ISEギガビットイーサネット1インターフェイスを使用したTACACS+の設定

内容

はじめに

このドキュメントでは、ルータおよびスイッチがネットワークデバイスとして動作するギガビットイーサネット1インターフェイスを使用したISE TACACS+の設定について説明します。

背景説明

Cisco ISEは最大6つのイーサネットインターフェイスをサポートします。債券は、債券0、債券1、債券2の3つのみです。結合の一部であるインタフェースを変更したり、結合のインタフェー

スの役割を変更したりすることはできません。

前提条件

要件

次の項目に関する知識が推奨されます。

- ネットワークの基礎知識
- Cisco Identity Service Engine.

使用するコンポーネント

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

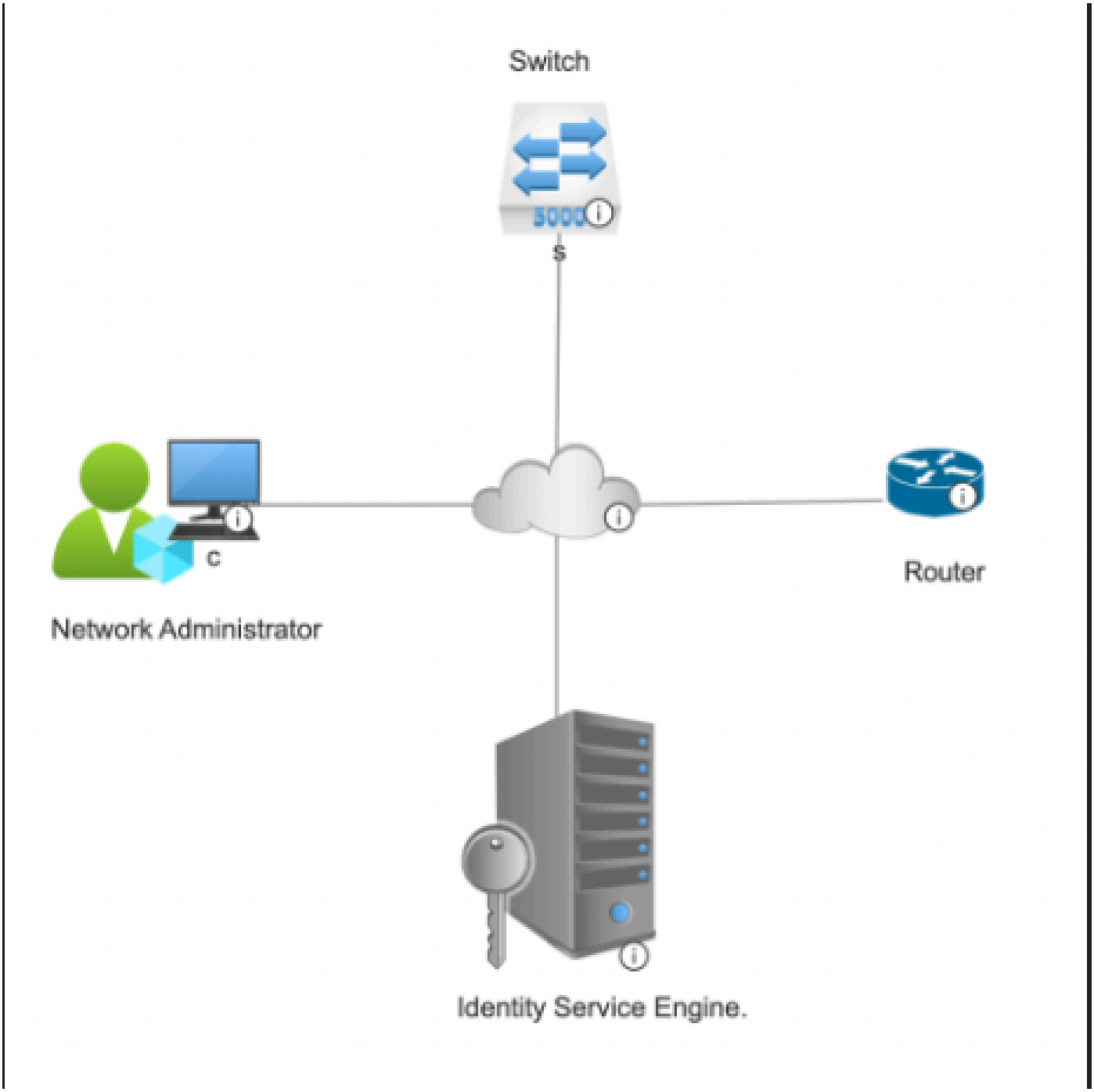
- Cisco Identity Service Engine v3.3
- Cisco IOS®ソフトウェアリリース17.x
- Cisco C9200スイッチ

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

設定の目的は、TACACS+用にISEのギガビットイーサネット1を設定し、TACACS+を使用するスイッチおよびルータをISEとともに認証サーバとして認証することです。

ネットワーク図

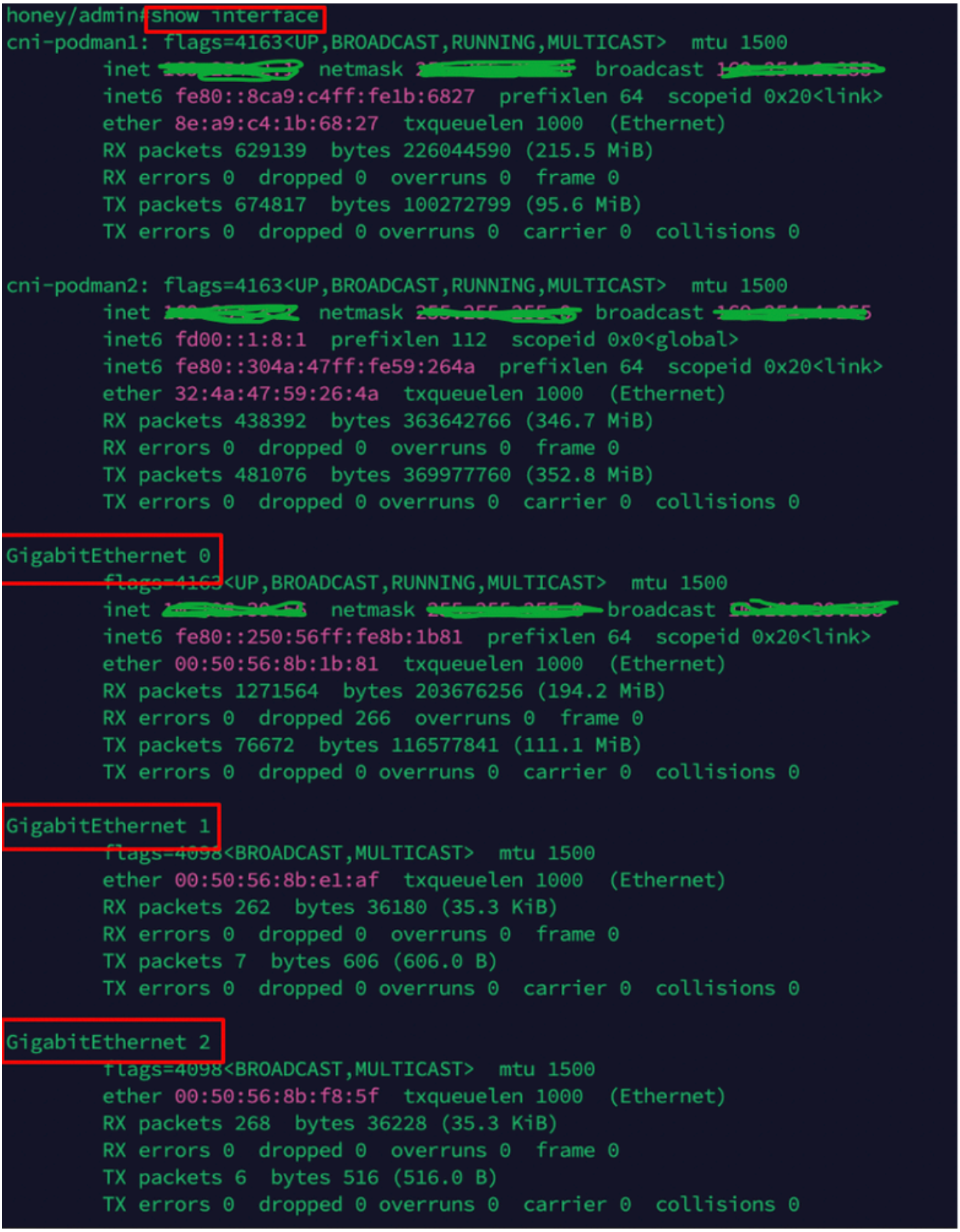


Network Topology

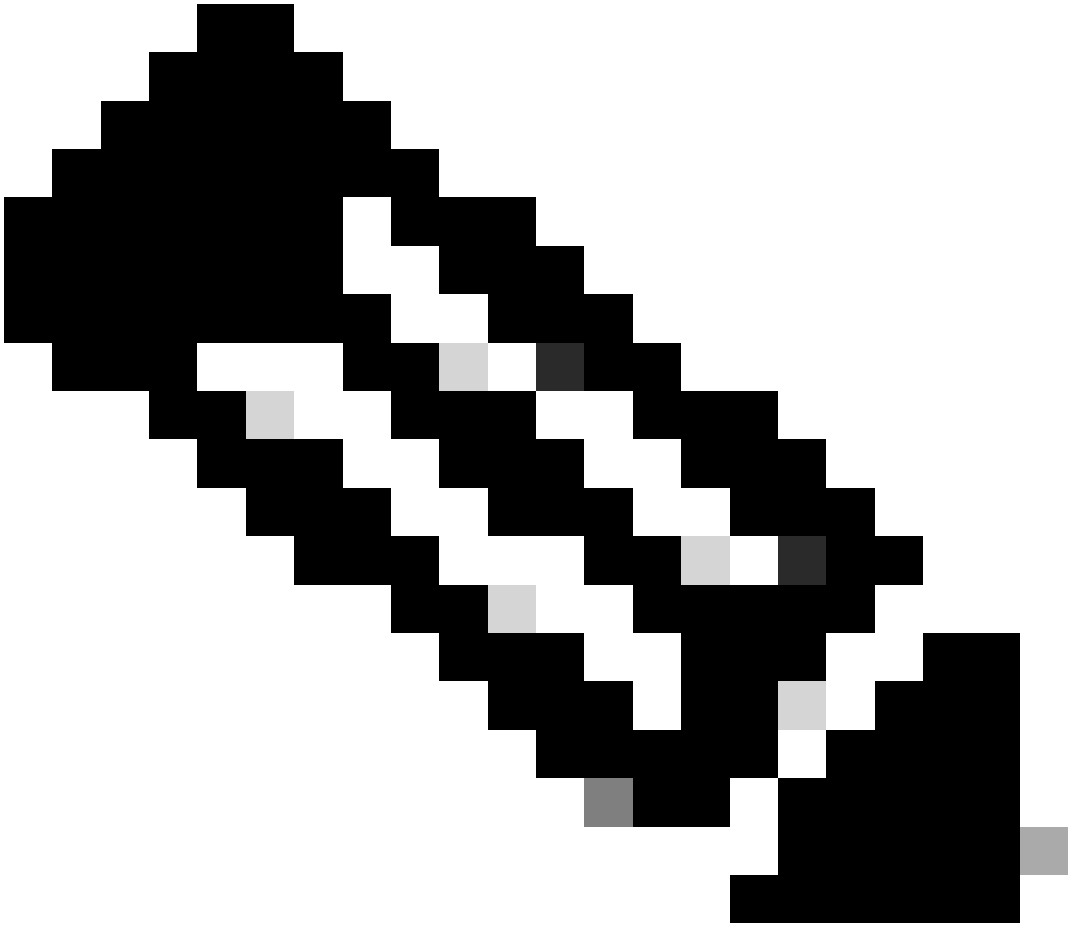
TACACS+用Identity Services Engineの設定

ISEでのギガビットイーサネット1インターフェイスのIPアドレスの設定

1. デバイスadminが有効になっているISE PSNノードのCLIにログインし、show interfaceコマンドを使用して使用可能なインターフェイスを確認します。



ISEのインターフェイスの検証



注：この設定では、ギガビットイーサネット1インターフェイスに重点を置いて、3つのインターフェイスだけがISEで設定されます。同じ手順を適用して、すべてのインターフェイスのIPアドレスを設定できます。デフォルトでは、ISEは最大6つのギガビットイーサネットインターフェイスをサポートします。

---

2. 同じPSNノードのCLIから、次のコマンドを使用して、ギガビットイーサネット1インターフェイスにIPアドレスを割り当てます。

hostnameofise#configure t

hostnameofise/admin(config)#interface Gigabit Ethernet 1

hostnameofise/admin(config-GigabitEthernet-1)# <ip address> <subnet netmask> % IPアドレスを変更すると、ISEサービスが再起動する場合があります

Continue with IP address change?

