ISEを使用したNexusデバイスでのTACACS+ over TLS 1.3の設定

内容

- はじめに
  - 概要
  - このガイドの使用方法
- 前提条件
  - 要件
  - 使用するコンポーネント
  - ライセンス
- Device Admin用のISEの設定
  - TACACS+サーバ認証用の証明書署名要求の生成
  - TACACS+サーバ認証用のルートCA証明書のアップロード
  - 署名付き証明書署名要求(CSR)のISEへのバインド
  - TLS 1.3を有効にする
  - ISEでのデバイス管理の有効化
  - TLS経由のTACACSの有効化
  - ネットワークデバイスとネットワークデバイスグループ
  - アイデンティティストアの設定
  - TACACS+シェルプロファイルの設定
  - NX-OS管理
  - NX-OSヘルプデスク
  - デバイス管理ポリシーセットの設定
- TACACS+ over TLS用のCisco NX-OSの設定
  - TACACS+サーバの設定
  - トラストポイントの設定
  - TACACS+ TLSの設定
  - AAA 設定
- NX-OSのユーザアクセスのテストとトラブルシューティング
  - 検証
  - 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、サーバとしてCisco Identity Services Engine(ISE)、クライアントとしてCisco NX-OSデバイスを使用したTACACS+ over TLSの例について説明します。

概要

Terminal Access Controller Access-Control System Plus(TACACS+)プロトコル[RFC8907]を使用すると、1台以上のTACACS+サーバを介して、ルータ、ネットワークアクセスサーバ、およびその他のネットワークデバイスを一元的に管理できます。認証、許可、アカウンティング(AAA)サービスを提供し、デバイス管理のユースケースに合わせて特別に調整されています。

TACACS+ over TLS 1.3 [RFC8446]は、安全性の高いトランスポート層を導入して機密性の高いデータを保護することで、プロトコルを強化します。この統合により、TACACS+クライアントとサーバ間の接続およびネットワークトラフィックの機密性、整合性、および認証が確保されます。

このガイドの使用方法

このガイドでは、アクティビティを2つの部分に分けて、ISEでCisco NX-OSベースのネットワークデバイスの管理アクセスを管理できるようにします。
- パート1:Device Admin用のISEの設定
- パート2:TACACS+ over TLS用のCisco NX-OSの設定

前提条件

要件

TACACS+ over TLSを設定するための前提条件：

- ISEおよびネットワークデバイスの証明書に署名するためにTACACS+ over TLSで使用される証明書に署名するための認証局(CA)。
- 認証局(CA)からのルート証明書。

- ネットワークデバイスとISEにはDNS到達可能性があり、ホスト名を解決できます。

使用するコンポーネント

この文書の情報は、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。

- ISE VMware仮想アプライアンス、リリース3.4パッチ2
- Nexus 9000スイッチモデルC9364D-GX2A、Cisco NX-OS version 10.5(3t)

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。

ライセンス

デバイス管理ライセンスを使用すると、ポリシーサービスノードでTACACS+サービスを使用できます。ハイアベイラビリティ(HA)スタンドアロン導入では、デバイス管理ライセンスにより、HAペアの単一のポリシーサービスノードでTACACS+サービスを使用できます。

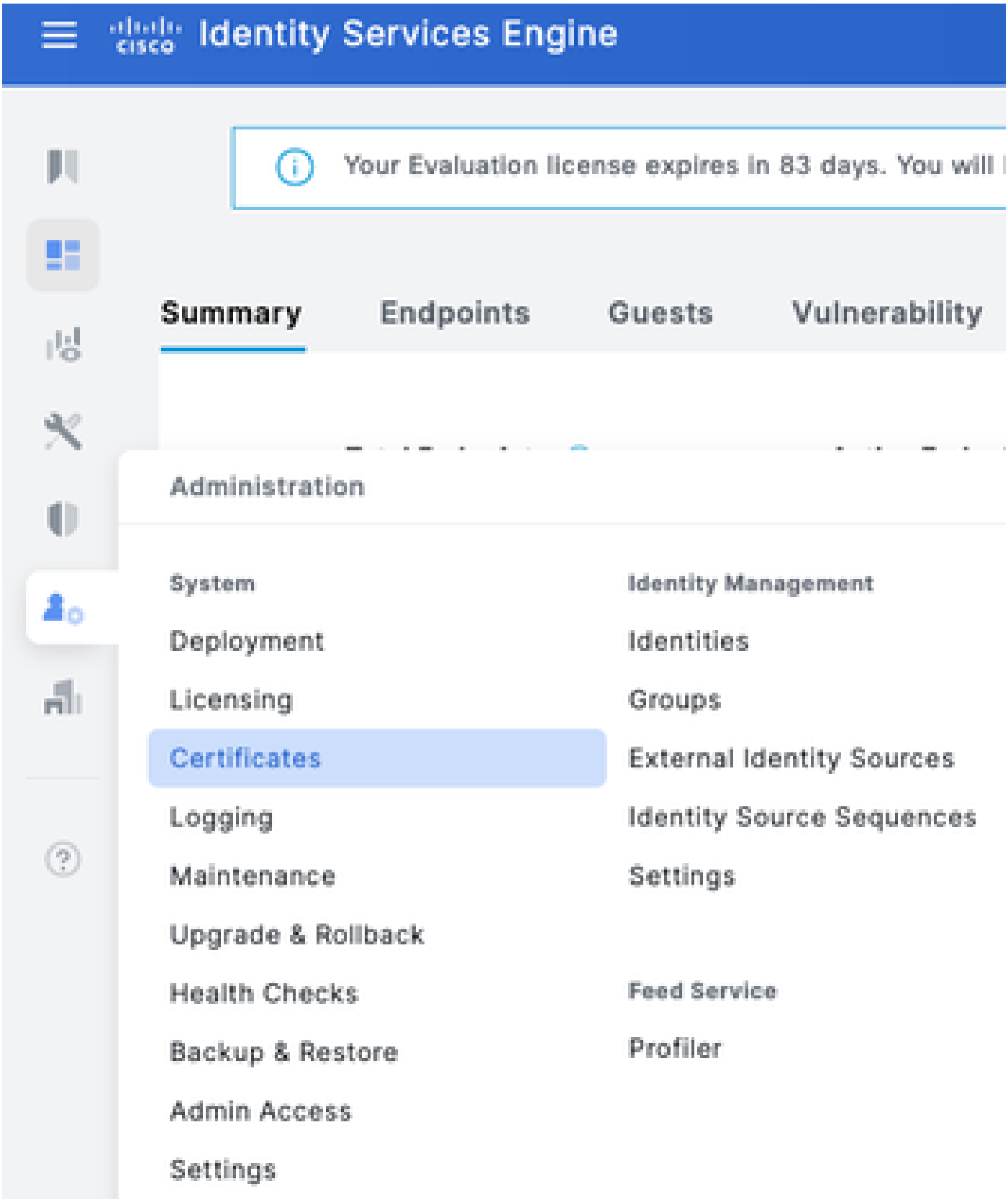
Device Admin用のISEの設定

TACACS+サーバ認証用の証明書署名要求の生成

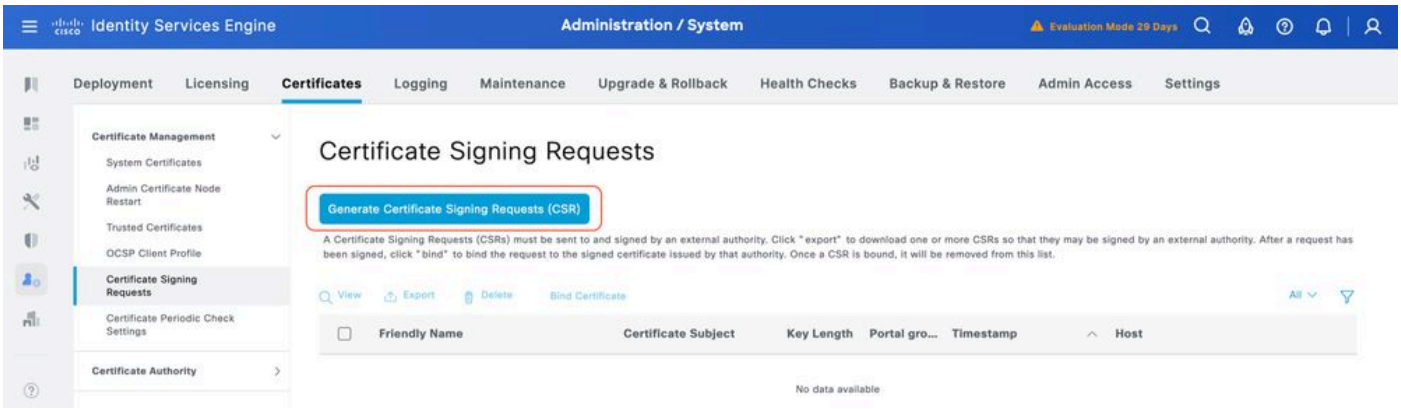
ステップ 1：サポートされているいずれかのブラウザを使用して、ISE管理Webポータルにログインします。

デフォルトでは、ISEはすべてのサービスに自己署名証明書を使用します。最初の手順では、証明書署名要求(CSR)を生成して、認証局(CA)によって署名されるようにします。

ステップ 2：Administration > System > Certificatesの順に選択します。

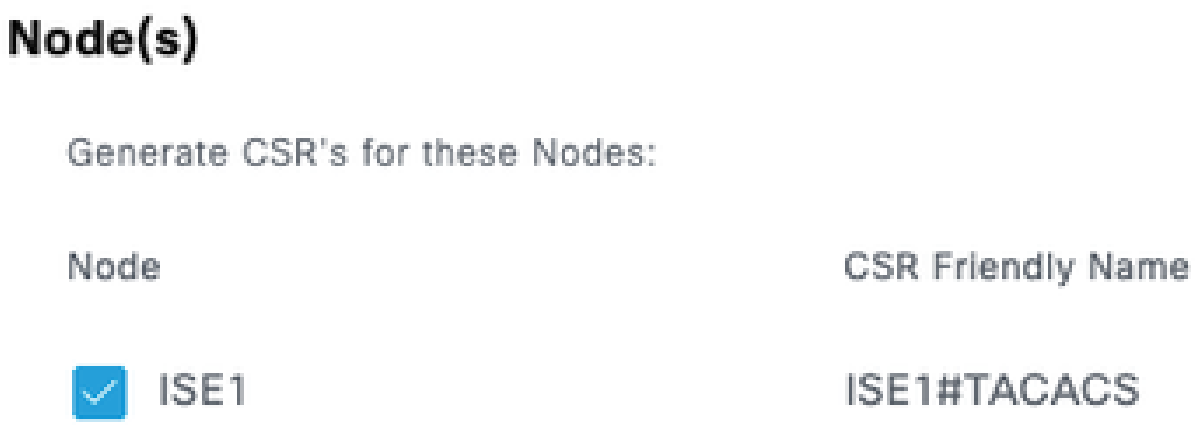


ステップ3:Certificate Signing Requestsで、Generate Certificate Signing Requestをクリックします。

