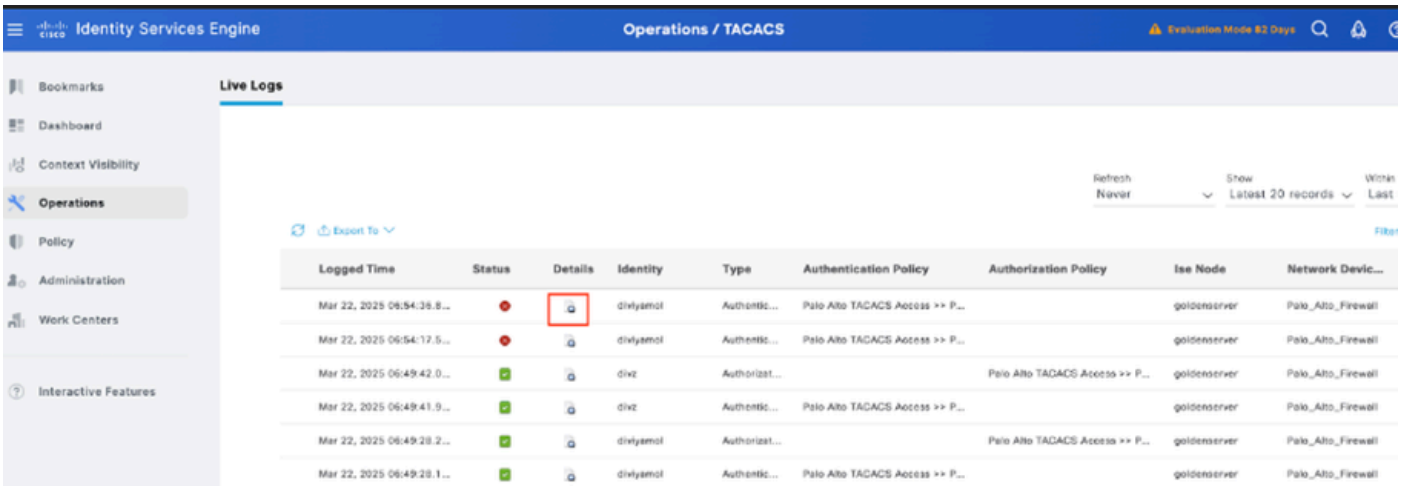
ステップ 1：TACACS+サービスアビリティが実行されているかどうかを確認します。これは次のようにチェックインできます。

- GUI:Administration -> System -> Deploymentで、サービスDEVICE ADMINとともにノードがリストされているかどうかを確認します。
- CLI：コマンドshow ports | include 49を実行して、TACACS+に属するTCPポートに接続があることを確認します

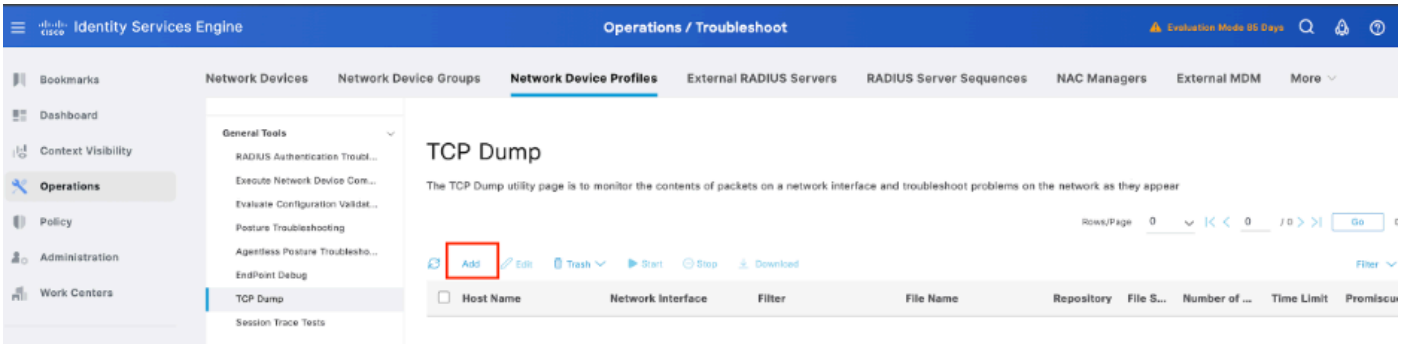
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