続行しますか？[yes,no]はい

3. ステップ2を実行すると、ISEノードサービスが再起動します。ISEサービスのステータスを確認するには、show application status iseコマンドを実行し、次のスクリーンショットに示すように、サービスのステータスがrunningになっていることを確認します。

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

ISEサービスステータスの検証

4. show interfaceコマンドを使用して、Gig1インターフェイスのIPアドレスを確認します。

V

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

CLIからのISE Gig2インターフェイスIPアドレスの確認

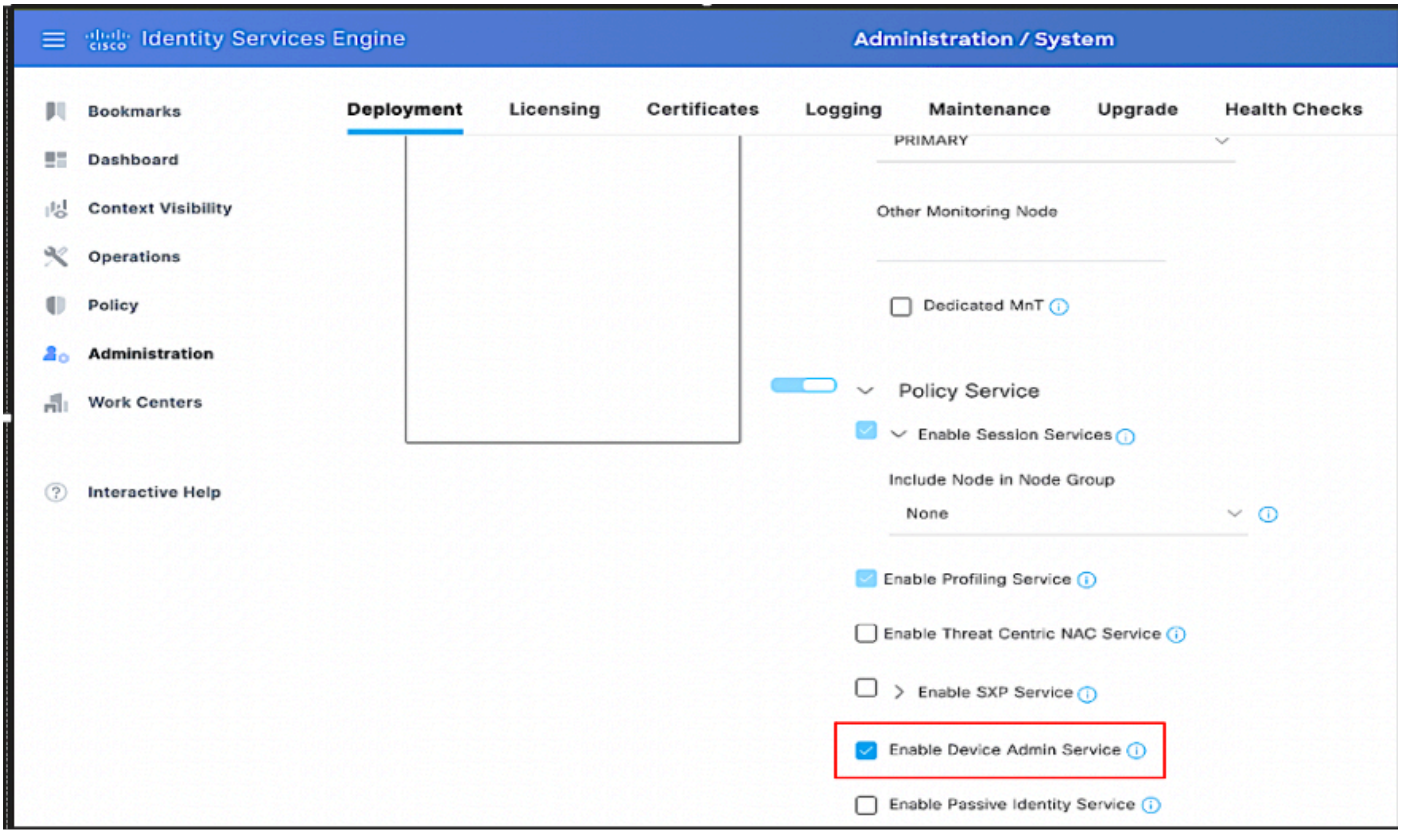
5.show ports | inc 49コマンドを使用して、ISEノードのポート49の割り当てを確認します。

```
honey/admin#show ports | include 49
        tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

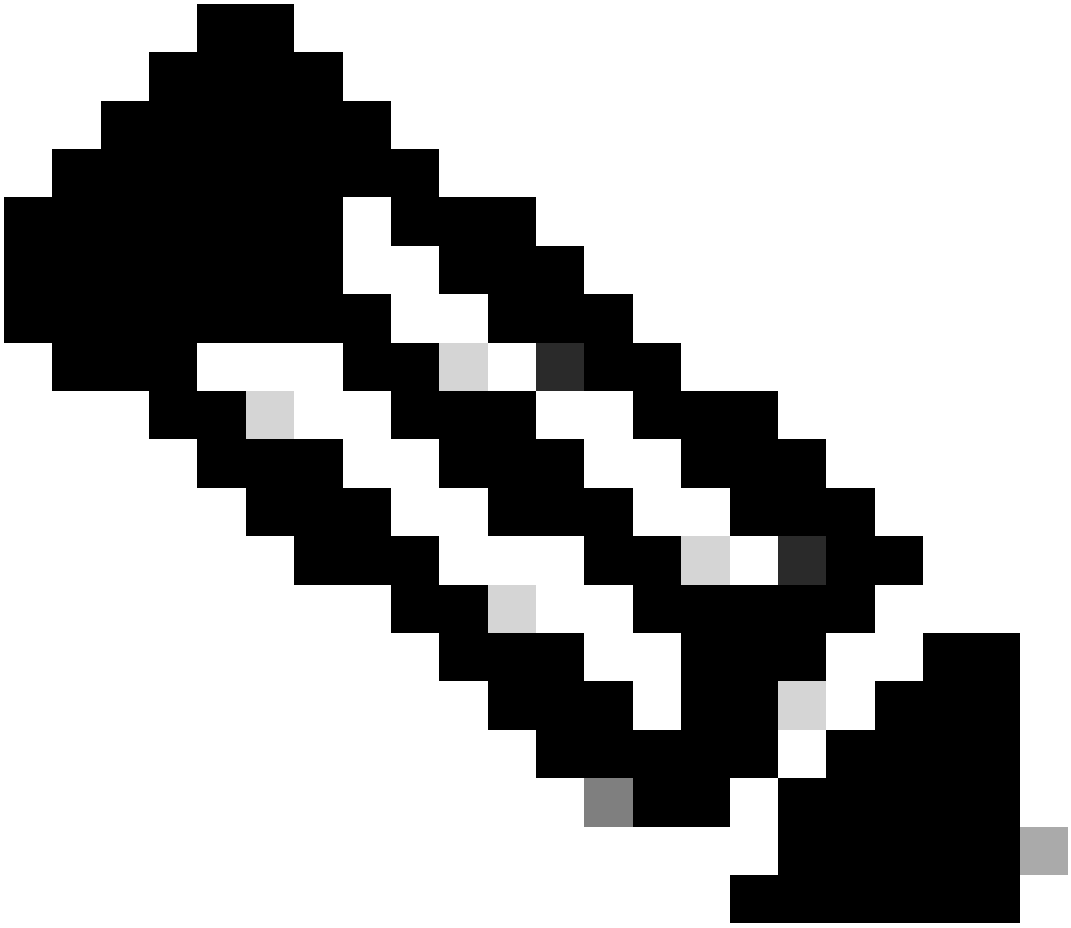
iseでのポート49許可の検証

ISEでのデバイス管理の有効化

ISEのGUI > Administration > Deployment > PSNノードを選択し、Enable Device admin serviceにチェックマークを付けます。



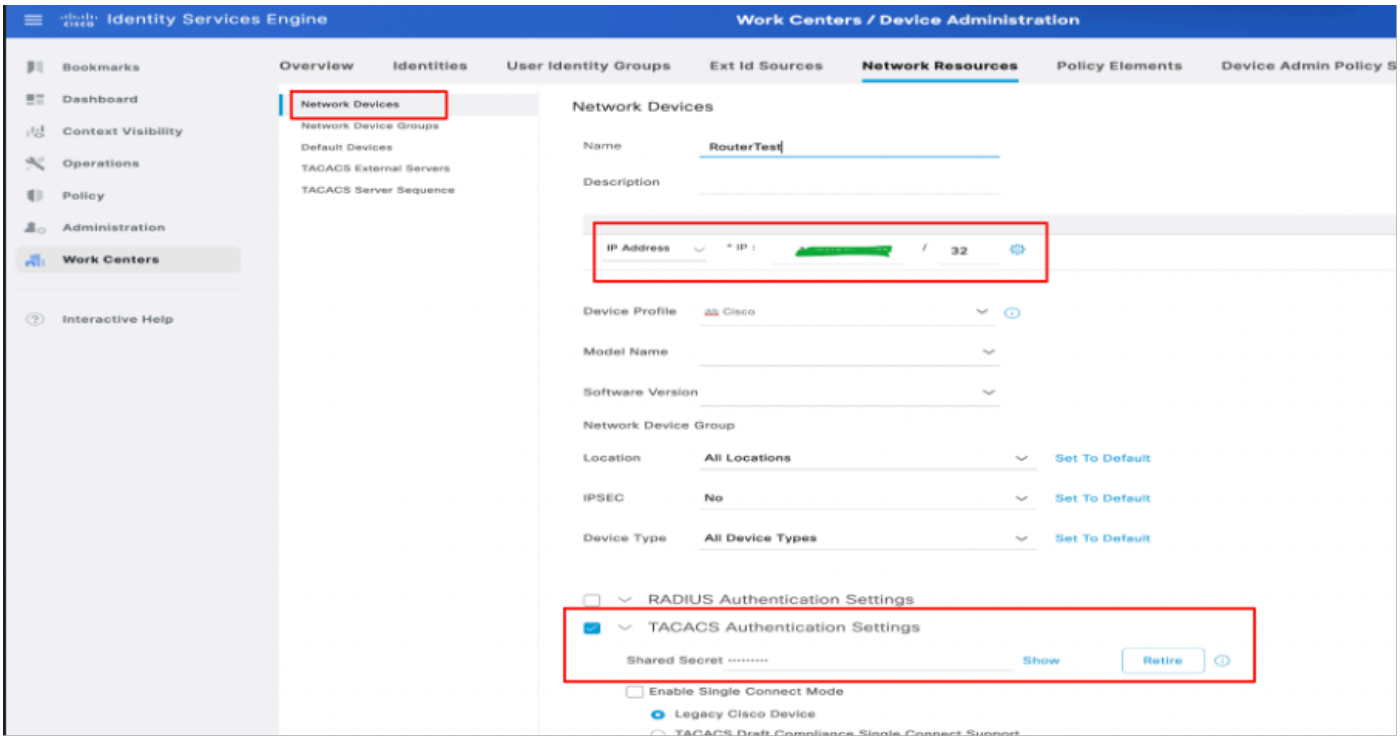
ISEでデバイス管理サービスを有効にする



注:Device Adminサービスを有効にするには、Device Administrationライセンスが必要です。

ISE でのネットワークデバイスの追加

1.ワークセンター>デバイス管理>ネットワークリソース>ネットワークデバイスに移動します。[Add] をクリックします。名前とIPアドレスを入力します。TACACS+ Authentication Settingsチェックボックスを選択して、共有秘密鍵を指定します。



ISEでのネットワークデバイスの設定

2. 上記の手順に従って、TACACS認証に必要なすべてのネットワークデバイスを追加します。

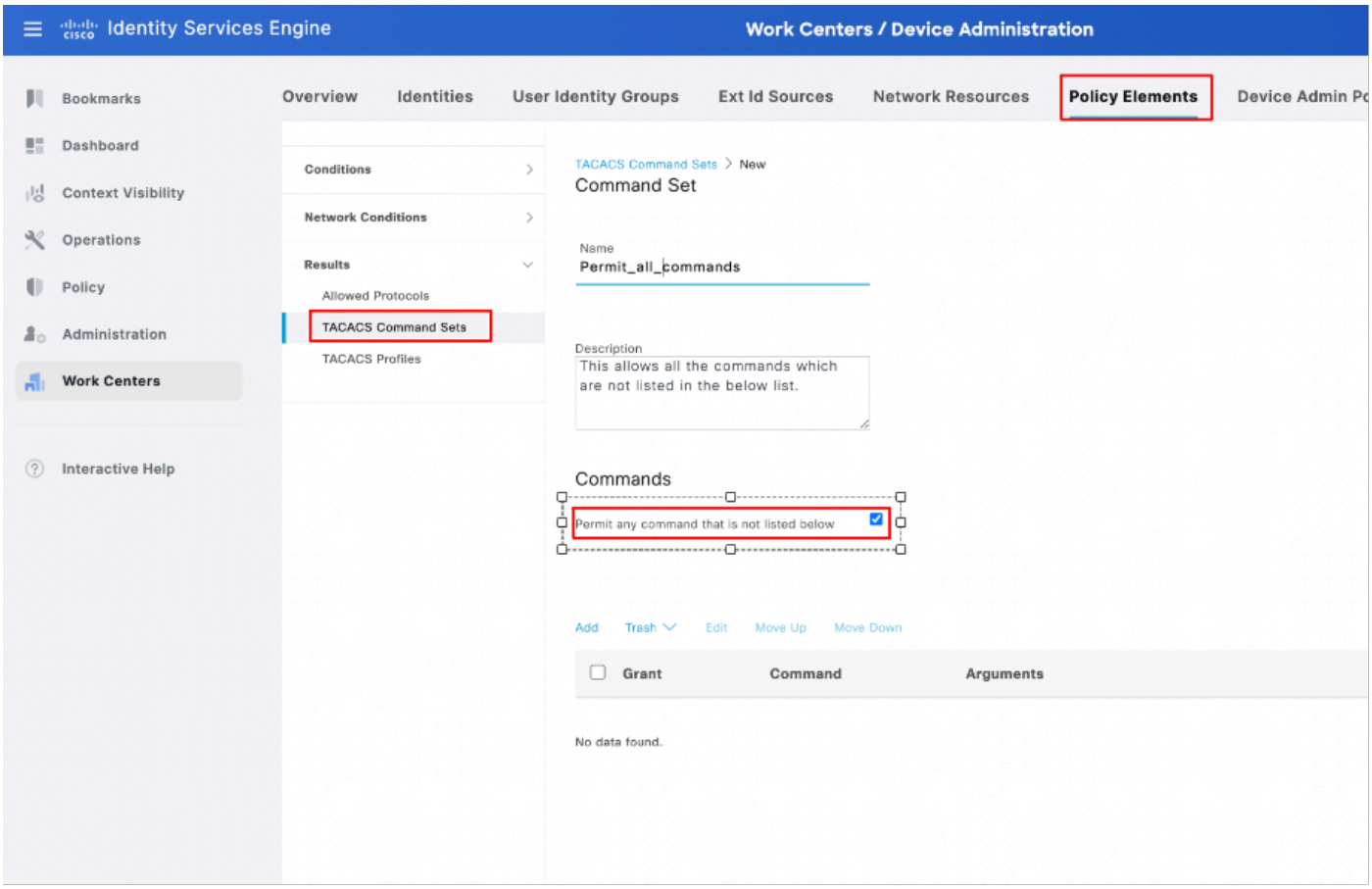
TACACS+コマンドセットの設定

このデモンストレーションでは、次の2つのコマンドセットを設定します。

Permit_all_commandsコマンドがユーザadminに割り当てられ、デバイスですべてのコマンドを許可します。

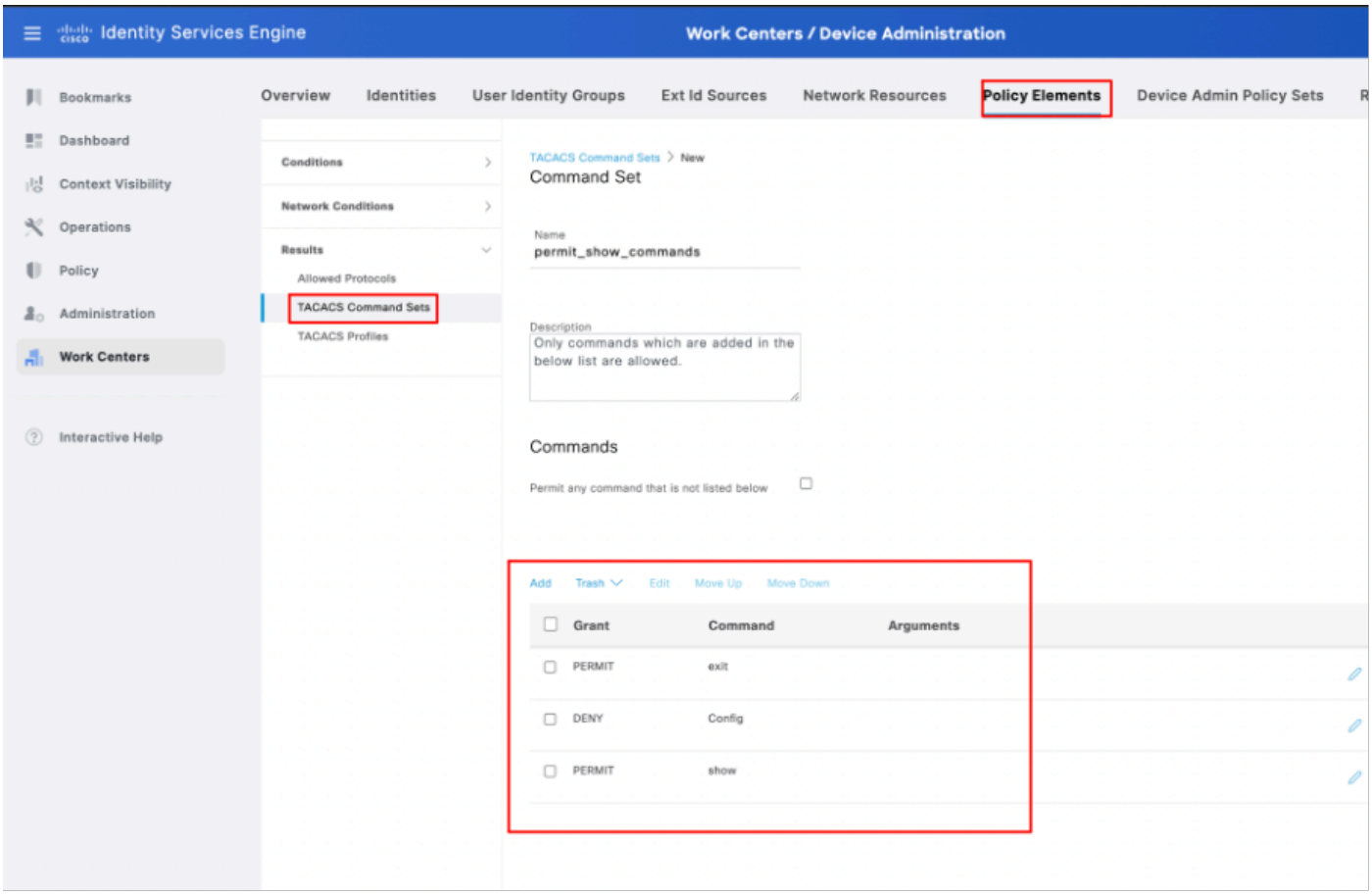
permit_show_commandsコマンドがユーザに割り当てられており、showコマンドだけが許可されます