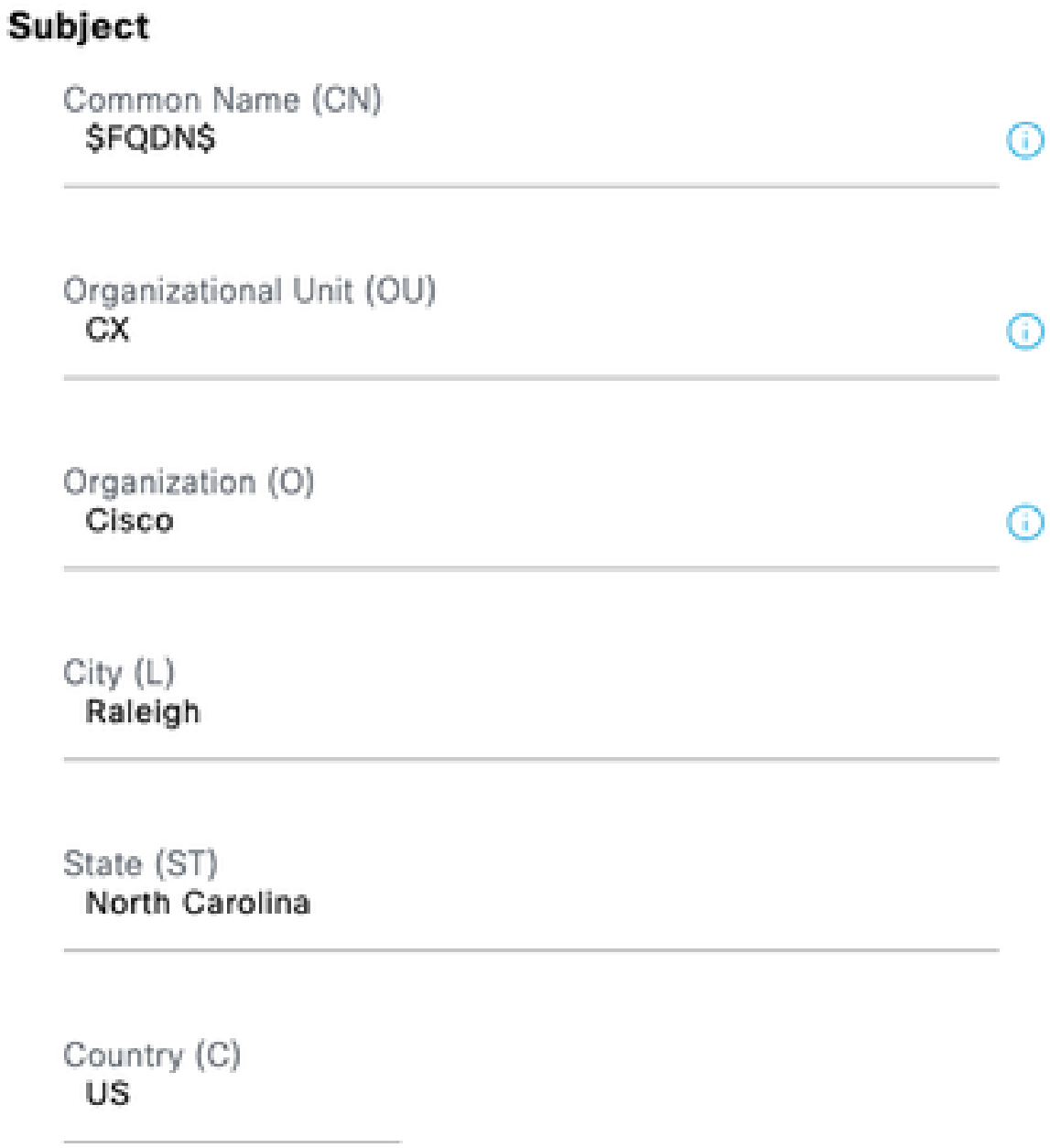


ステップ 4：TACACSをUsageで選択します。

ステップ 5：TACACS+が有効になっているPSNを選択します。



手順 6： Subjectフィールドに、適切な情報を入力します。



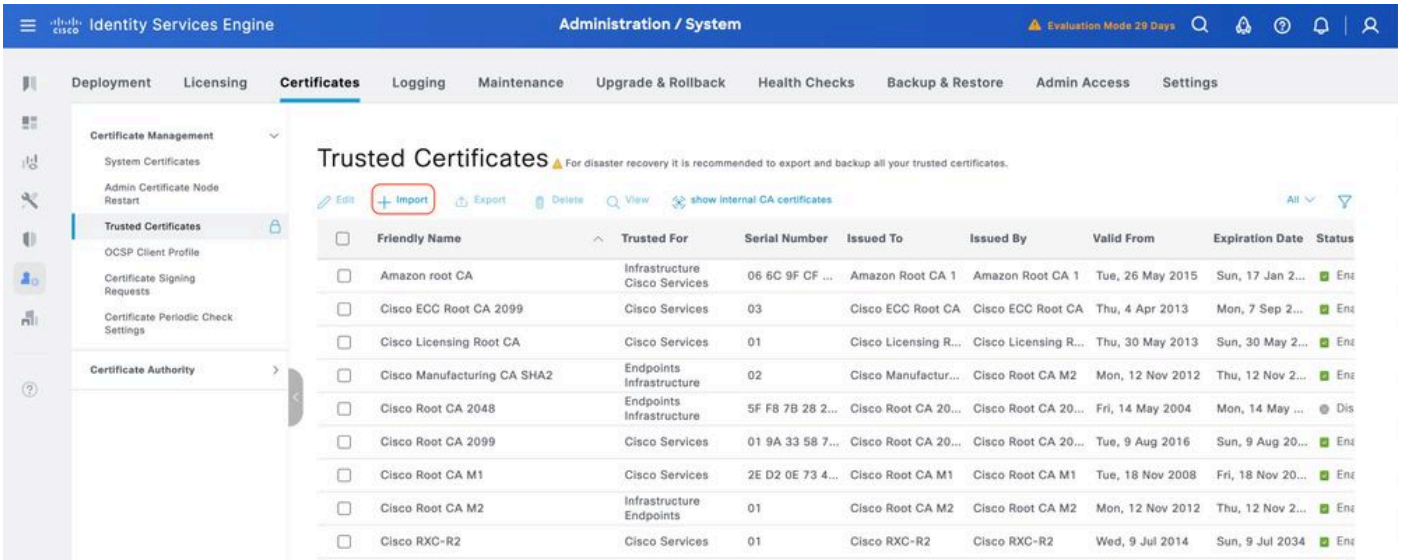
手順 7：Subject Alternative Name (SAN)の下にDNS NameとIP Addressを追加します。

ステップ 8：Generateをクリックしてから、Exportをクリックします。

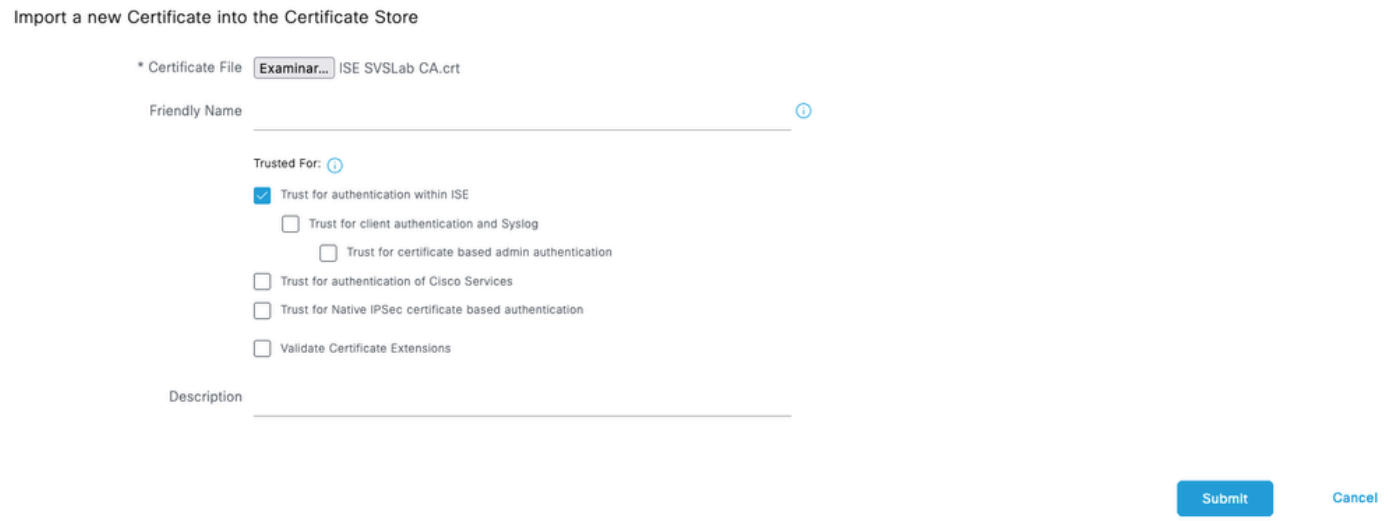
これで、認証局(CA)によって署名された証明書(CRT)を取得できます。

TACACS+サーバ認証用のルートCA証明書のアップロード

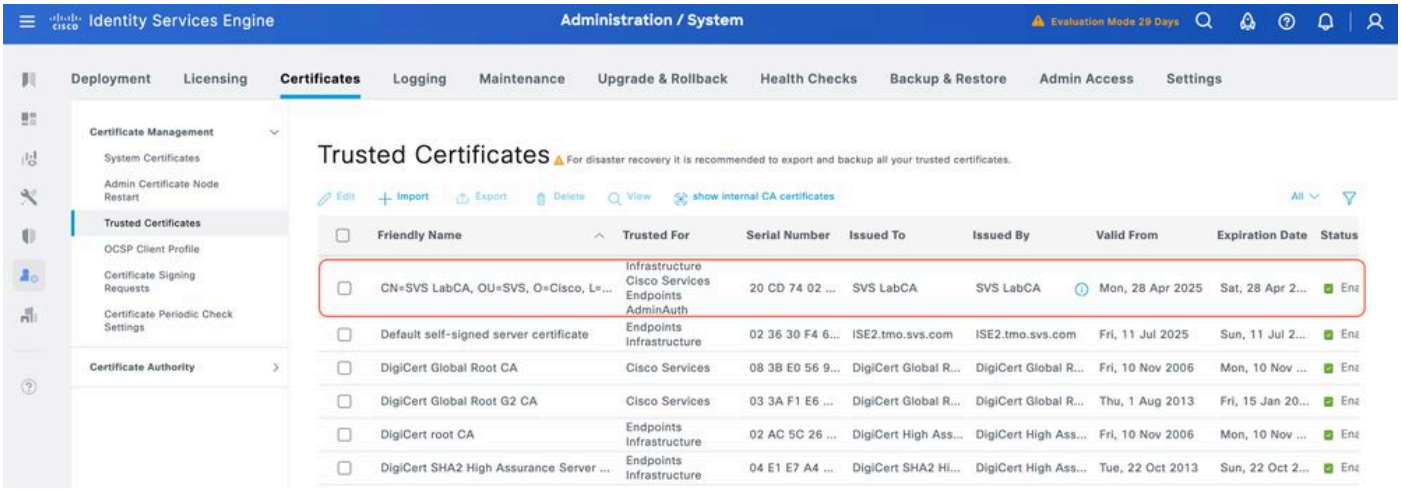
ステップ 1：Administration > System > Certificatesの順に選択します。Trusted Certificatesで、Importをクリックします。