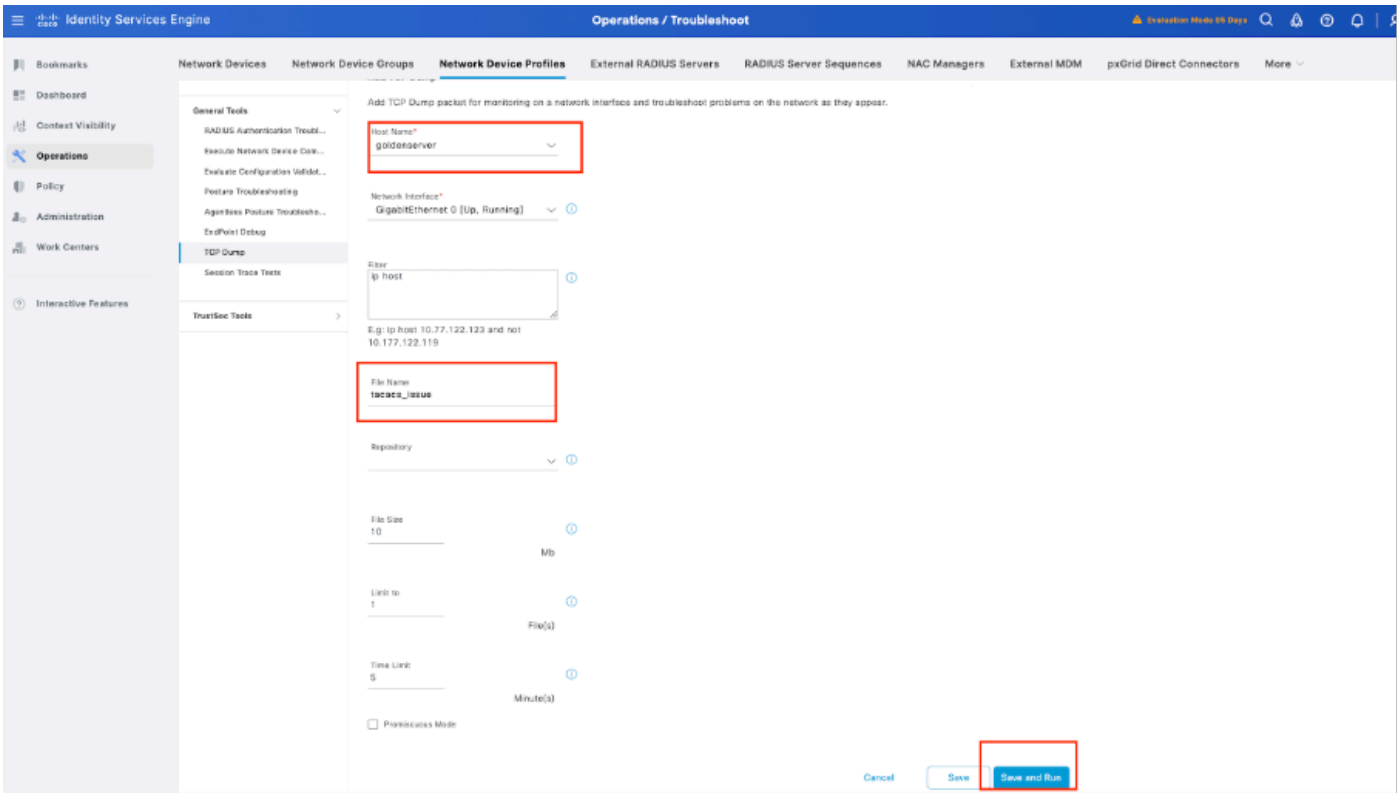
ステップ 2：TACACS+認証試行に関するライブログがあるかどうかを確認します(これは、「Operations -> TACACS -> Live logs」メニューで確認できます)。

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。



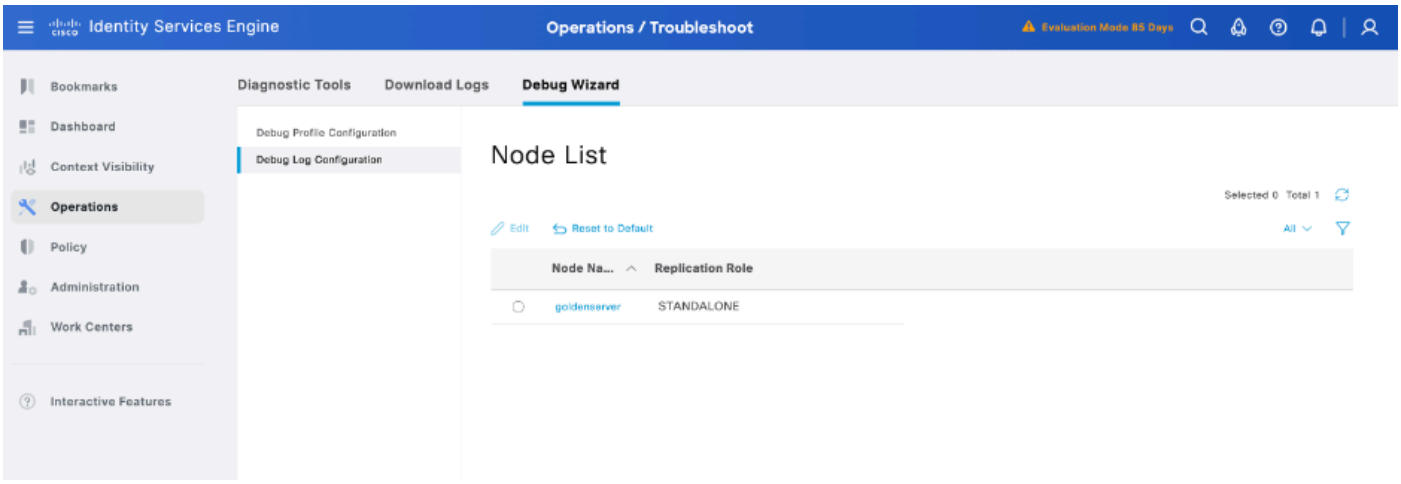
手順 3： ライブログが表示されない場合は、パケットキャプチャの実行に進み、Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dumpの順にメニューに移動し、Addを選択します。