1. [Work Centers] > [Device Administration] > [Policy Results] > [TACACS Command Sets] を選択します。 [Add] をクリックします。 名前を「PermitAllCommands」に指定し、表示されていない「Permit any command」チェックボックスを選択します。[Submit] をクリックします。



ISEでのコマンドセットの設定

2. Work Centers > Device Administration > Policy Results > TACACS Command Setsの順に移動します。 [Add] をクリックします。 名前を「PermitShowCommands」に指定し、Addをクリックし、最後に「permit」showコマンドと「exit」コマンドをクリックします。デフォルトでは、引数を空白のままにすると、すべての引数が含まれます。[Submit] をクリックします。

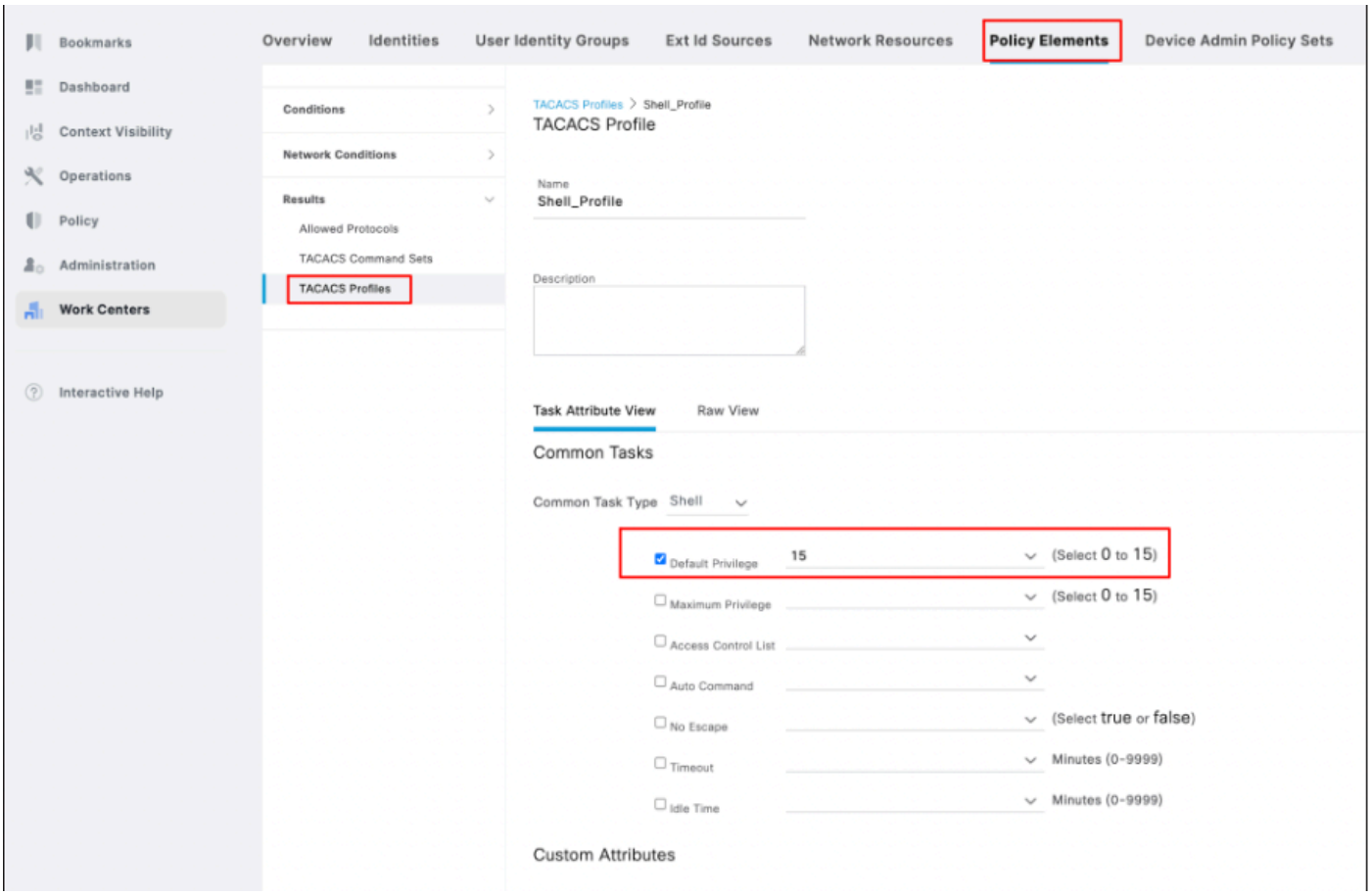


ISEでのpermit_show_commandsの設定

TACACS+プロファイルの設定

単一のTACACS+プロファイルが設定され、コマンド許可はコマンドセットを介して実行されます。

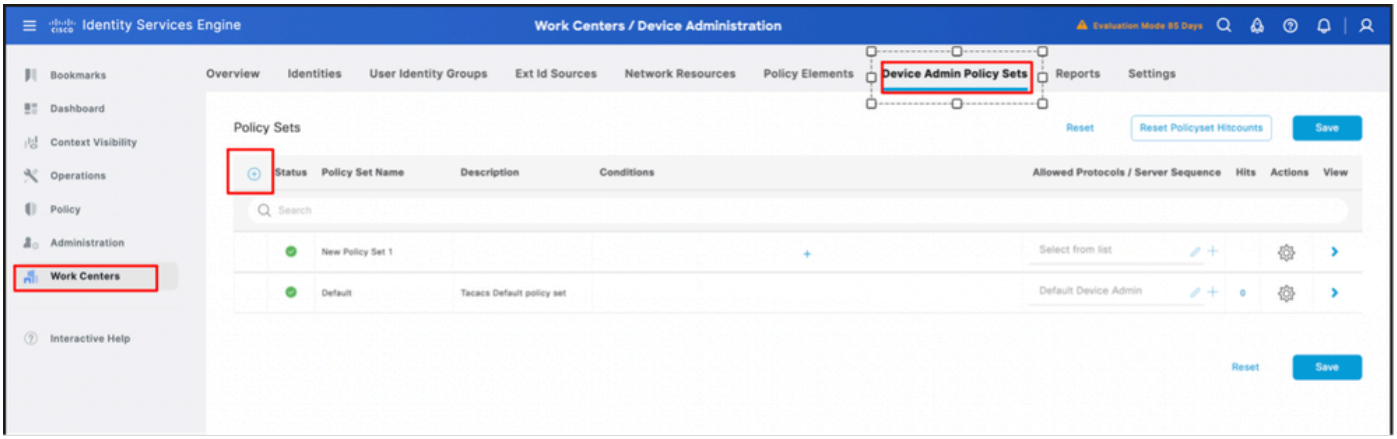
TACACS+プロファイルを設定するには、Work Centers > Device Administration > Policy Results > TACACS Profilesの順に選択します。Addをクリックして、シェルプロファイルの名前を指定し、Default Privilegeチェックボックスを選択して、値15を入力します。最後に、Submitをクリックします。



ISEでのTACACSプロファイルの設定

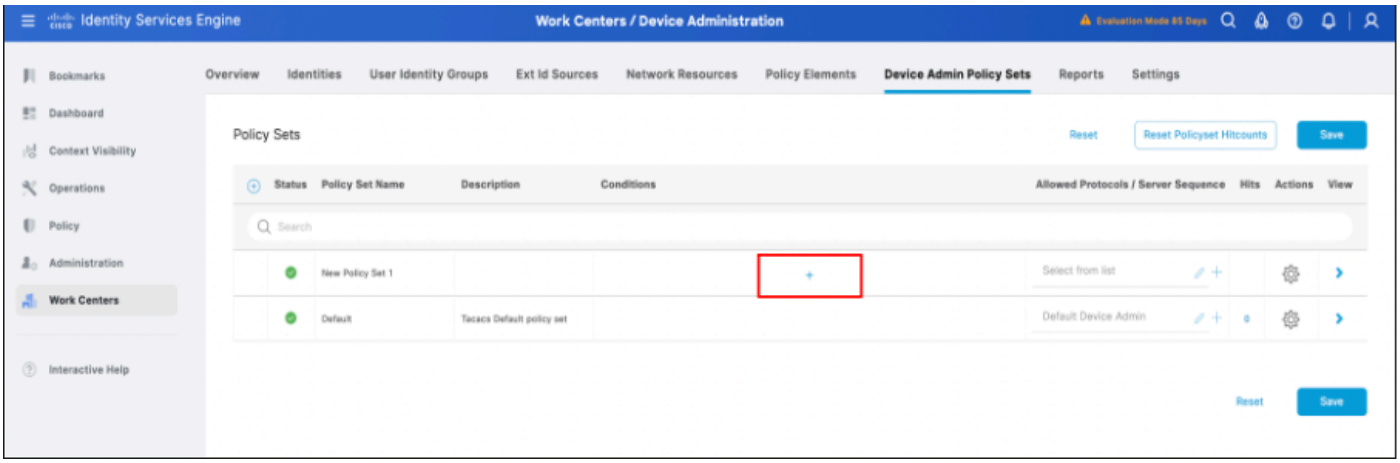
TACACS+認証および認可プロファイルの設定

1. ISE PAN GUI -> Administration -> Work Centers -> Device administration -> Device admin policy setsにログインします。+（プラス）アイコンをクリックして、新しいポリシーを作成します。この場合、ポリシーセットはNew Policy set 1という名前になります。



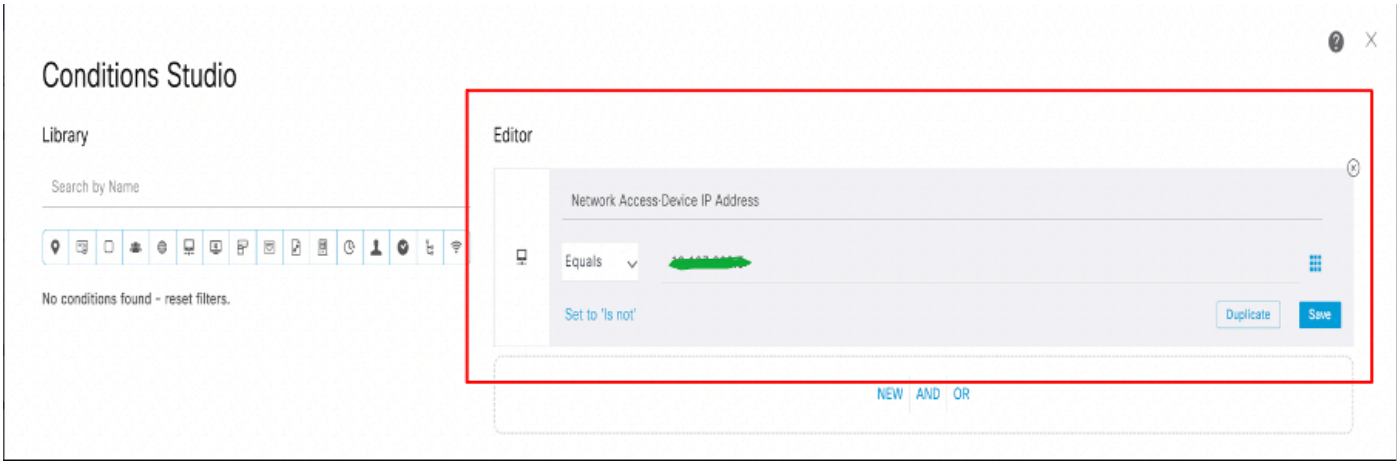
ISEでのポリシーセットの設定

2. ポリシーセットを保存する前に、次のスクリーンショットに示すように条件を設定する必要があります。+（プラス）アイコンをクリックして、ポリシーセットの条件を設定します。

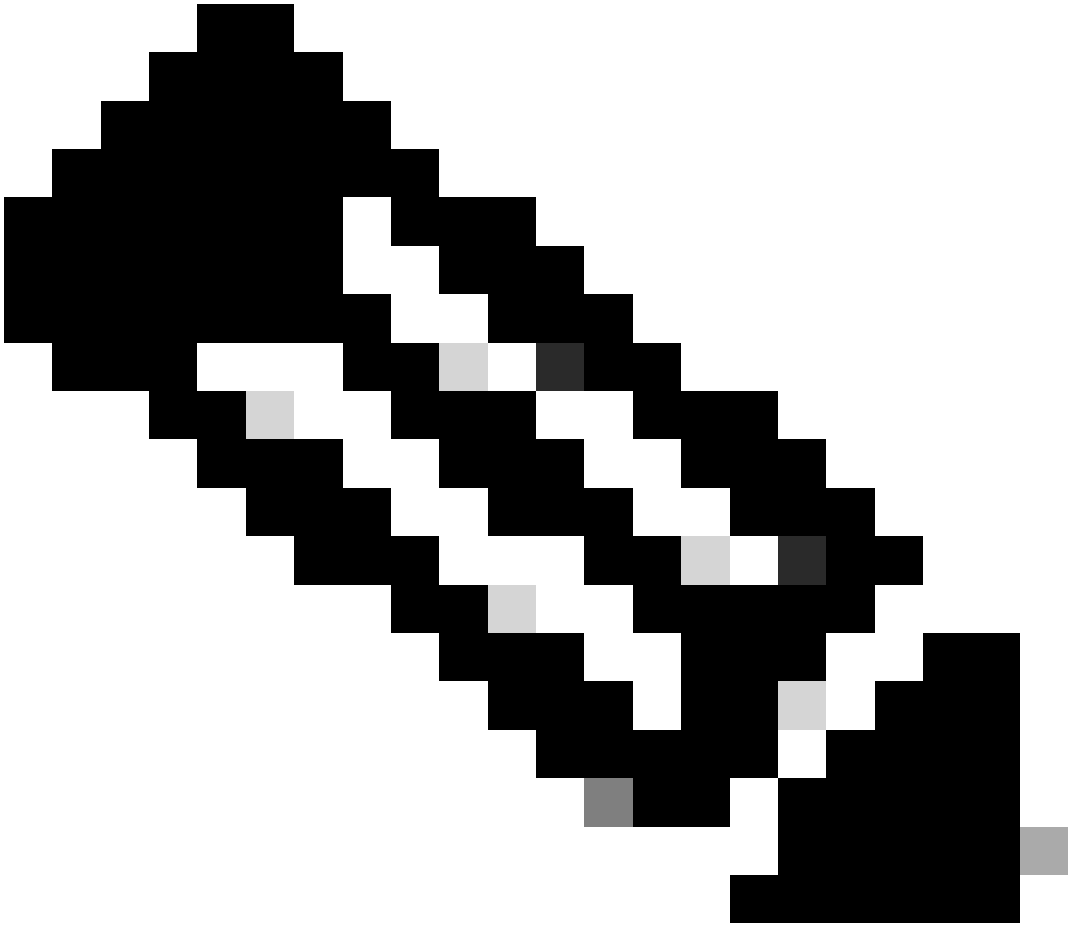


ISEでのポリシーセット条件の設定

3. ステップ2で説明した+ (プラス) アイコンをクリックすると、「conditions studio」ダイアログ・ボックスが開きます。そこで、必要な条件を設定します。 新しい条件または既存の条件で条件を保存し、スクロールします。useをクリックします。

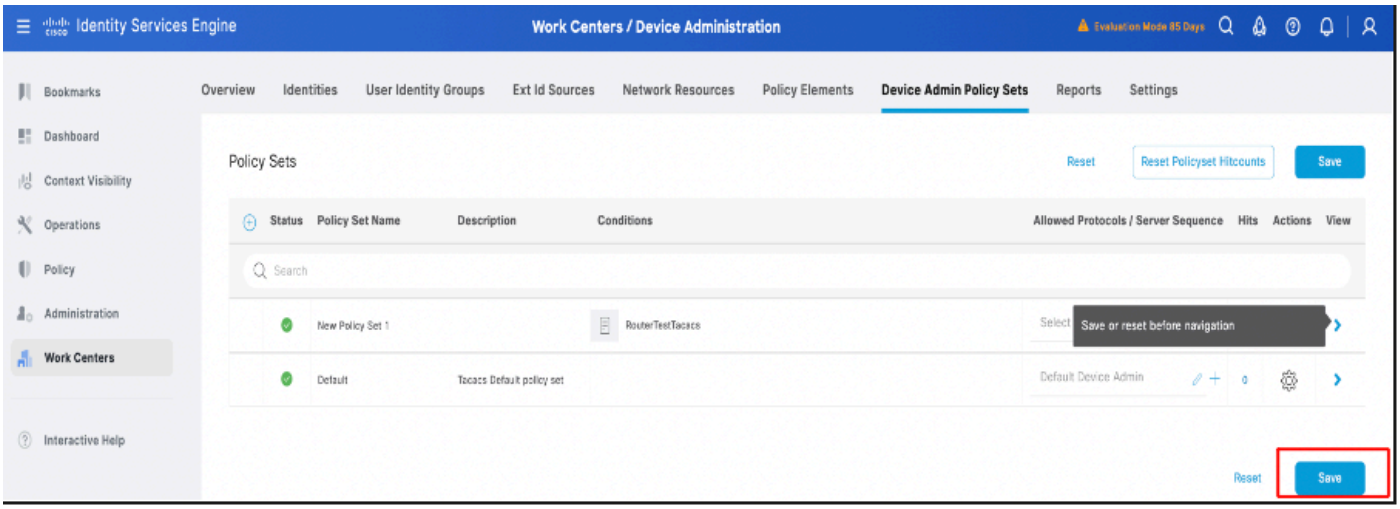


ISEでのポリシーセット条件の設定