ステップ 2：TACACS証明書署名要求(CSR)に署名した認証局(CA)によって発行された証明書を選択します。 Trust for authentication within ISEオプションが有効になっていることを確認します。



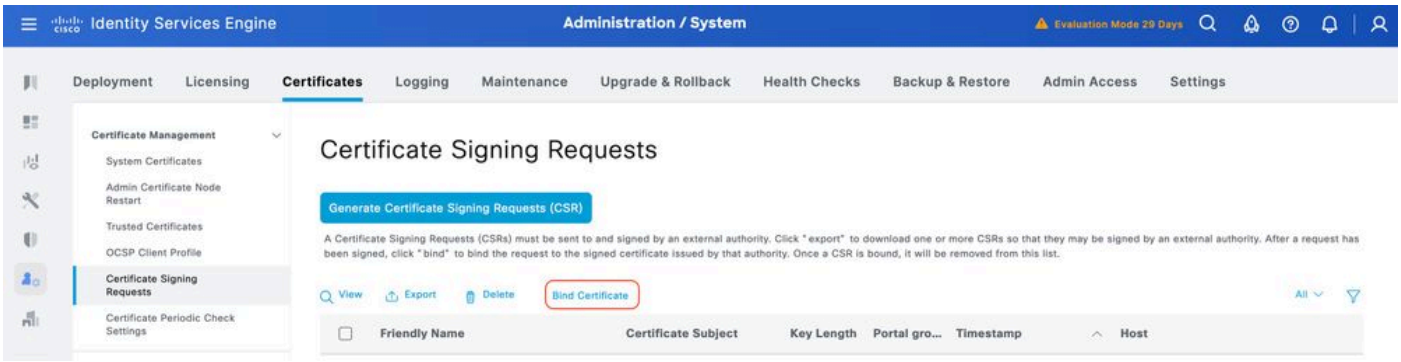
[Submit] をクリックします。 証明書がTrusted Certificatesの下に表示されている必要があります。



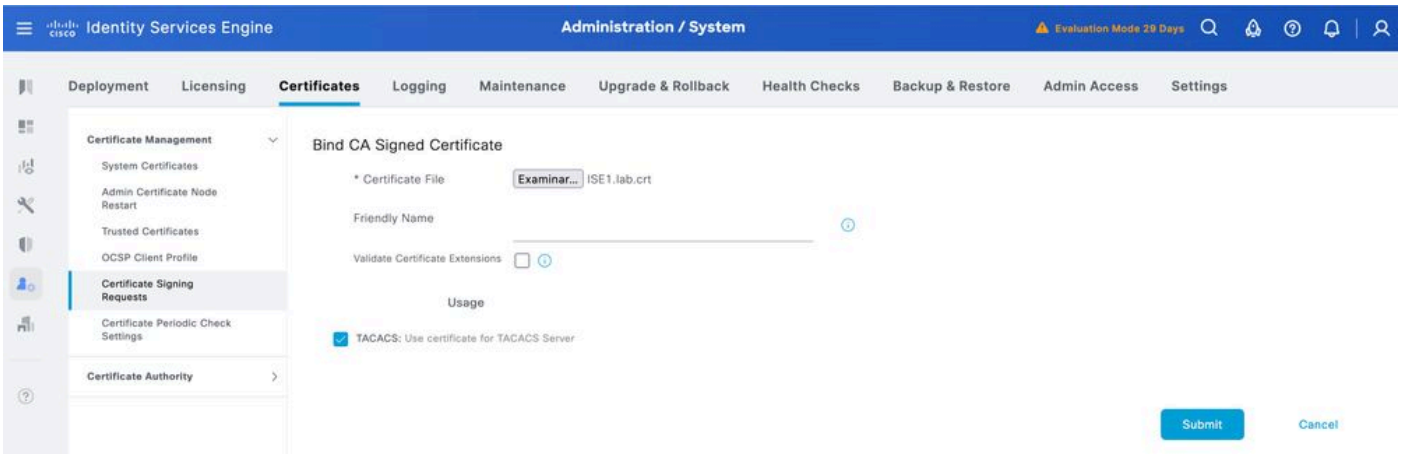
署名付き証明書署名要求(CSR)のISEへのバインド

証明書署名要求(CSR)が署名されたら、署名付き証明書をISEにインストールできます。

ステップ 1：Administration > System > Certificatesの順に選択します。Certificate Signing Requestsの下で、前のステップで生成したTACACS CSRを選択し、Bind Certificateをクリックします。

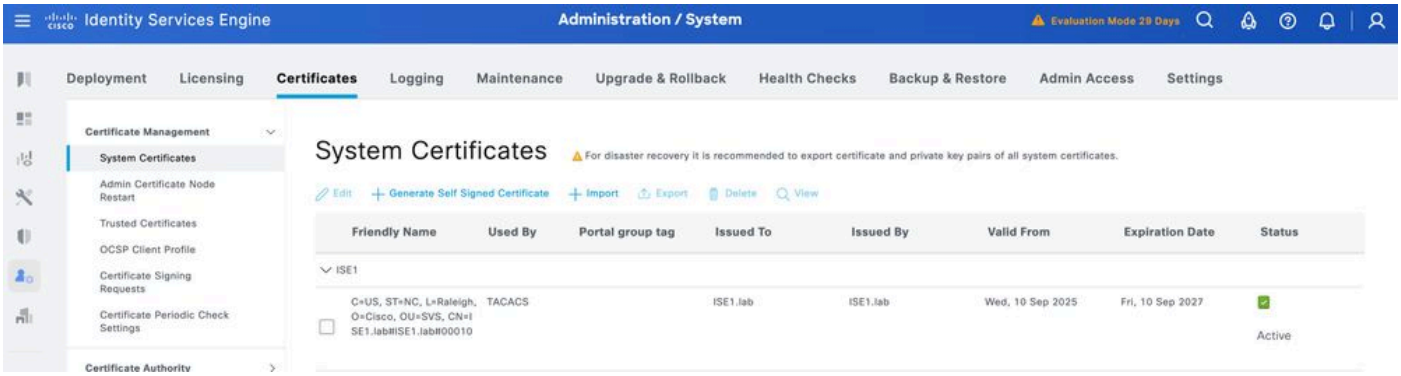


ステップ 2：署名付き証明書を選択し、Usageの下のTACACSチェックボックスが選択されたままになっていることを確認します。



ステップ 3：[Submit] をクリックします。既存の証明書の置き換えに関する警告が表示されたら、Yesをクリックして続行します。

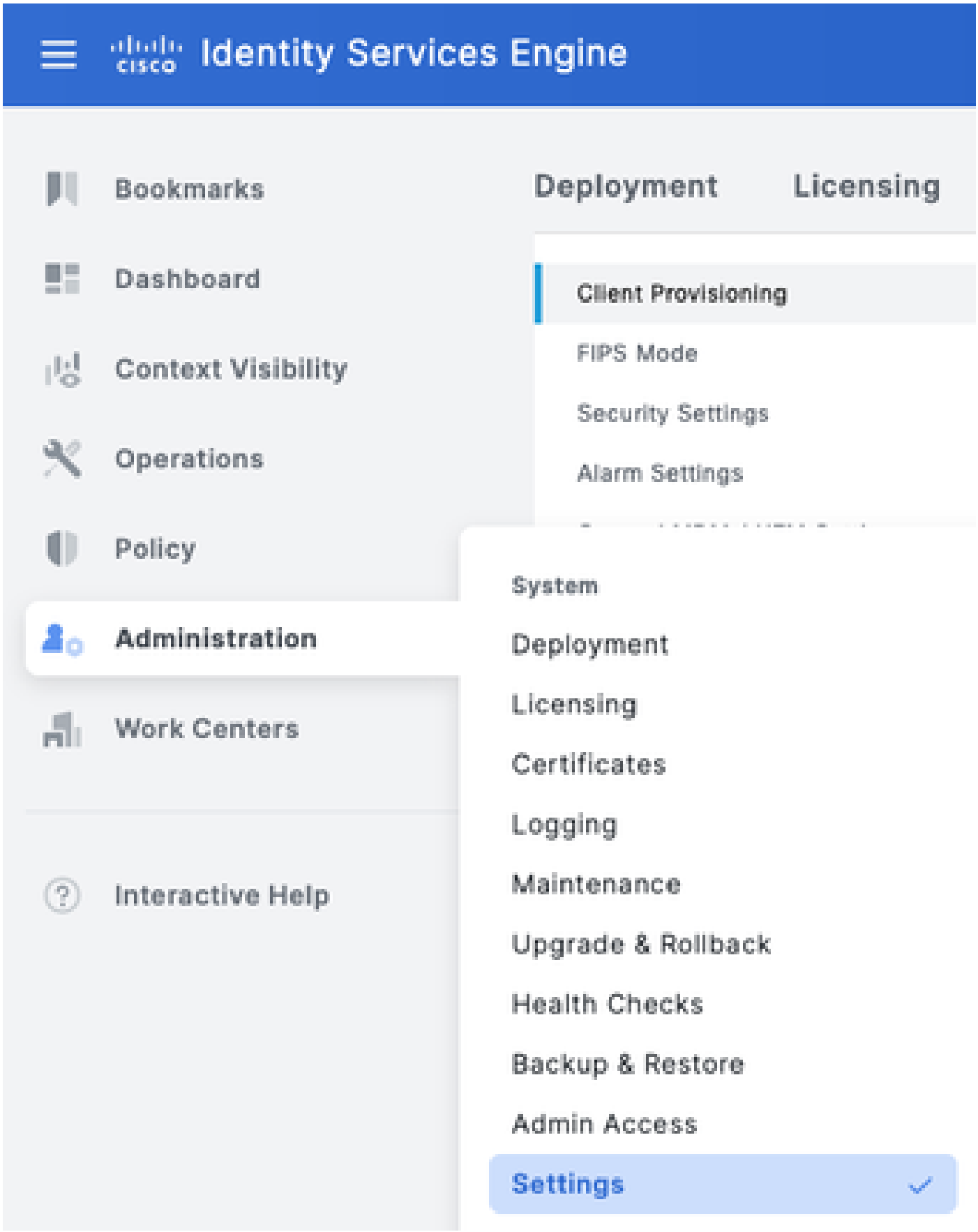
これで、証明書が正しくインストールされました。これは、「システム証明書」で確認できます。