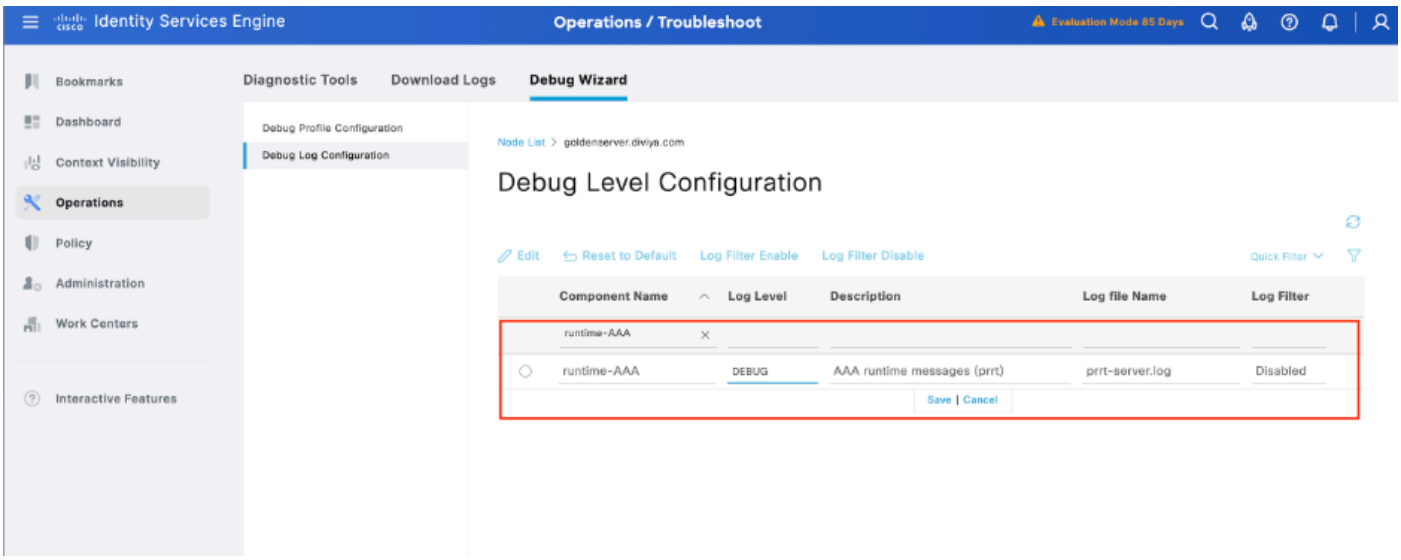




ステップ 4：認証が実行されるPSN内のデバッグのコンポーネントruntime-AAAを、Operations > Troubleshoot > Debug Wizard > Debug log configurationで有効にし、PSNノード（ノードID）を

選択してから、editボタンでnextを選択します。





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

TACACS：無効なTACACS+要求パケット – 共有秘密の不一致の可能性

問題

Cisco ISEとPalo Altoファイアウォール（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。
「Invalid TACACS+ request packet - possibly mismatched Shared Secrets」（無効なTACACS+要求パケット – 共有秘密が一致しない可能性があります）

Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/532805123/143
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-05-13 20:16:26.897000 +05:30
Logged Time	2025-05-13 20:16:26.897
Epoch Time (sec)	1747147586
ISE Node	goldenserver
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Failure Reason	
Resolution	
Root Cause	
Username	
Network Device Name	

これにより、管理ログインの成功が防止され、中央集中型の認証を通じてデバイスアクセス制御に影響を与える可能性があります。

考えられる原因

- Cisco ISEとPalo Altoファイアウォールまたはネットワークデバイスで設定されている共有秘密鍵の不一致。
- デバイスのTACACS+サーバ設定が正しくない（IPアドレス、ポート、プロトコルが正しくない）。

解決方法

この問題には、次のようないくつかの解決策があります。

1. 共有秘密を確認します。

- Cisco ISE上：
  Administration > Network Resources > Network Devicesの順に移動し、影響を受けるデバイスを選択して、共有秘密鍵を確認します。

- Palo Altoファイアウォール：
  Device > Server Profiles > TACACS+の順に選択し、大文字と小文字および特殊文字を含めて、共有秘密が正確に一致していることを確認します。

2. TACACS+サーバ設定を確認します。

- ファイアウォールのTACACS+プロファイルで、Cisco ISEの正しいIPアドレスとポート（デフォルトは49）が設定されていることを確認します。

- プロトコルタイプがTACACS+（RADIUSではない）であ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。