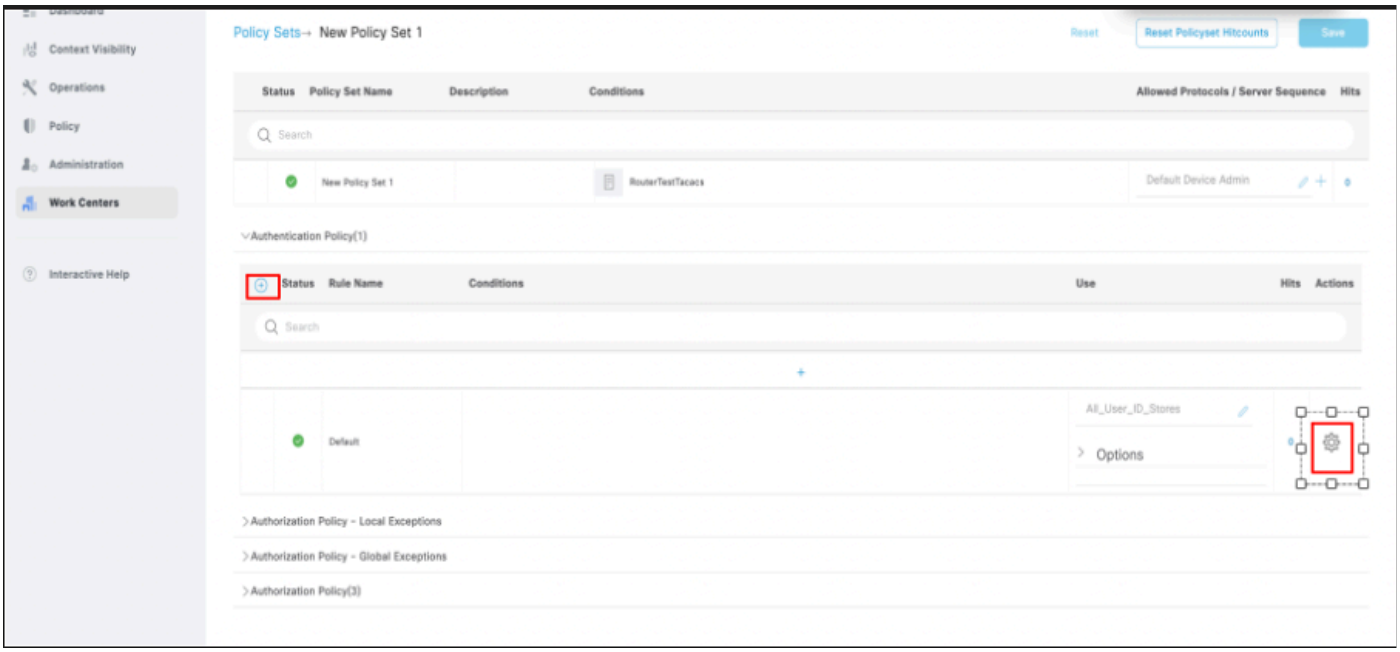
注：このドキュメントでは、条件はネットワークデバイスのIPと一致しています。ただし、導入要件に応じて条件を変更できます。

4. 条件を設定して保存した後、許可されるプロトコルをDefault device adminとして設定します。Saveオプションをクリックして、作成したポリシーセットを保存します。

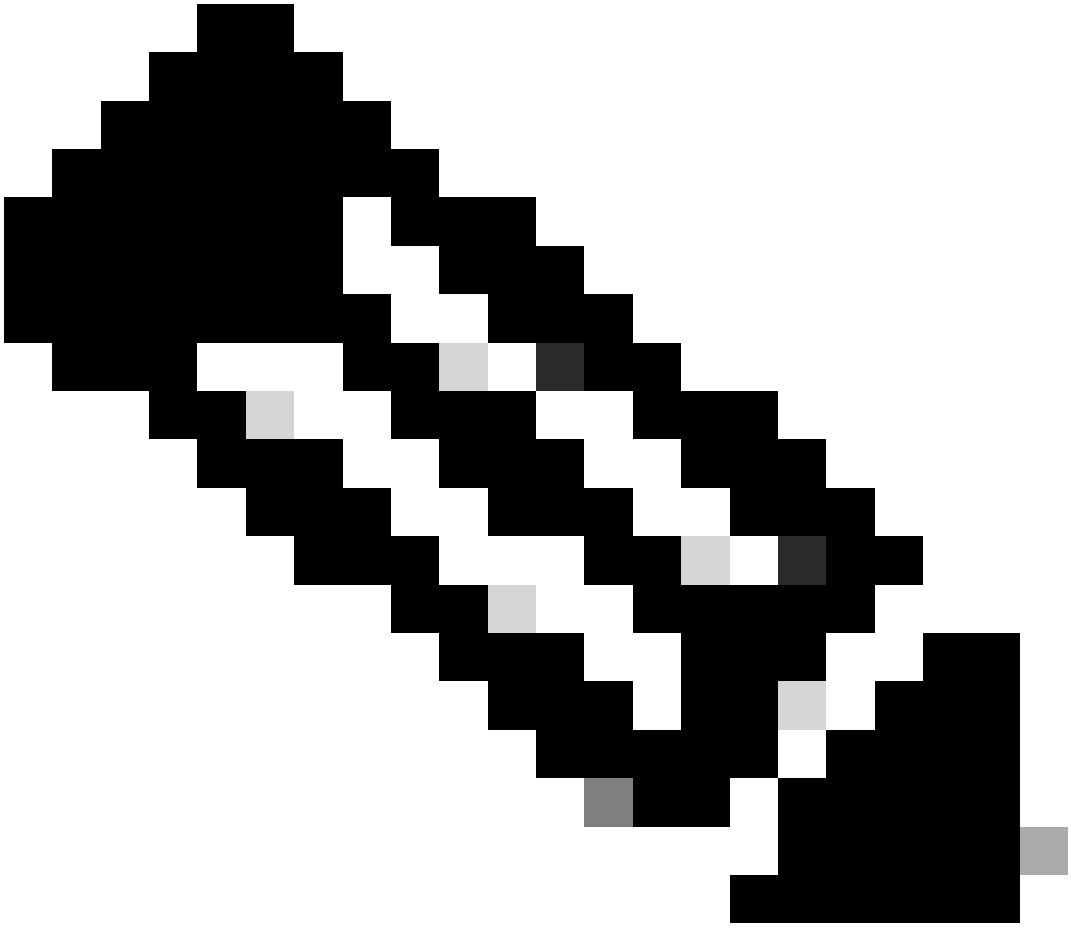


ポリシーセット設定の確認。

5. New Policy set -> Authentication Policy (1) -> Create a new authentication policy by click + (plus) アイコンをクリックするか、gear Iconをクリックしてから、Insert new row aboveをクリックして、新しい認証ポリシーを作成します。



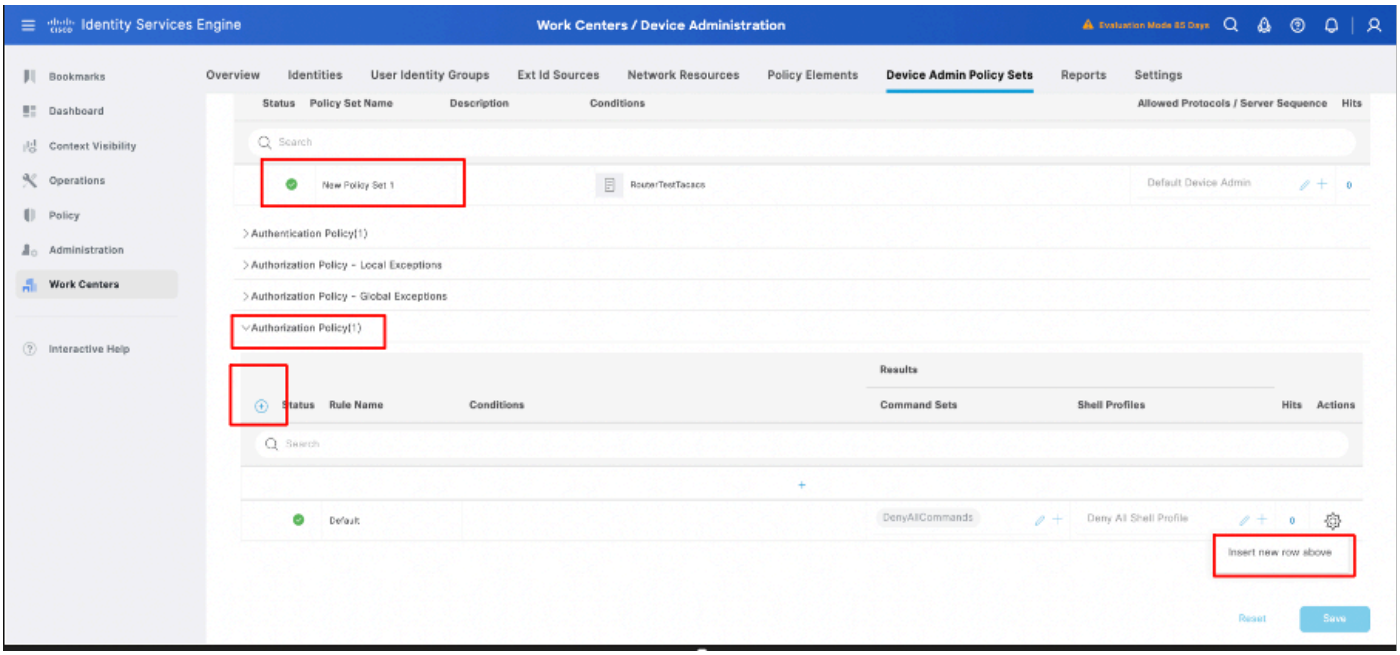
ポリシーセットの認証ポリシーの設定。



注：このデモンストレーションでは、All_User_ID_Storesで設定されているデフォルトの認証ポリシーが使用されます。ただし、IDストアの使用は、導入要件に従ってカスタマイズできます。

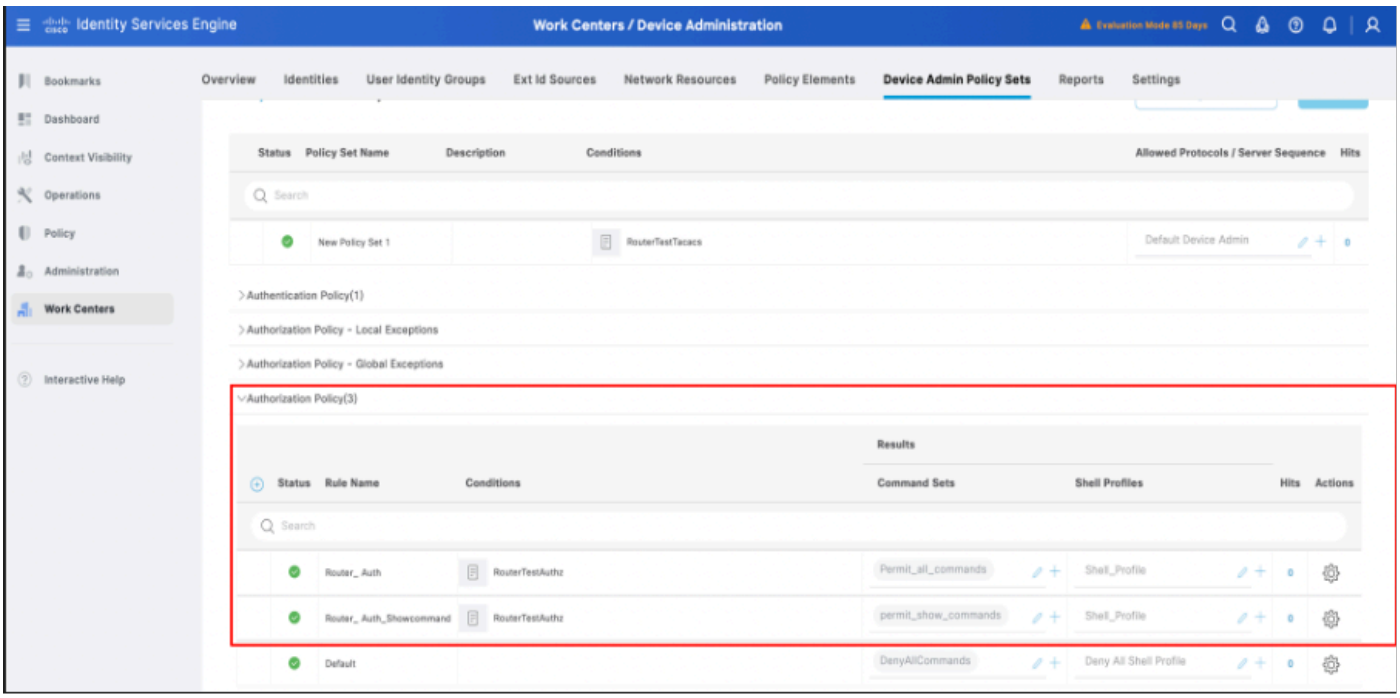
---

6. New Policy set -> Authorization Policy (1)の順に展開します。+（プラス）アイコンをクリックするか、歯車アイコンをクリックします。次に、認可ポリシーを作成するために新しい行を上に挿入します。

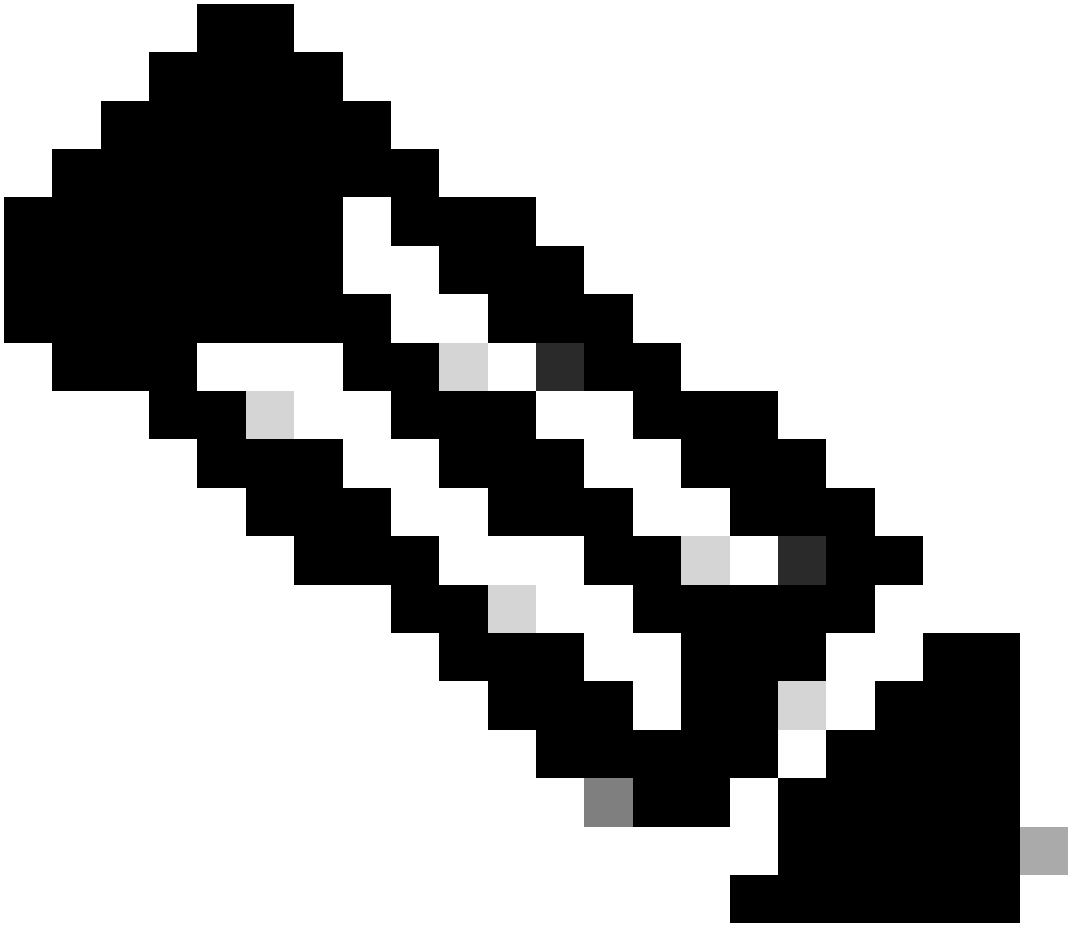


許可ポリシーの設定

7. 承認ポリシーにマップされた条件、コマンドセット、およびシェルプロファイルを使用して承認ポリシーを設定します。



ISEでの認可ポリシーの完全な設定

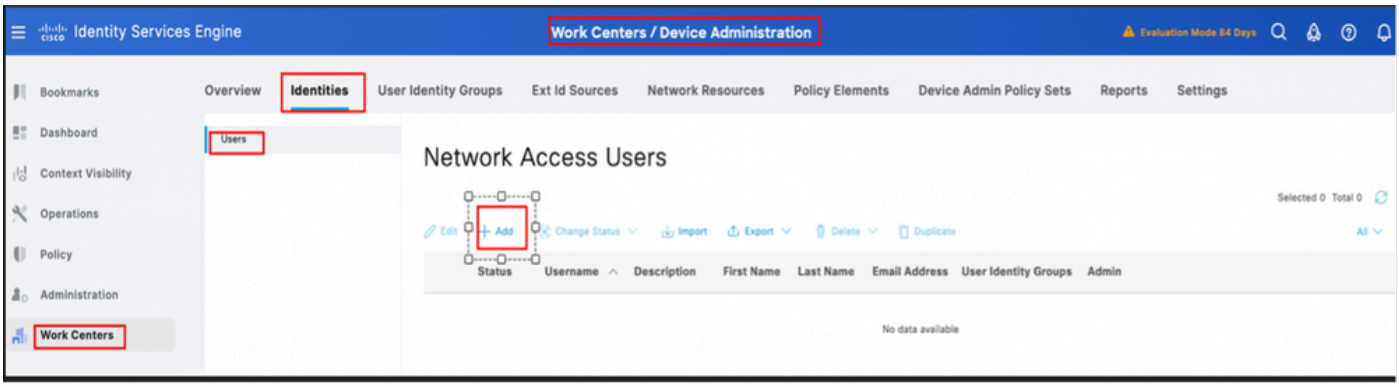


注：設定される条件はラボ環境に従ったものであり、導入要件に従って設定できます。

8. 最初の6つの手順に従って、スイッチまたはTACACS+に使用される他のネットワークデバイスのポリシーセットを設定します。

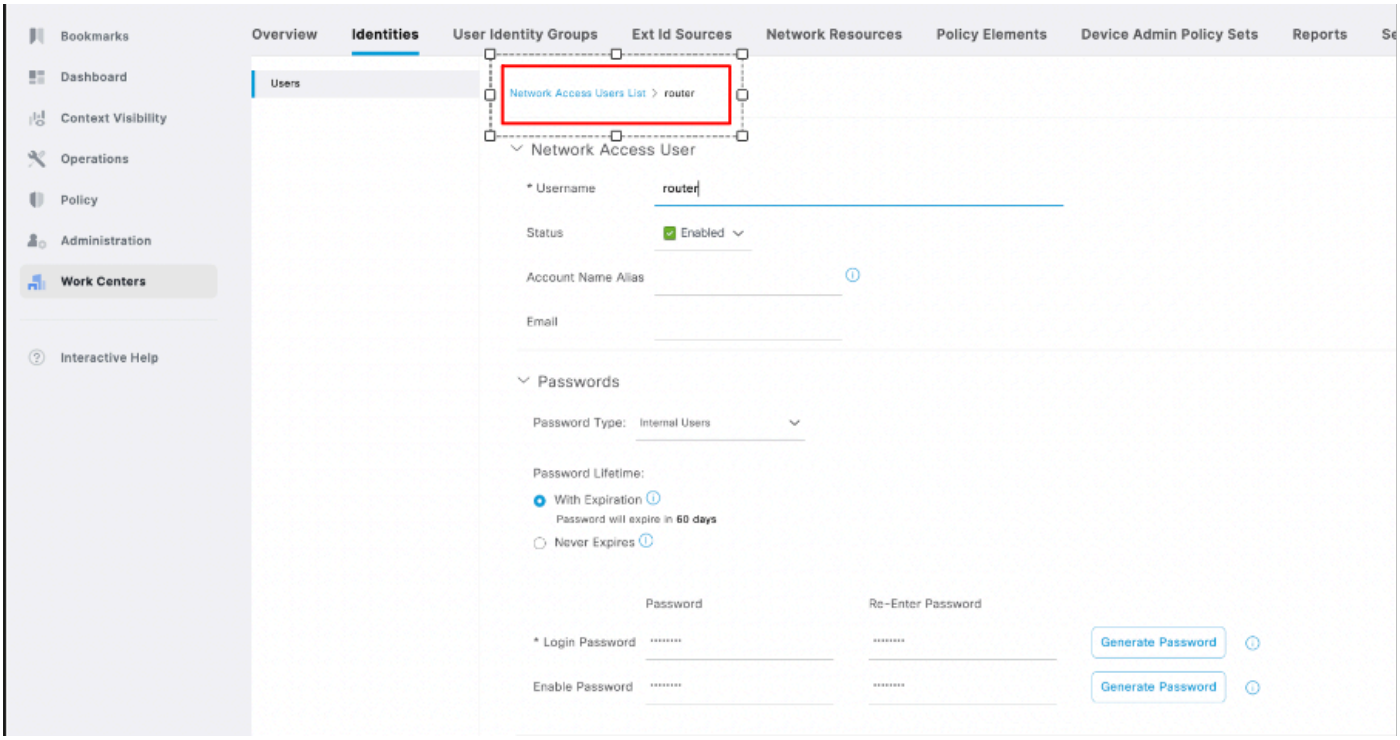
ISEでのNADのTACACS認証用のネットワークアクセスユーザの設定

1. Workcenters -> Device Administration -> Identities -> Usersの順に移動します。+ (プラス) アイコンをクリックして、新しいユーザを作成します。



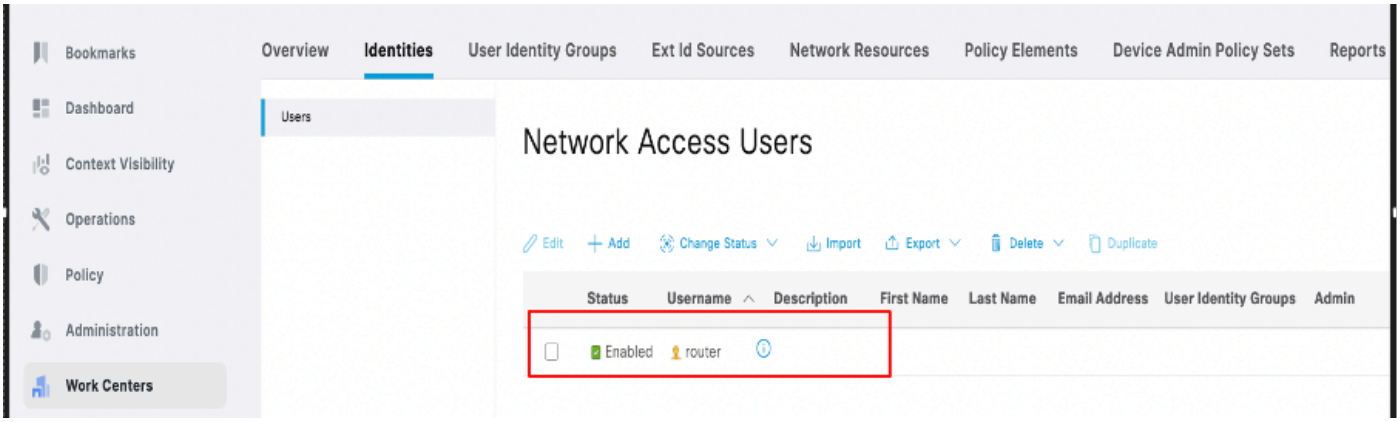
ISEでのネットワークアクセスユーザの設定

2. 「Username」および「Password」の詳細を展開するには、ユーザーをユーザーIDグループ（オプション）にマッピングし、「Submit」をクリックします。



ネットワークアクセスユーザの設定：続き