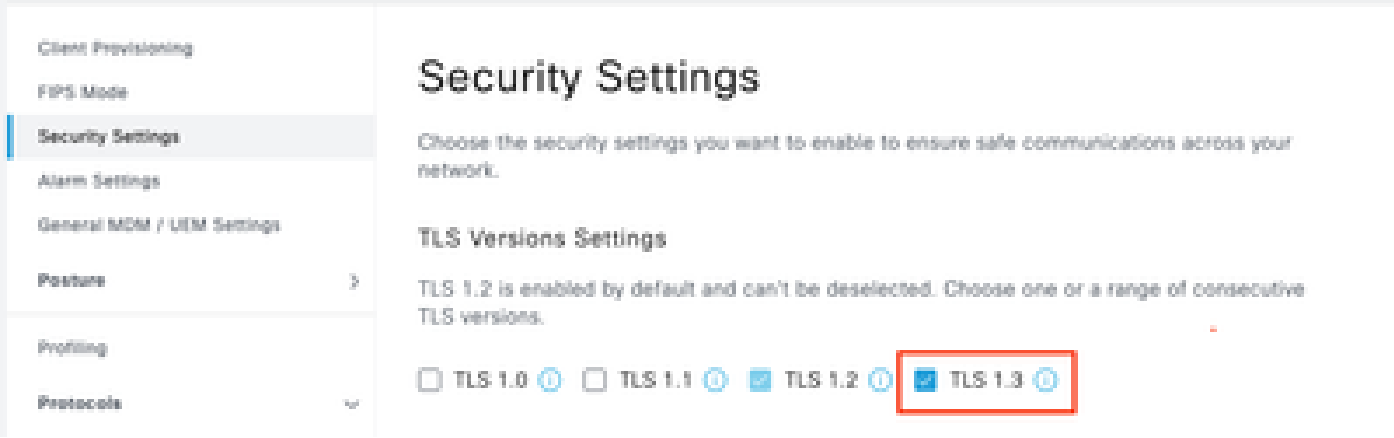
TLS 1.3を有効にする

TLS 1.3は、ISE 3.4.xではデフォルトで有効になっていません。手動で有効にする必要があります。

ステップ 1：[Administration] > [System] > [Settings] に移動します。



ステップ 2：Security Settingsをクリックし、TLS Version Settingsの下でTLS1.3の横にあるチェックボックスをオンにしてから、Saveをクリックします。

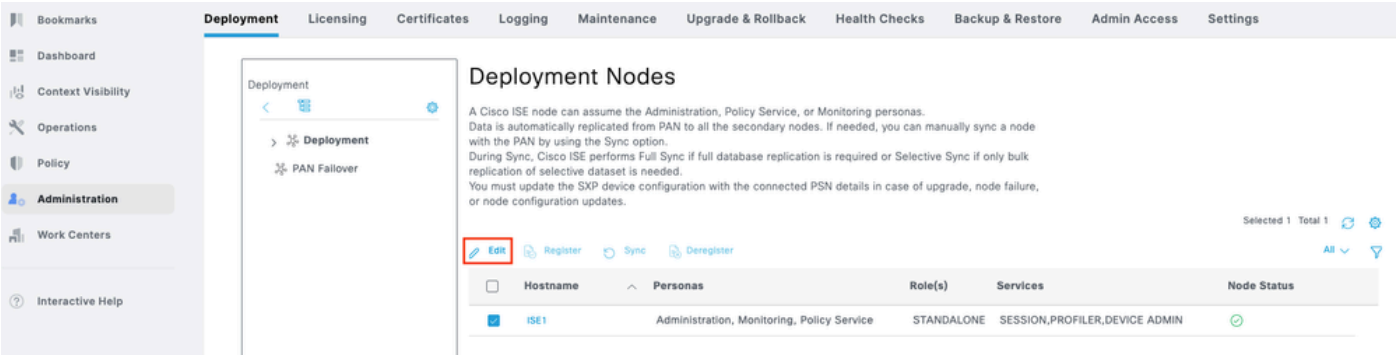


警告:TLSバージョンを変更すると、Cisco ISEアプリケーションサーバがすべてのCisco ISE導入マシンで再起動します。

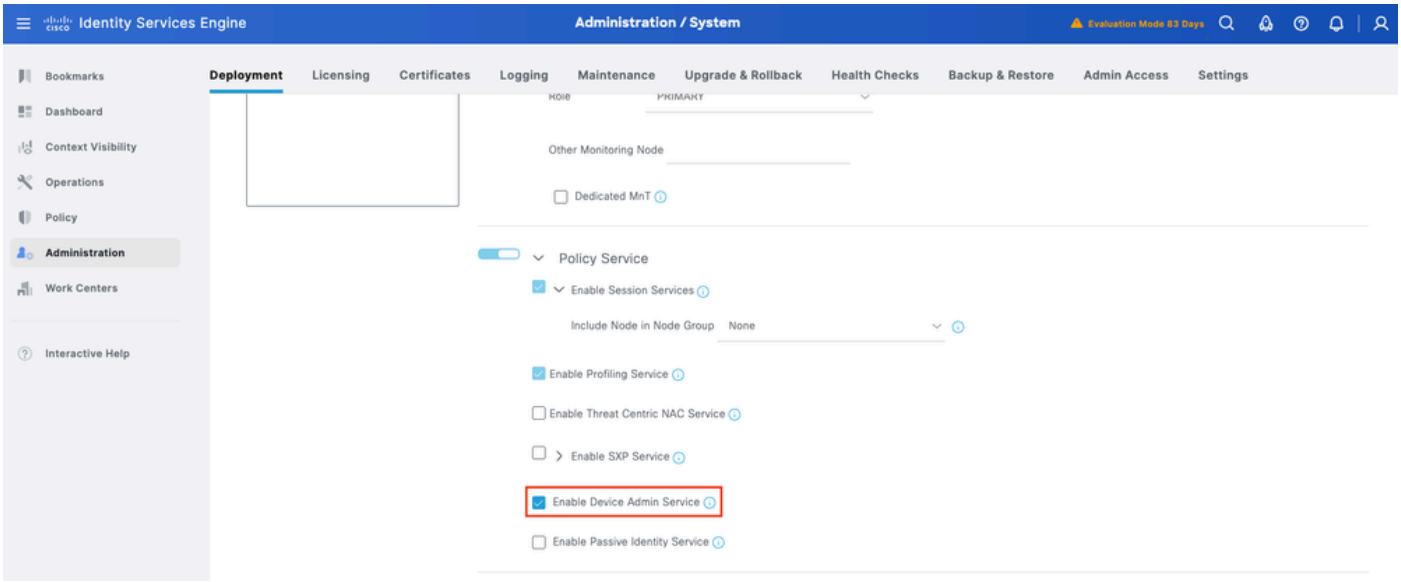
ISEでのデバイス管理の有効化

ISEノードでは、デバイス管理サービス(TACACS+)はデフォルトで有効になっていません。PSNノードでTACACS+を有効にします。

ステップ 1：[Administration] > [System] > [Deployment] を選択します。ISEノードの横にあるチェックボックスをオンにし、Editをクリックします。



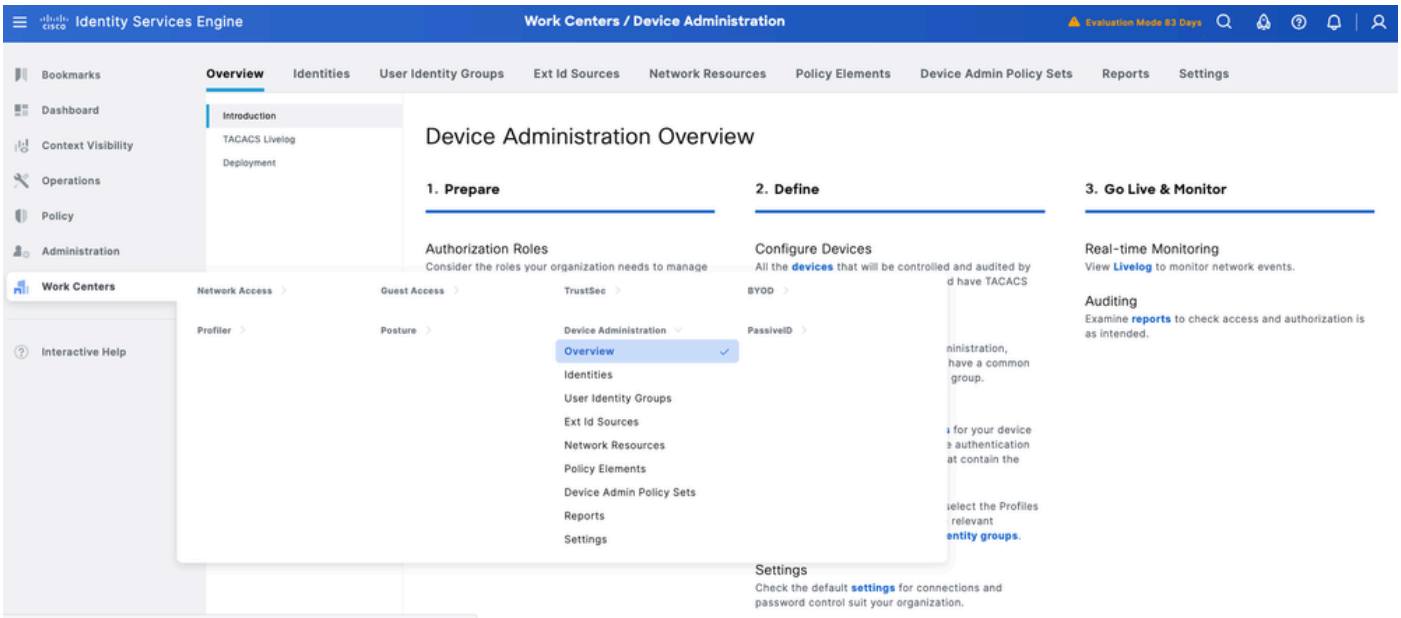
ステップ 2：General Settingsで、下にスクロールしてEnable Device Admin Serviceの横にあるチェックボックスをオンにします。



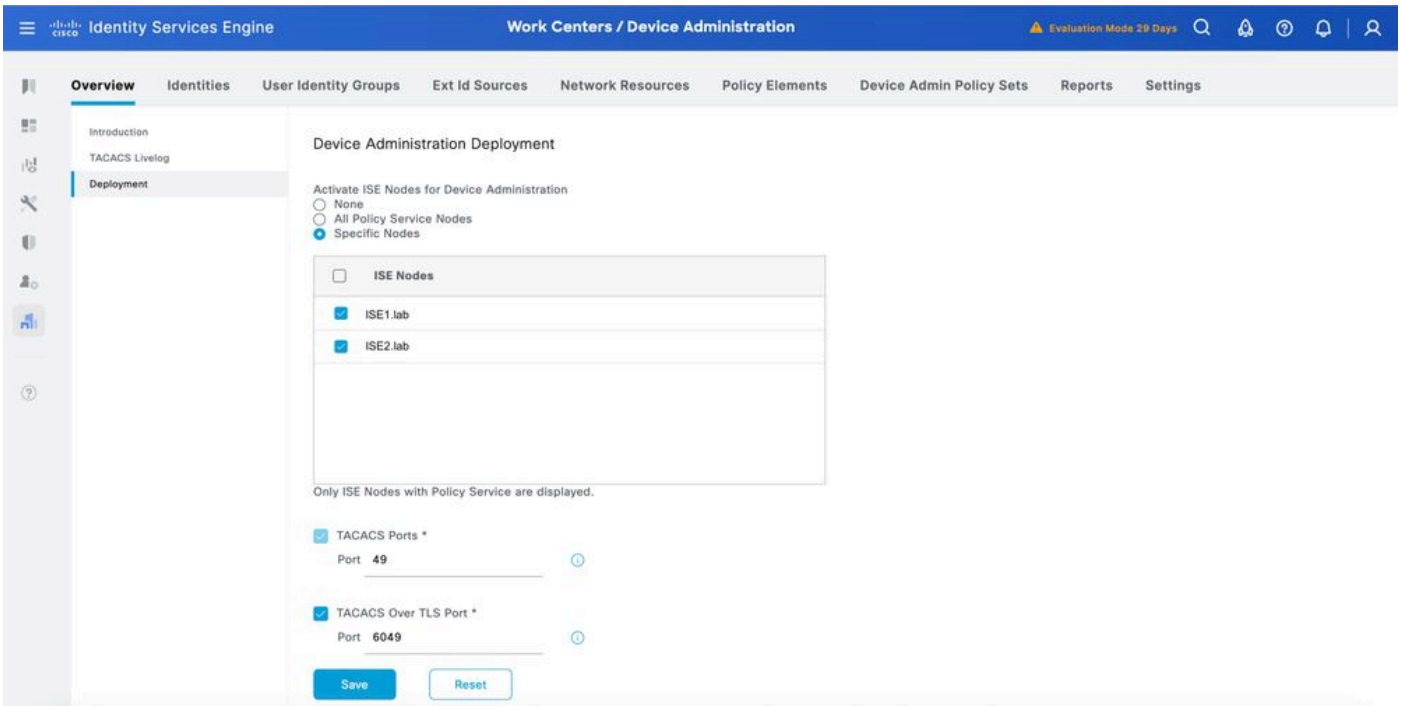
ステップ 3： 設定を保存します。Device Admin ServiceがISEで有効になりました。

TLS経由のTACACSの有効化

ステップ 1：Work Centers > Device Administration > Overviewの順に移動します。



ステップ 2：Deploymentをクリックします。TACACS over TLSを有効にするPSNノードを選択します。

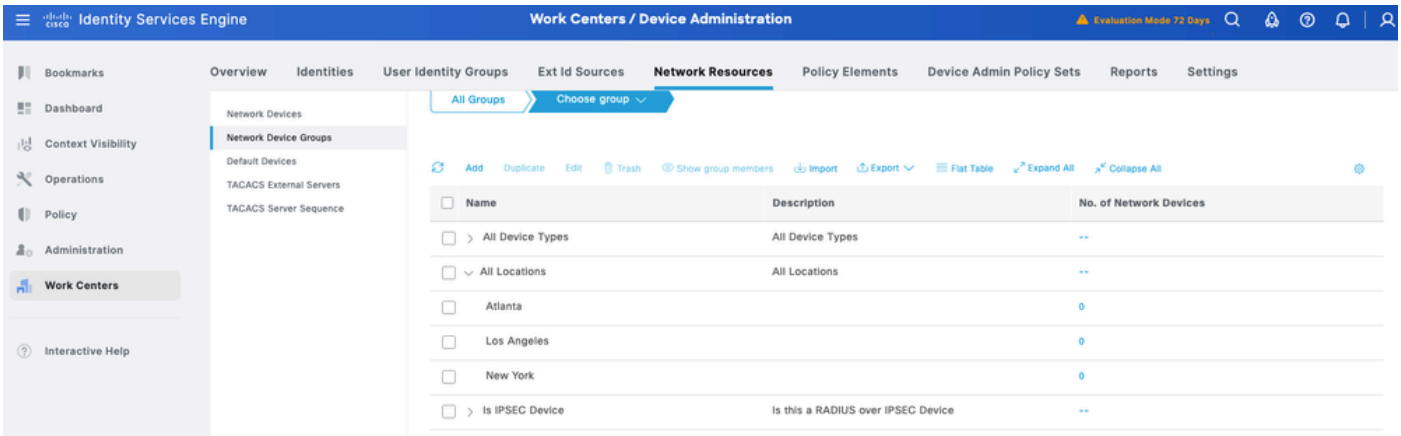


ステップ 3：デフォルトのポート6049をそのまま使用するか、TACACS over TLSに別のTCPポートを指定して、Saveをクリックします。

ネットワークデバイスとネットワークデバイスグループ

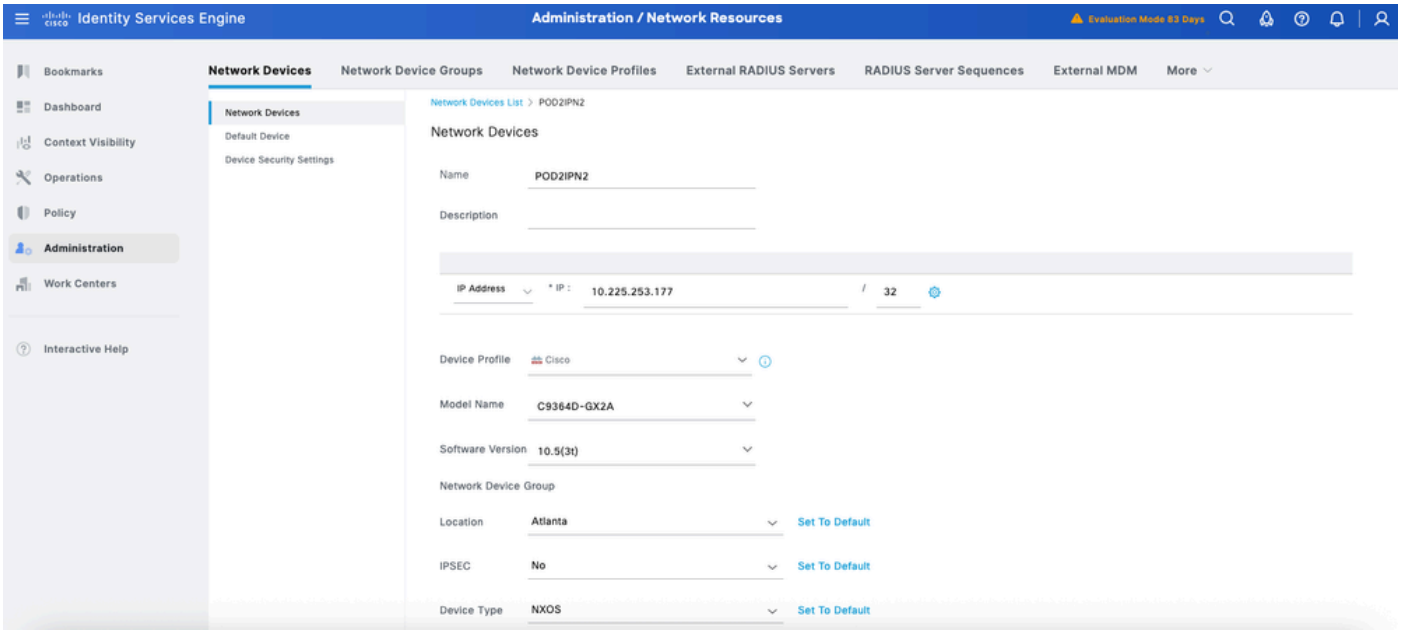
ISEは、複数のデバイスグループ階層を使用した強力なデバイスグループ化を提供します。各階層は、ネットワークデバイスの個別の独立した分類を表します。

ステップ 1：Work Centers > Device Administration > Network Resourceの順に移動します。[Network Device Groups] をクリックします。



すべてのデバイスタイプとすべてのロケーションは、ISEによって提供されるデフォルトの階層です。独自の階層を追加し、ポリシー条件で後から使用できるネットワークデバイスの識別でさまざまなコンポーネントを定義します。

ステップ 2：次に、NS-OXデバイスをネットワークデバイスとして追加します。Work Centers > Device Administration > Network Resourcesの順に移動します。Addをクリックして、新しいネットワークデバイスPOD2IPN2を追加します。



ステップ 3：デバイスのIPアドレスを入力し、デバイスの場所とデバイスタイプがマッピングされていることを確認します。最後に、TACACS+ over TLS認証設定を有効にします。

Identity Services Engine | Administration / Network Resources | Evaluation Mode 83 Days

Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | External MDM | More

Network Devices
Default Device
Device Security Settings

RADIUS Authentication Settings

TACACS Authentication Settings

TACACS over TLS Authentication Settings

This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.

Subject Alternative Name (SAN)*

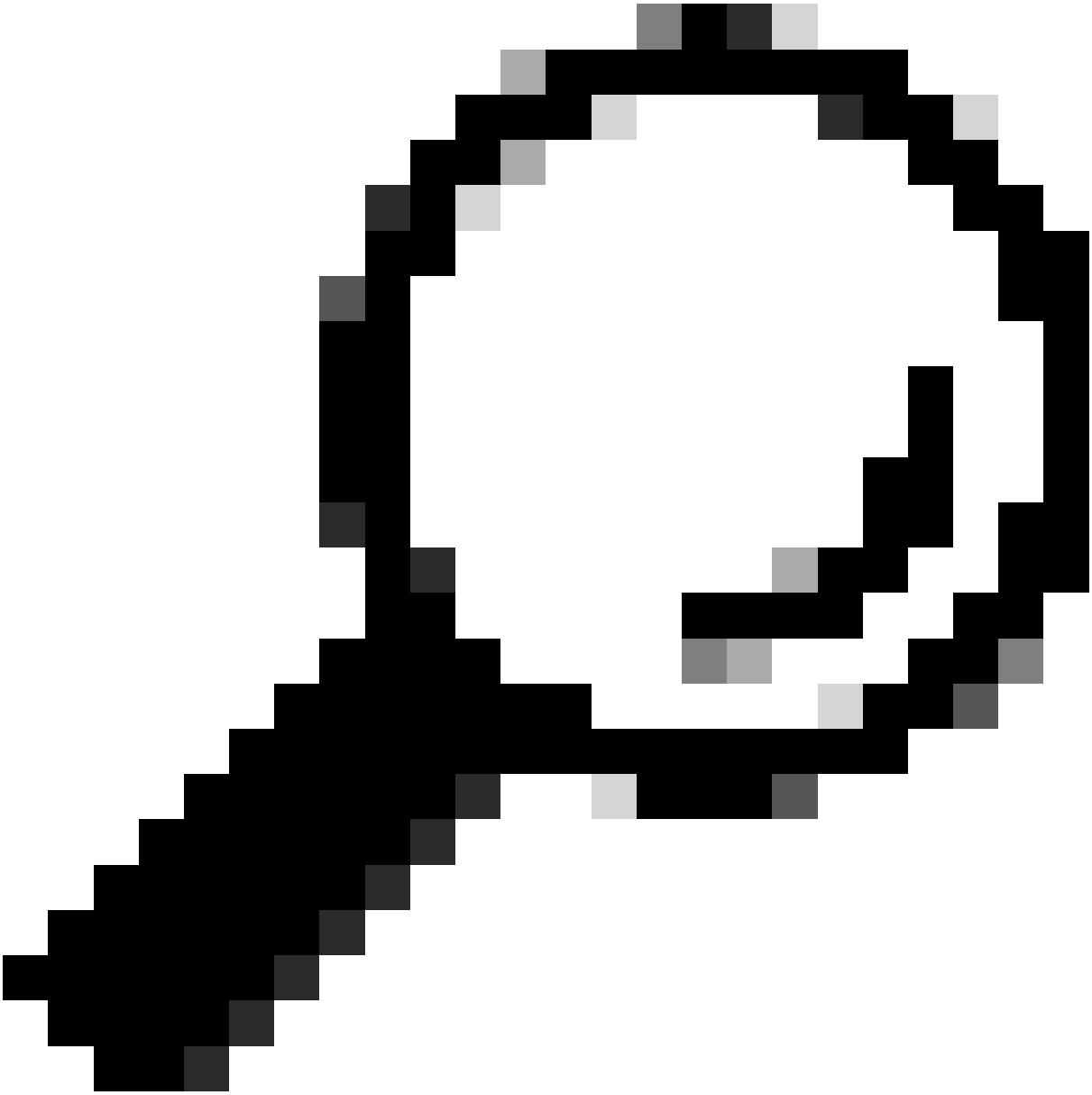
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (iPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.