3. ユーザ名の設定をWork Centers -> Identities -> Users -> Network Access users で送信した後、ユーザは視覚的に設定され有効になっています。



TACACS+用のルータの設定

TACACS+認証および許可のためのCisco IOSルータの設定

1. ルータのCLIにログインし、次のコマンドを実行してルータにTACACSを設定します。

ASR1001-X(config)#aaa new-model:NADでaaaを有効にするために必要なコマンド

ASR1001-X(config)#aaa session-id共通— NADでaaaを有効にするために必要なコマンド。

ASR1001-X(config)#aaa authentication login default group tacacs+ local

ASR1001-X(config)#aaa認証exec defaultグループtacacs+

ASR1001-X(config)#aaa許可ネットワークリスト1グループtacacs+

ASR1001-X(config)#tacacsサーバise1

ASR1001-X(config-server-tacacs)#address ipv4 <TACACSサーバのIPアドレス> . — ISEインターフェイスG1 IPアドレス。

ASR1001-X(config-server-tacacs)#キーXXXXX

ASR1001-X(config)# aaa group server tacacs+ isegroup

ASR1001-X(config-sg-tacacs+)#serverの名称ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1

ASR1001-X（設定）#exit

2. ルータのTACACS+設定を保存した後、show run aaaコマンドを使用してTACACS+の設定を確認します。

ASR1001-X#show run aaa

!

AAA認証ログインデフォルトグループISEGROUPローカル

AAA許可EXECデフォルトグループISEGROUP

aaa許可ネットワークリスト1グループisegroup

username admin password 0 XXXXXXX

!

tacacsサーバise1

address ipv4:TACACSサーバのIPアドレス

キーXXXXX

!

!

aaaグループサーバtacacs+ isegroup

サーバ名ise1

ip vrf forwarding Mgmt-intf

ip tacacs source-interface GigabitEthernet1

!

!

!

aaa new-model

aaa session-id共通

!

!

TACACS+用のスイッチの設定

TACACS+認証および認可のためのスイッチの設定

1. スイッチのCLIにログインし、次のコマンドを実行してスイッチにTACACSを設定します。

C9200L-48P-4X#設定t

Enter configuration commands, one per line. CNTL/Z で終了します。