IP Address
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details Show

Additional SAN Attributes

Enable Single Connect Mode
Allow a network device to use one TCP connection for all TACACS+ requests,reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

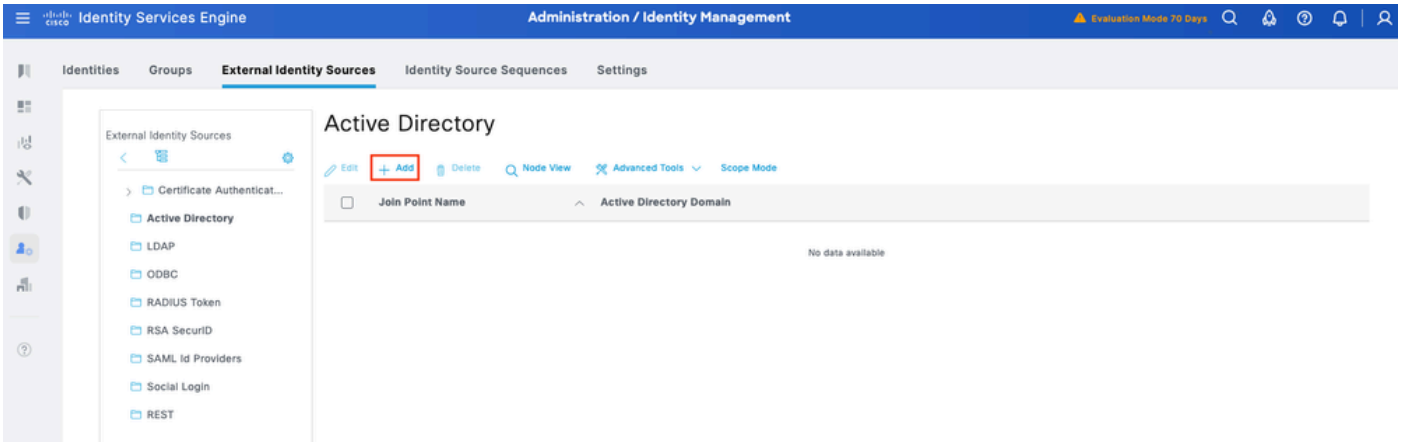


ヒント：デバイスにコマンドが送信されるたびにTCPセッションが再起動しないように、シングル接続モードを有効にすることを推奨します。

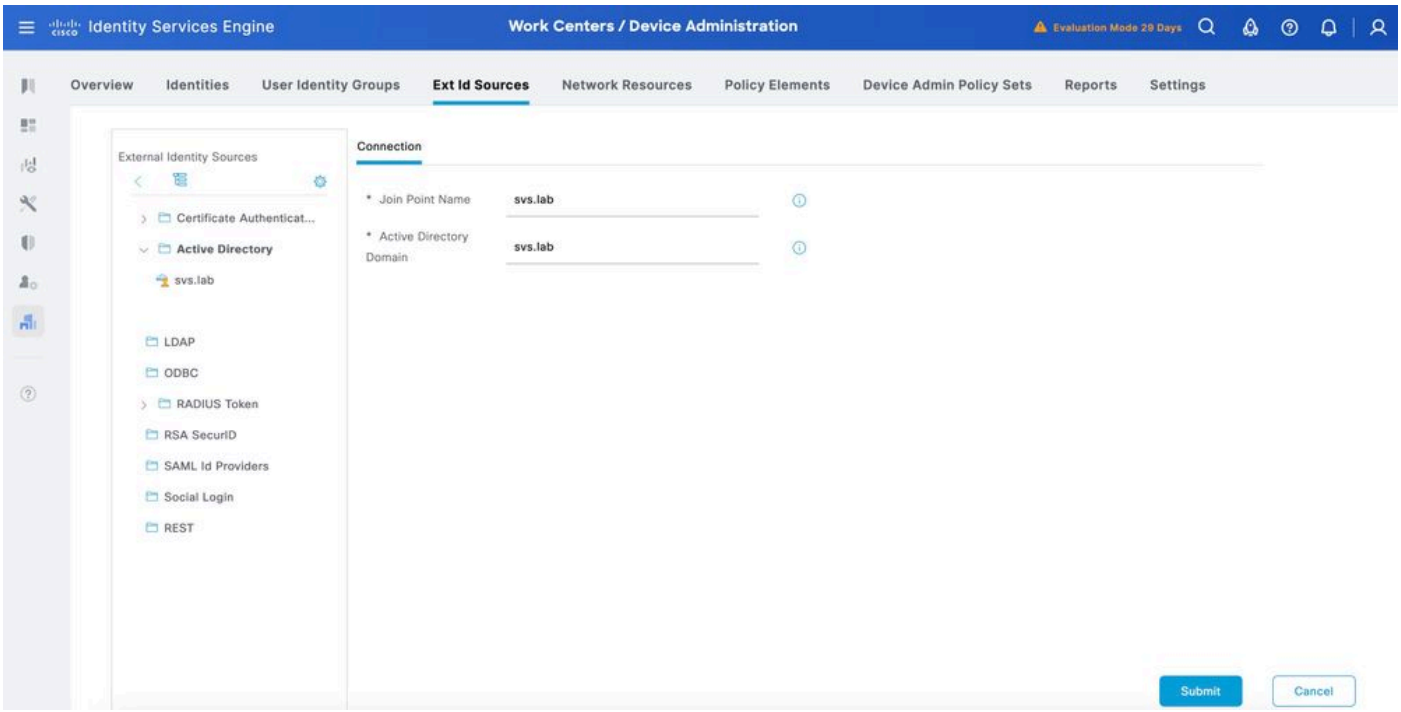
アイデンティティストアの設定

このセクションでは、デバイス管理者用のアイデンティティストアを定義します。これは、ISE内部ユーザおよびサポートされる任意の外部アイデンティティソースにすることができます。ここでは、外部IDソースであるActive Directory(AD)を使用します。

手順 1：Administration > Identity Management > External Identity Stores > Active Directoryの順に移動します。Addをクリックして、新しいADジョイントポイントを定義します。