C9200L-48P-4X(config)#aaa newモデル。— NADでaaaを有効にするために必要なコマンド

C9200L-48P-4X(config)#aaa session-id common.— NADでaaaを有効にするために必要なコマンド。

C9200L-48P-4X(config)#aaa authentication login default group isegroup local

C9200L-48P-4X(config)#aaa認証execデフォルトグループisegroup

C9200L-48P-4X(config)#aaa認証ネットワークリスト1グループisegroup

C9200L-48P-4X(config)#tacacsサーバise1

C9200L-48P-4X(config-server-tacacs)#address ipv4 <TACACSサーバのIPアドレス>:ISEインターフェイスG1 IPアドレス。

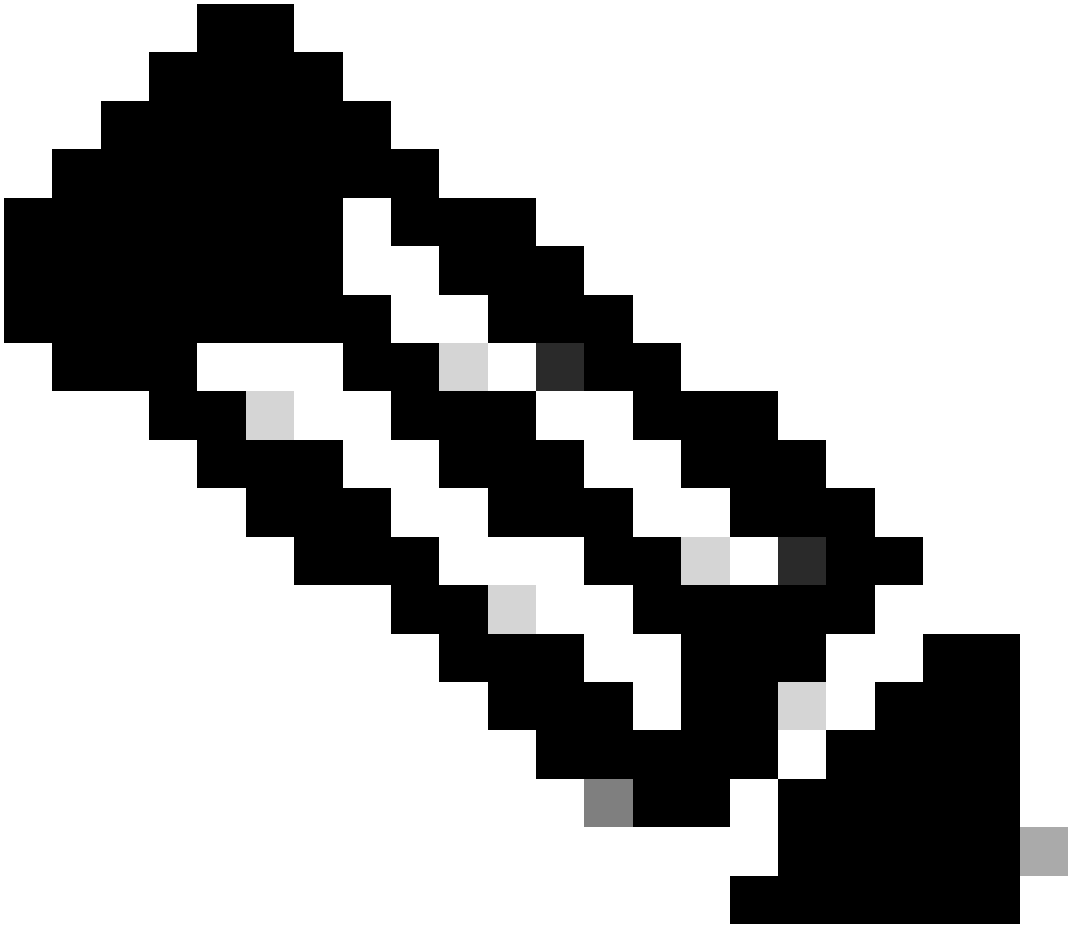
C9200L-48P-4X(config-server-tacacs)#key XXXXX

C9200L-48P(config)#aaaグループサーバtacacs+ isegroup

C9200L-48P(config-sg-tacacs+)#server名称ise1

C9200L-48P-4X（構成）#exit

C9200L-48P-4X#wr mem



注:NAD TACACS+設定で、tacacs+ は導入要件に従ってカスタマイズできるグループです。

2. スイッチのTACACS+設定を保存した後、show run aaaコマンドを使用して、TACACS+の設定を確認します。

C9200L-48P#show run aaa

!

AAA認証ログインデフォルトグループISEGROUPローカル

AAA許可EXECデフォルトグループISEGROUP

aaa許可ネットワークリスト1グループisegroup

ユーザ名adminパスワード0 XXXXX

!

!

tacacsサーバise1

address ipv4:TACACSサーバのIPアドレス

キーXXXXX

!

!

aaaグループサーバtacacs+ isegroup

サーバ名ise1

!

!

!

aaa new-model

aaa session-id共通

!

!

検証

ルータからの確認

ルータのCLIで、test aaa group tacacsgroupname username password newコマンドを使用して、ギガビットイーサネット1インターフェイスのISEに対するTACACS+のセキュリティ認証を行います。

ルータとISEからの出力例を次に示します。

ルータからのポート49の確認：

ASR1001-X#telnet ISE Gig 1インターフェイスIP 49

ISE GIg 1インターフェイスIPを試行しています，49...開く

ASR1001-X#test aaa group isegroup router XXXX new

パスワードの送信

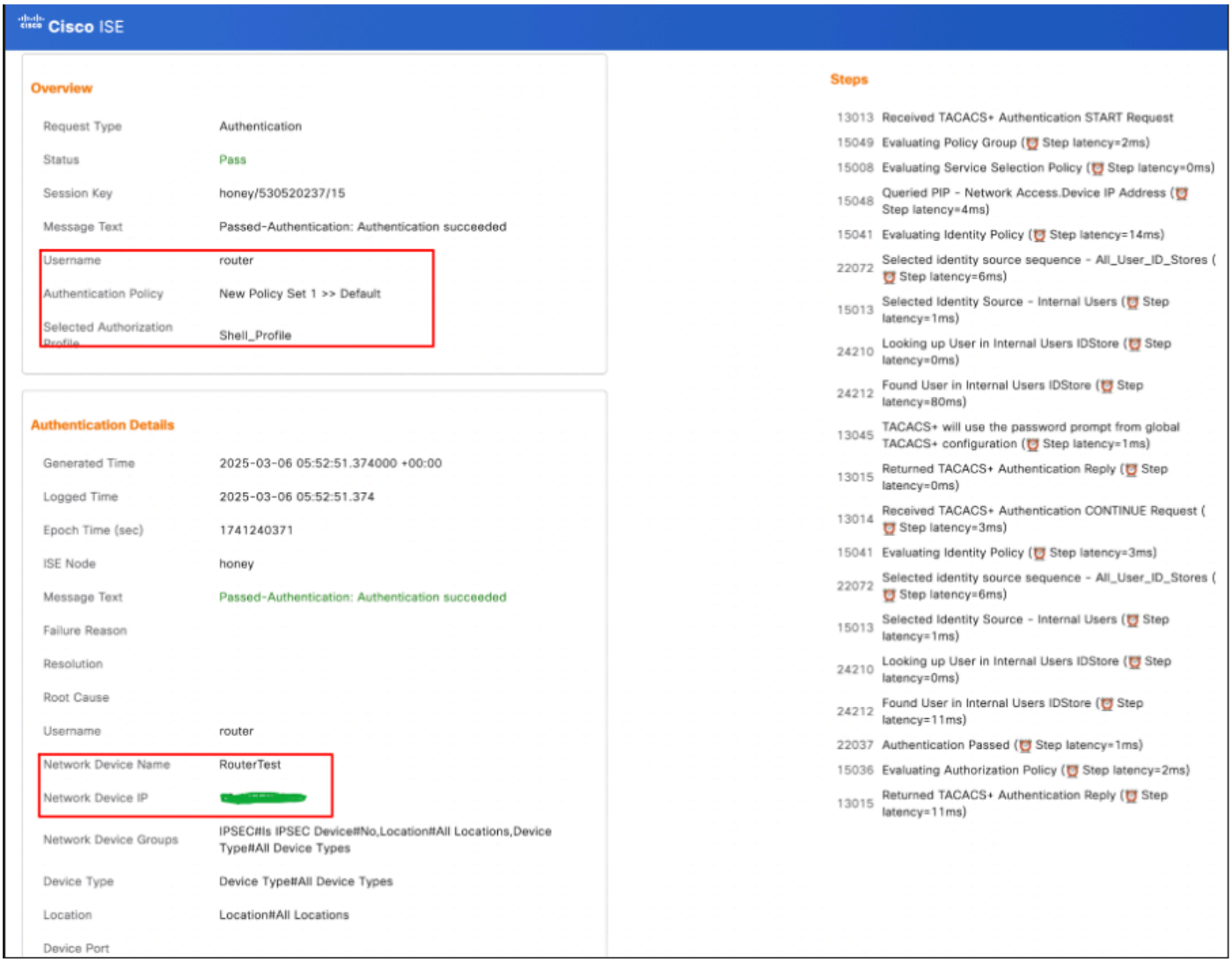
ユーザーが正常に認証されました