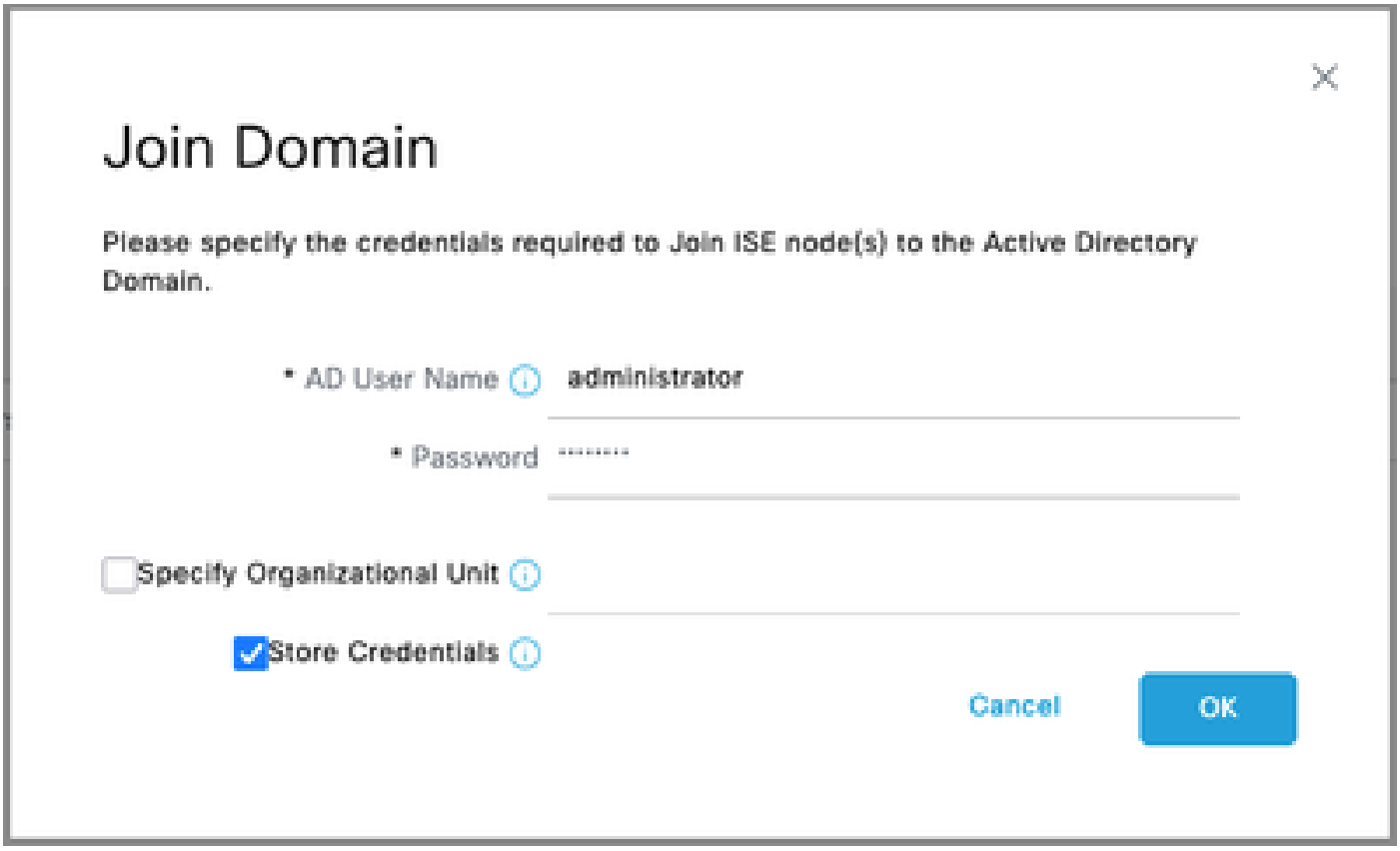


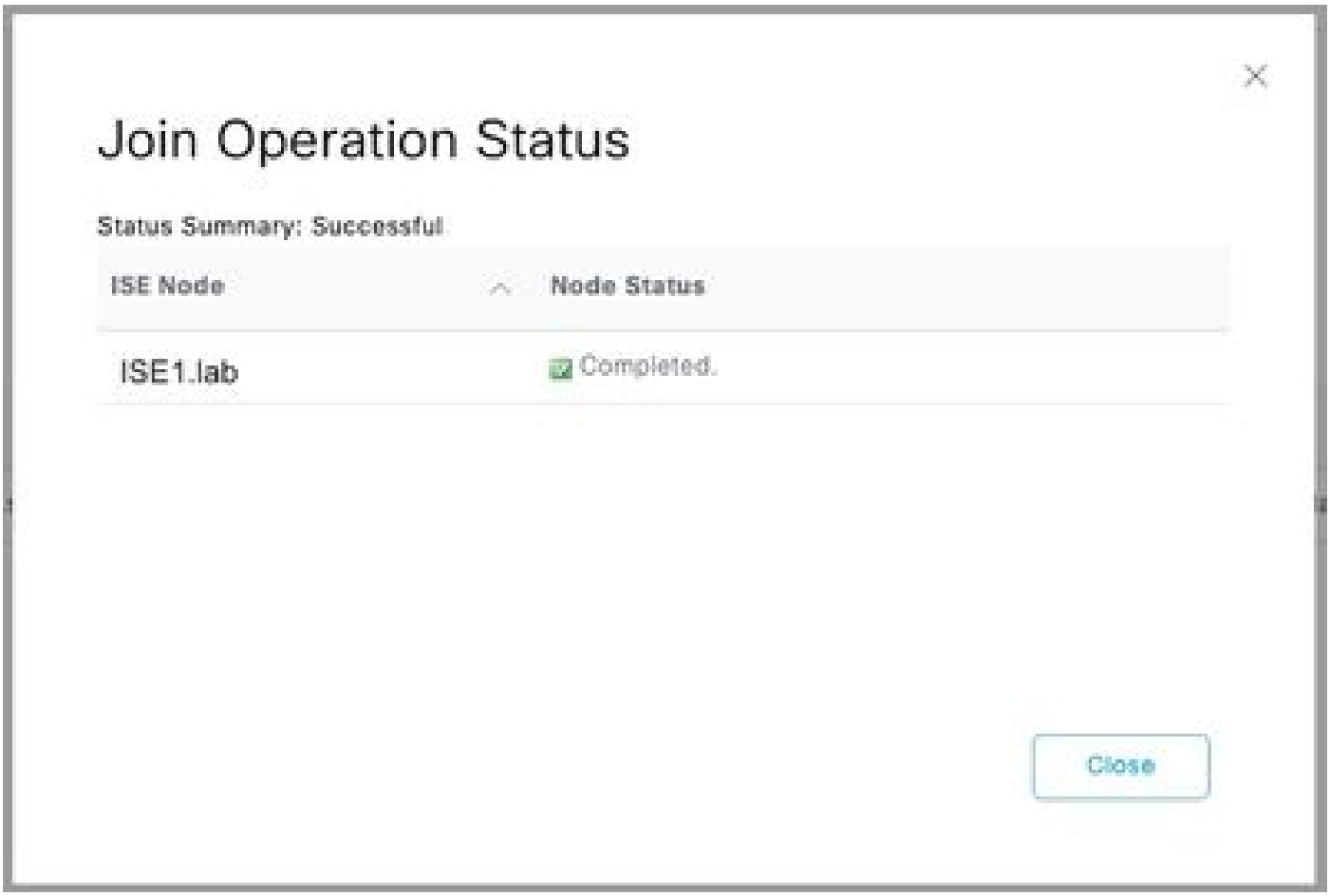
ステップ 2：参加ポイント名とADドメイン名を指定し、Submitをクリックします。



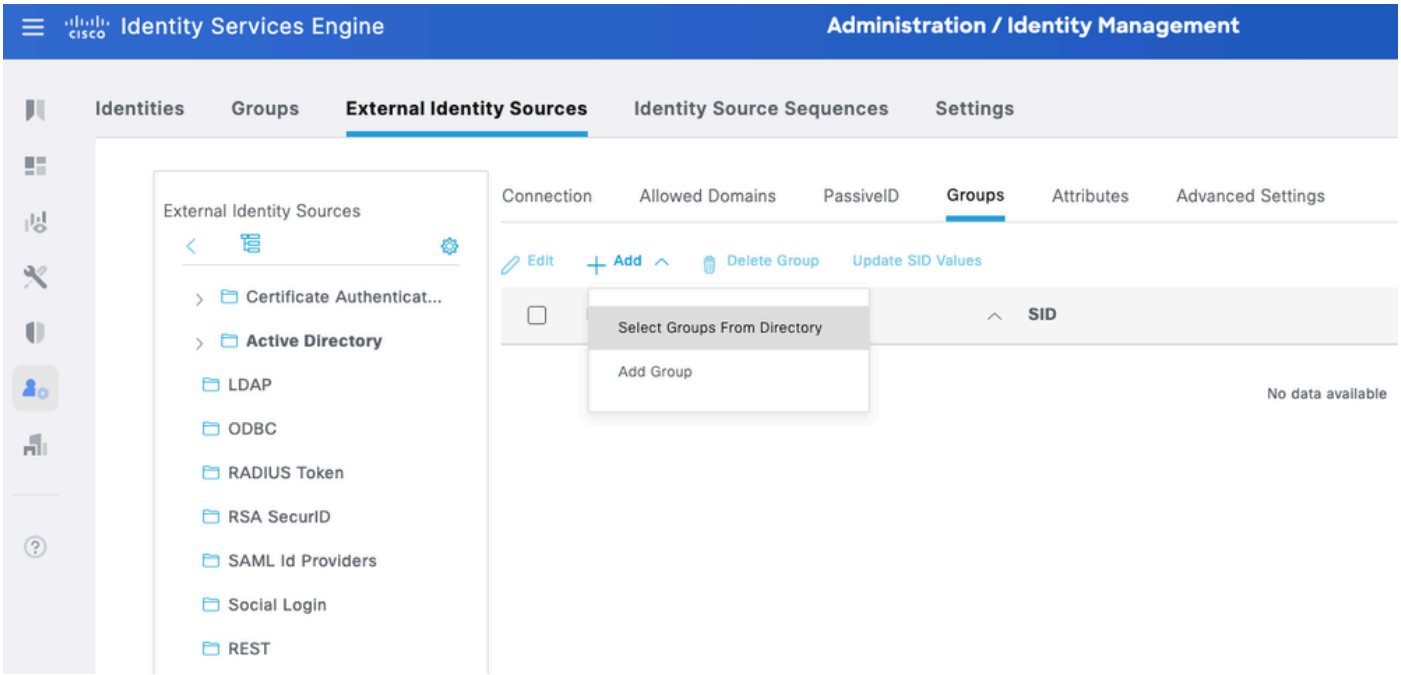
ステップ 3：「Would you like to Join all ISE Nodes to this Active Directory Domain?」というプロンプトが表示されたら、Yesをクリックします。

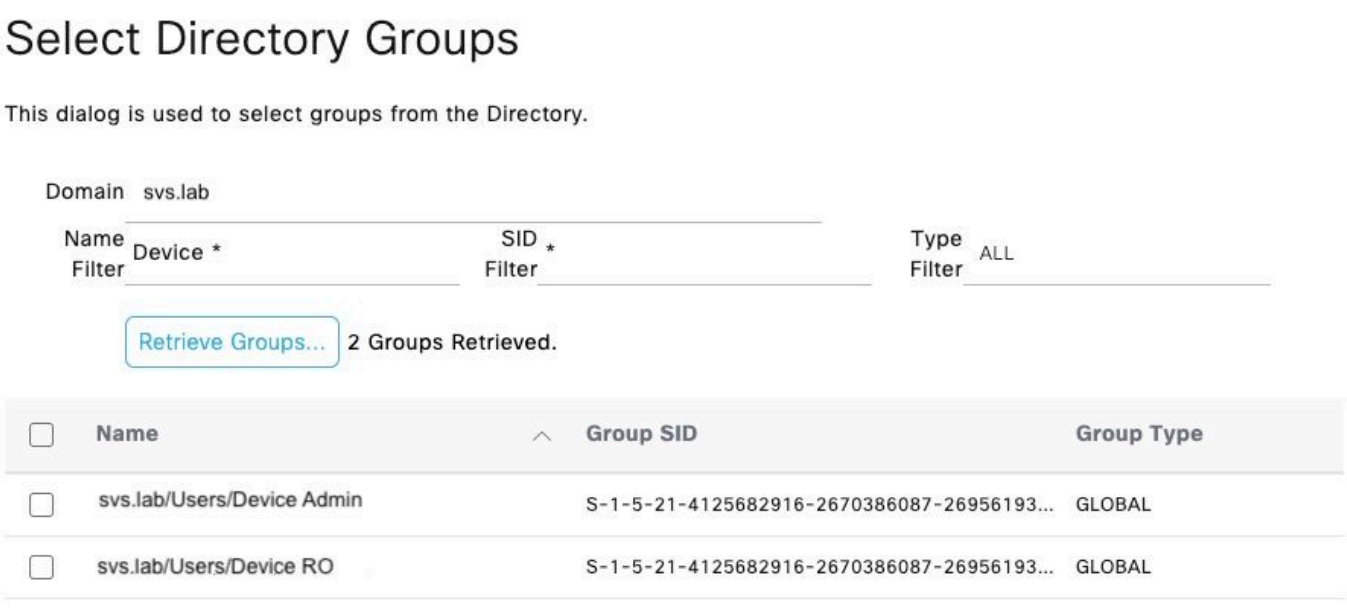
ステップ 4：AD参加権限を持つクレデンシャルを入力し、ISEをADに参加させます。ステータスをチェックして、動作していることを確認します。

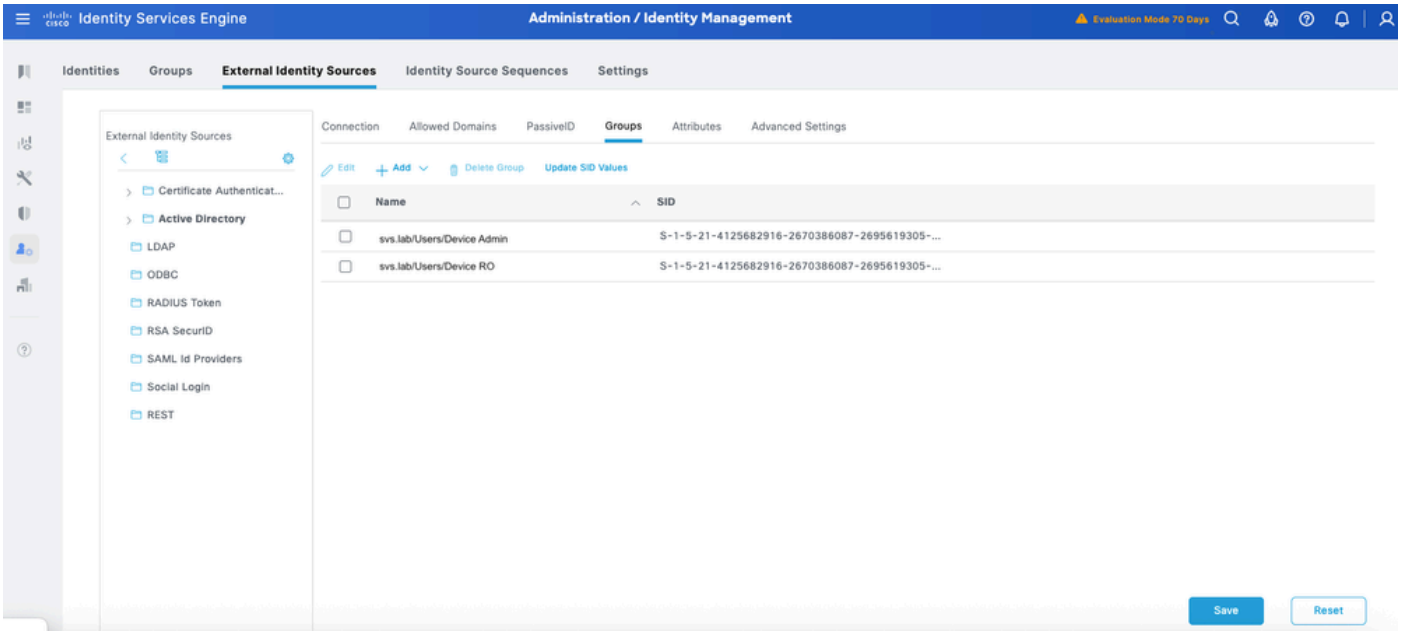




ステップ 5：Groupsタブに移動し、Addをクリックして、デバイスへのアクセスが許可されているユーザに基づいて、必要なすべてのグループを取得します。この例では、このガイドの認可ポリシーで使用されるグループを示します。