ユーザ属性

ユーザ名0「ルータ」

reply-message 0「パスワード：」

ISEから確認するには、GUI -> Operations -> TACACS live logsにログインし、Network Device Detailsフィールドでルータ IPを使用してフィルタリングします。



ISEからのTACACSライブログ：ルータの検証。

スイッチの検証

スイッチのCLIから、test aaa group tacacsgroupname username password newn コマンドを使用して、ギガビットイーサネット1インターフェイスのISEに対するTACACS+の認証を確認します。

これは、スイッチとISEからの出力例です。

スイッチからのポート49の確認：

C9200L-48P# telnet ISE Gig1インターフェイスIP 49

ISE Gig1インターフェイスIPを試行， 49...開く

C9200L-48P#test aaa group isegroup switch XXXX new

パスワードの送信

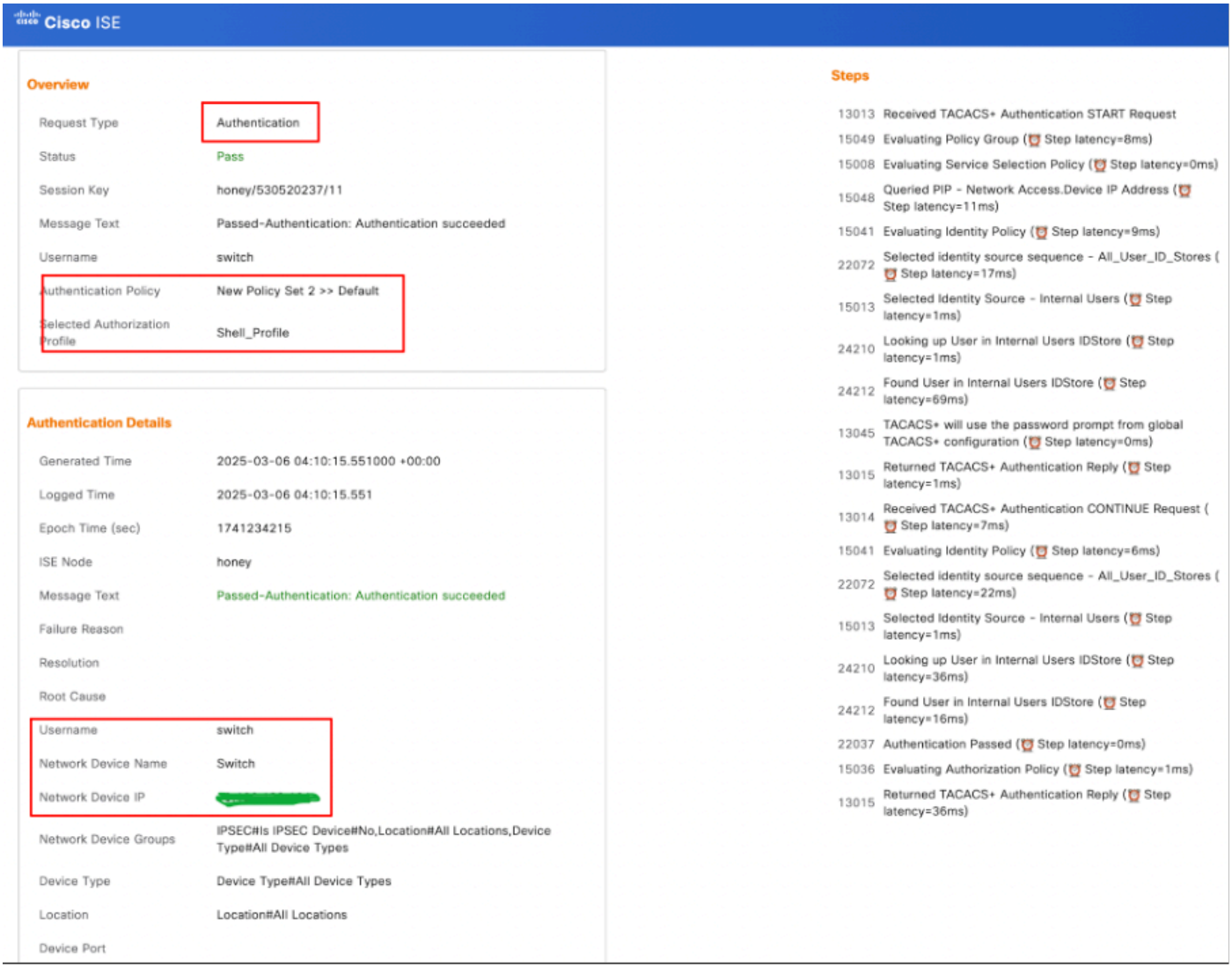
ユーザーが正常に認証されました

ユーザ属性

ユーザ名0「スイッチ」

reply-message 0「パスワード：」

ISEから確認するには、GUI -> Operations -> TACACS live logsにログインし、Network Device Detailsフィールドのスイッチ IPでフィルタリングします。



ISEからのTACACSライブログ：スイッチの検証。

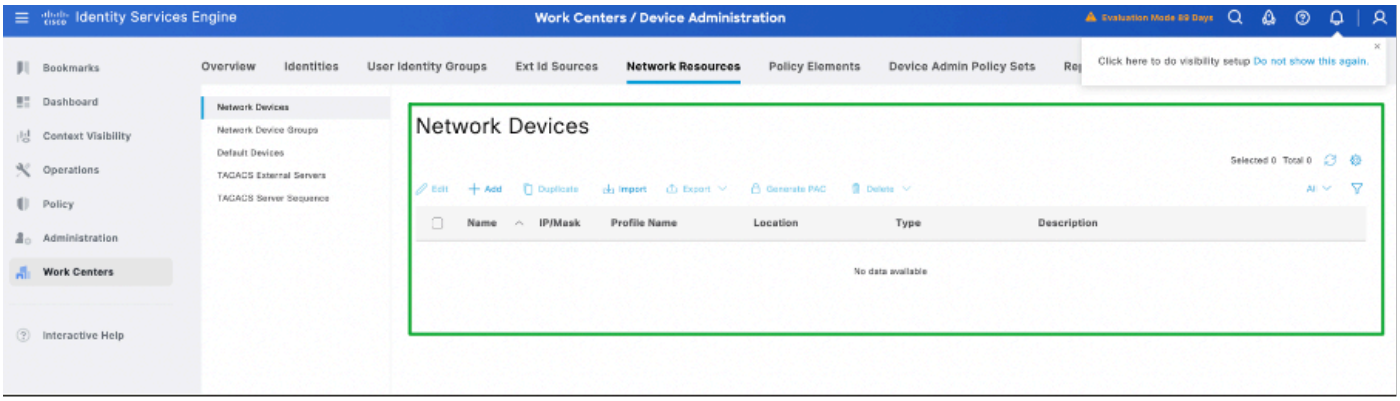
トラブルシュート

このセクションでは、TACACS+認証に関連して見つかる一般的な問題のいくつかについて説明します。

シナリオ1:TACACS+認証が「Error: 13017 Receved TACACS+ packet from unknown Network Device or AAA Client」で失敗する。

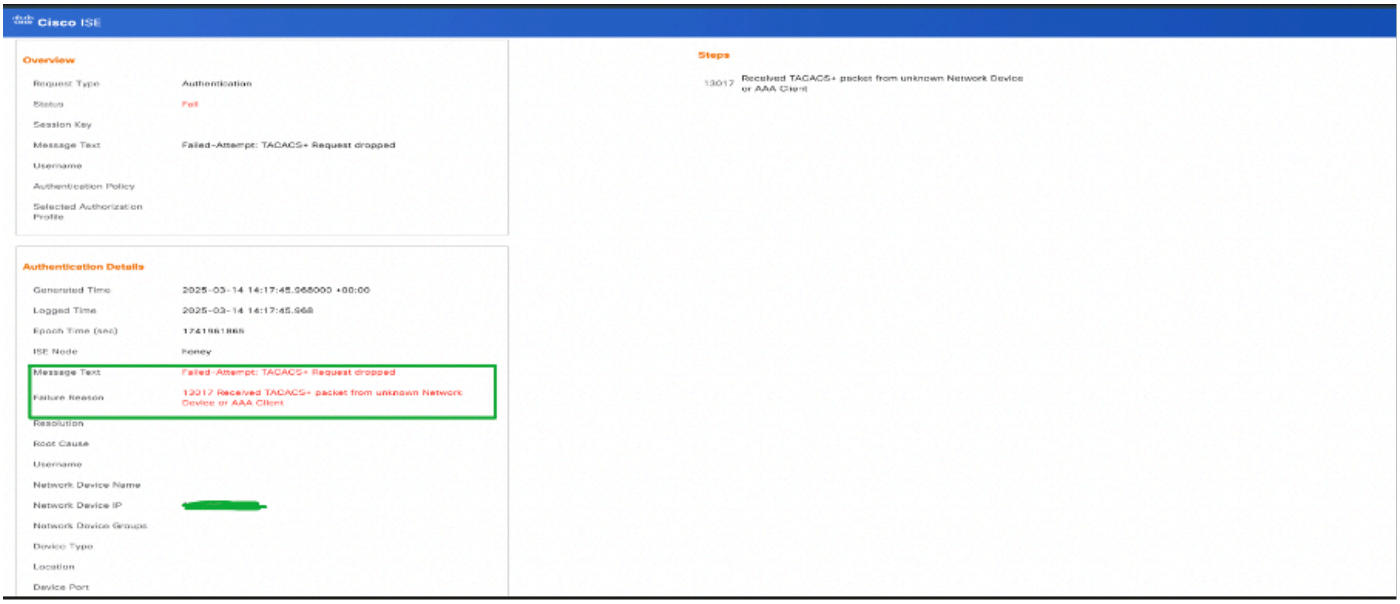
このシナリオは、ネットワークデバイスがISEのネットワークリソースとして追加されていない場合に発生します。このスクリーンショットに示すように、スイッチはISEのネットワークリソ

ースに追加されません。



トラブルシューティングシナリオ：ネットワークデバイスがISEに追加されない。

ここで、スイッチ/ネットワークデバイスから認証をテストすると、パケットは期待どおりにISEに到達します。ただし、次のスクリーンショットに示すように、認証がエラー「Error : 13017 Received TACACS+ packet from unknown Network Device or AAA Client」で失敗します。



TACACSライブログ：ネットワークデバイスがISEに追加されない場合の障害。

ネットワークデバイス（スイッチ）からの検証

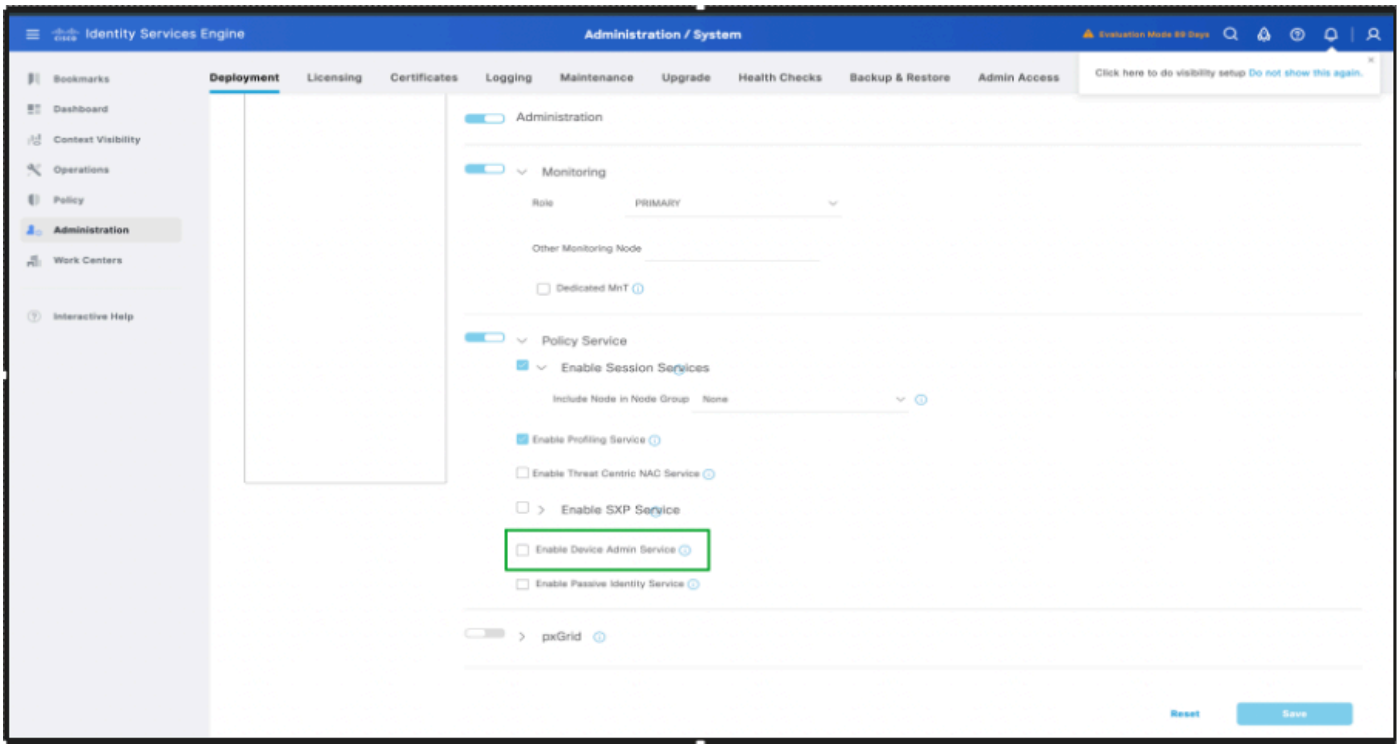
Switch#test aaa group isegroup switch XXXXXX new
ユーザーが拒否されました

解決策：スイッチ/ルータ/ネットワークデバイスがISEのネットワークデバイスとして追加されているかどうかを確認します。デバイスが追加されていない場合は、ISEのネットワークデバイスリストにネットワークデバイスを追加します。

シナリオ2:ISEは情報なしでTACACS+パケットをサイレントにドロップします。

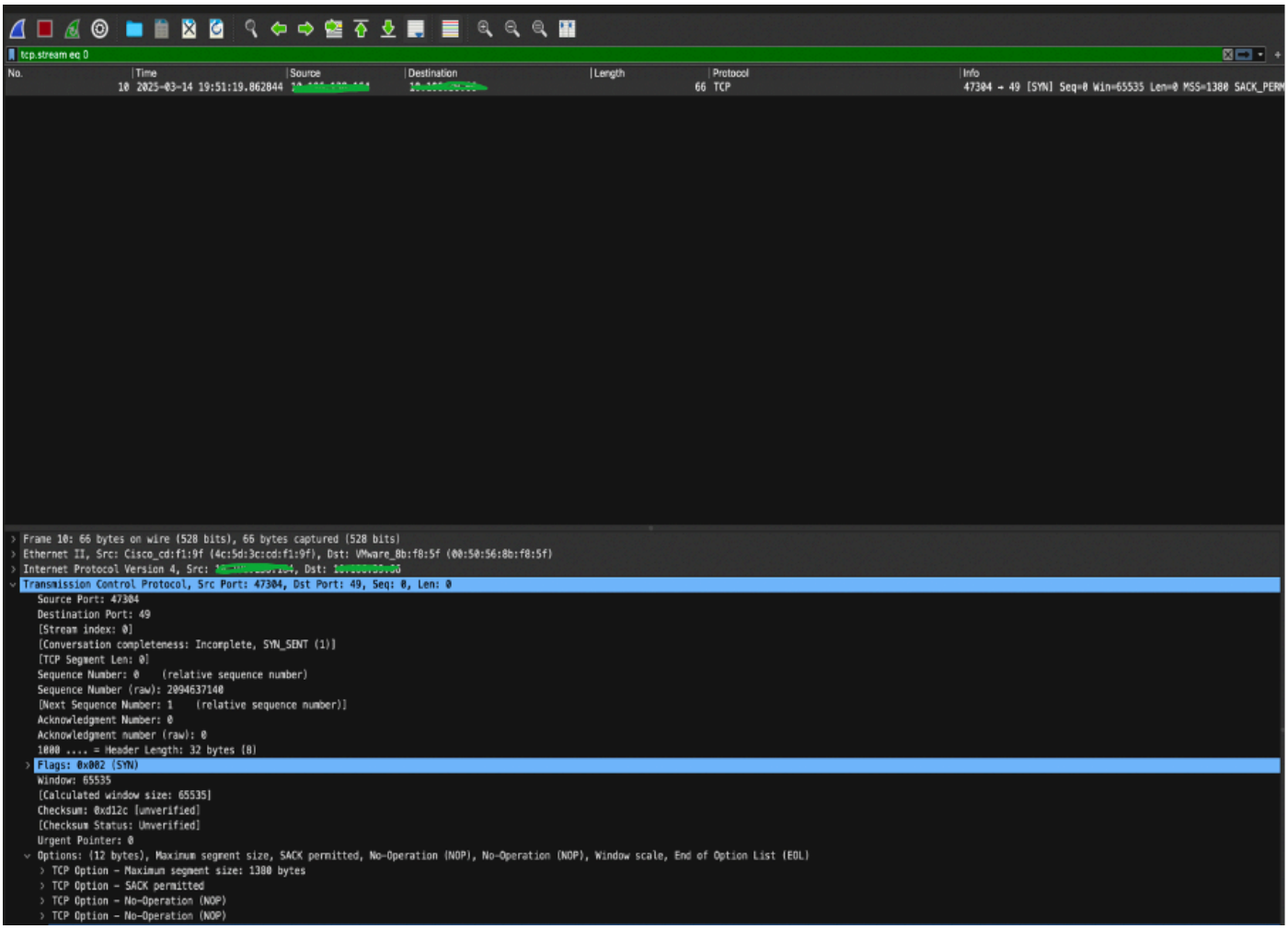
このシナリオは、ISEでDevice Administration Serviceが無効になっている場合に発生します。このシナリオでは、ISEがパケットをドロップし、ISEのネットワークリソースに追加されたネットワークデバイスから認証が開始されている場合でもライブログが表示されません。

このスクリーンショットに示すように、ISEではデバイス管理が無効になっています。



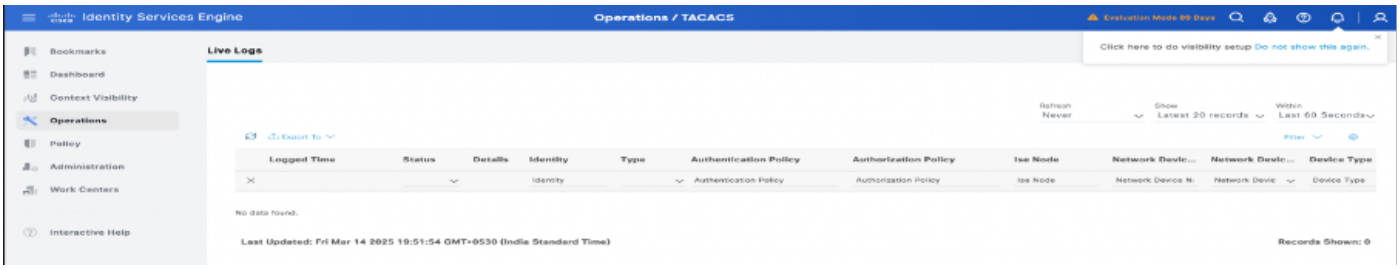
シナリオでは、デバイス管理はISEで有効になっていません。

ユーザがネットワークデバイスから認証を開始すると、ISEはライブログに情報を一切含めずにパケットを通知なしにドロップし、ISEはネットワークデバイスから送信されるSYNパケットに応答してTACACS認証プロセスを完了しません。次のスクリーンショットを参照してください。



TACACSの実行中にISEがパケットをサイレントドロップする

認証中、ISEはライブログを表示しません。



TACACSライブログなし：ISEからの確認

ネットワークデバイス (スイッチ) からの検証

Switch#
Switch#test aaa group isegroup switch XXXX new
ユーザーが拒否されました
Switch#
*Mar 14 13:54:28.144: T+：バージョン192 (0xC0)、タイプ1、シーケンス1、暗号化1、SC 0
*Mar 14 13:54:28.144: T+: session_id 10158877 (0x9B031D)、dlen 14 (0xE)
*Mar 14 13:54:28.144: T+: type:AUTHEN/START, priv_lvl:15 action:LOGIN ascii
*Mar 14 13:54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0
*3月14日13:54:28.144: T+:user: switch
*Mar 14 13:54:28.144: T+：ポート：
*Mar 14 13:54:28.144: T+: rem_addr:
*3月14日13:54:28.144: T+：データ：
*Mar 14 13:54:28.144: T+:End Packet

解決策：ISEでデバイス管理を有効にします。

参考

- TACACS 認証の問題のトラブルシューティング
- Cisco Identity Services Engine 管理者ガイド リリース 3.3
- TACACSサーバのVRF

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。