TACACS+シェルプロファイルの設定

許可に特権レベルを使用するCisco IOSデバイスとは異なり、Cisco NX-OSデバイスはロールベースアクセスコントロール(RBAC)を実装しています。 ISEでは、Nexusタイプの共通タスクを使用して、TACACS+プロファイルをCisco NX-OSデバイスのユーザロールにマッピングできます。

NX-OSデバイスで事前定義されているロールは、NX-OSプラットフォームによって異なります。次の2つの一般的な方法があります。

- network-admin：事前定義されたネットワーク管理者ロールには、スイッチ上のすべてのコマンドに対する完全な読み取りおよび書き込みアクセス権があります。デバイス（Nexus 7000など）に複数のVDCがある場合にのみ、デフォルトの仮想デバイスコンテキスト(VDC)で使用可能です。NX-OS CLIコマンドshow cli syntax roles network-adminを使用して、このロールで使用可能な完全なコマンドリストを表示します。

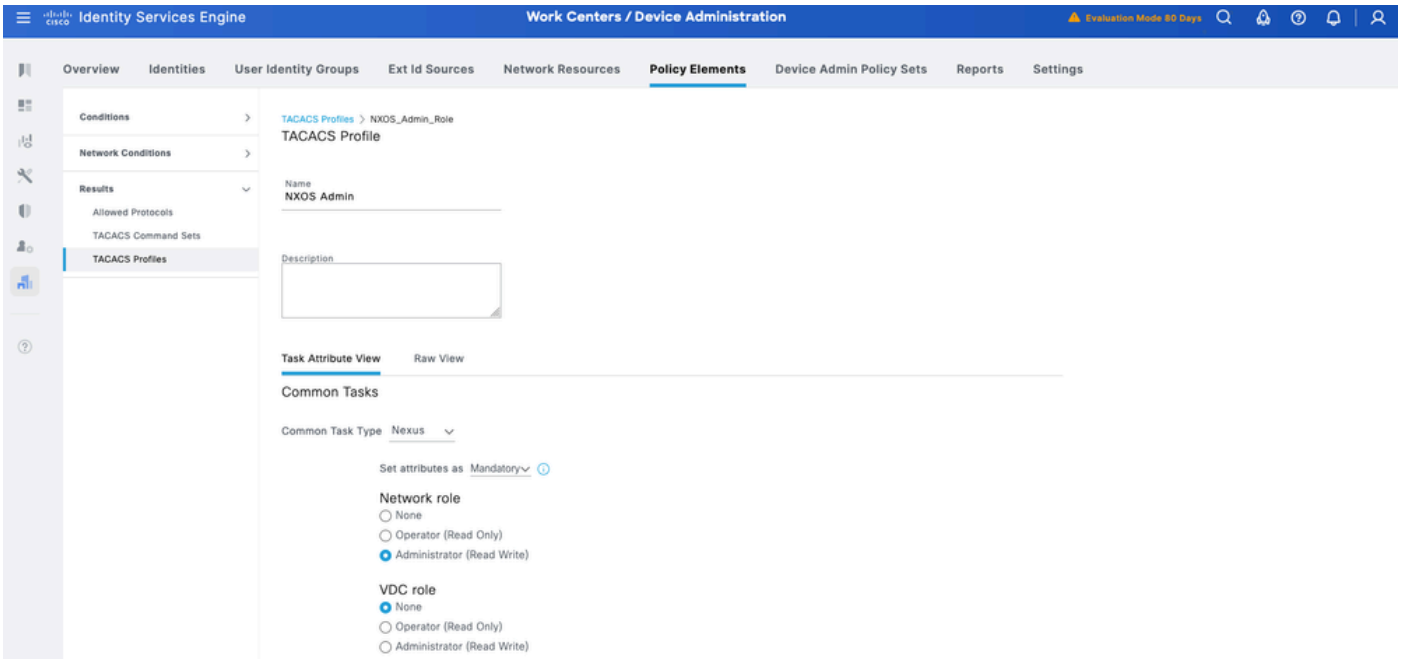
- network-operator：事前定義されたネットワーク管理者ロールには、スイッチ上のすべてのコマンドに対する完全な読み取りアクセス権があります。デバイス（Nexus 7000など）に複数のVDCがある場合にのみ、デフォルトのVDCで使用可能です。NX-OS CLIコマンドshow cli syntax roles network-operatorを使用して、このロールで使用可能な完全なコマンドリストを確認します。

次に、NXOS AdminとNXOS HelpDeskの2つのTACACSプロファイルが定義されています。

NX-OS管理

ステップ 1：別のプロファイルを追加し、NX-OS Adminという名前を付けます。

ステップ 2：Set attributes asドロップダウンからMandatoryを選択します。Common Tasksの下のNetwork-roleオプションからAdministratorを選択します。



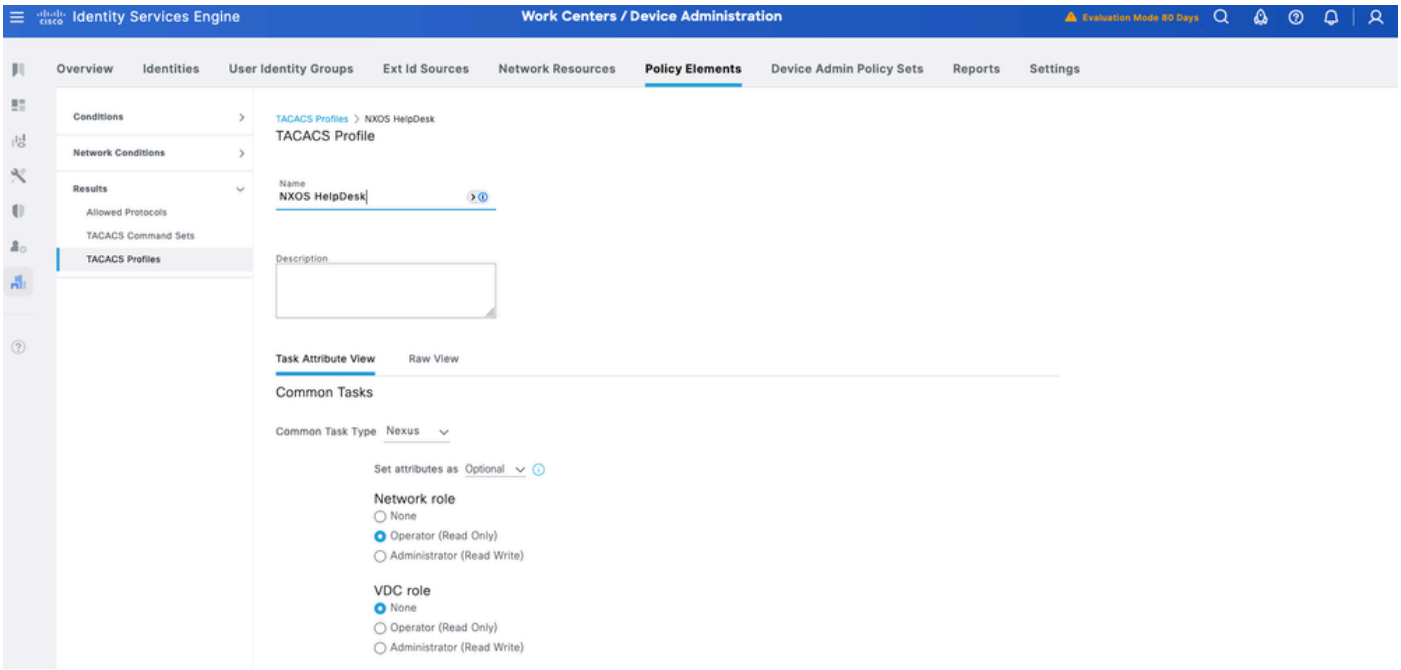
ステップ 3：[Submit] をクリックしてプロファイルを保存します。

NX-OSヘルプデスク

ステップ 1：ISE UIから、Work Centers > Device Administration > Policy Elements > Results > TACACS Profilesの順に移動します。新しいTACACSプロファイルを追加し、NXOS HelpDeskという名前を付けます。Common Task Typeドロップダウンに移動し、 Nexusです。

ユーザロールに固有のテンプレートの変更を確認できます。これらのオプションは、設定するユーザロールに対応して選択できます。

ステップ 2：Set attributes asドロップダウンからMandatoryを選択します。Common Tasksの下のNetwork-roleオプションからOperatorを選択します。

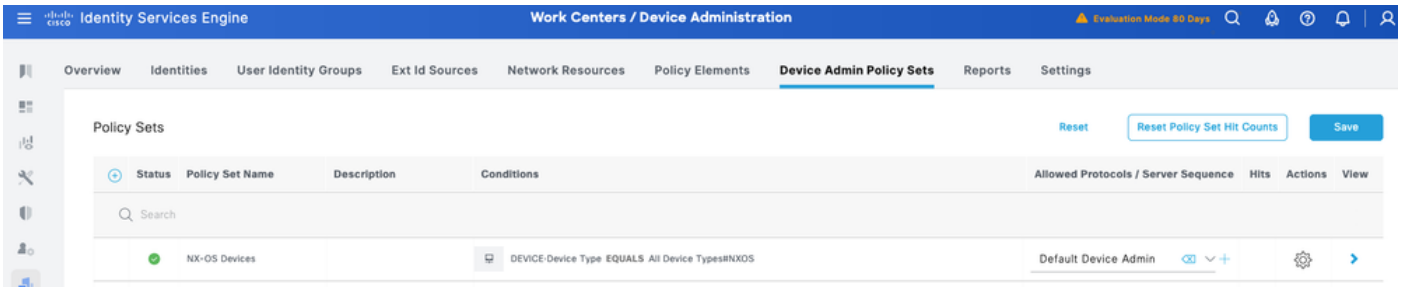


ステップ3:Saveをクリックして、プロファイルを保存します。

デバイス管理ポリシーセットの設定

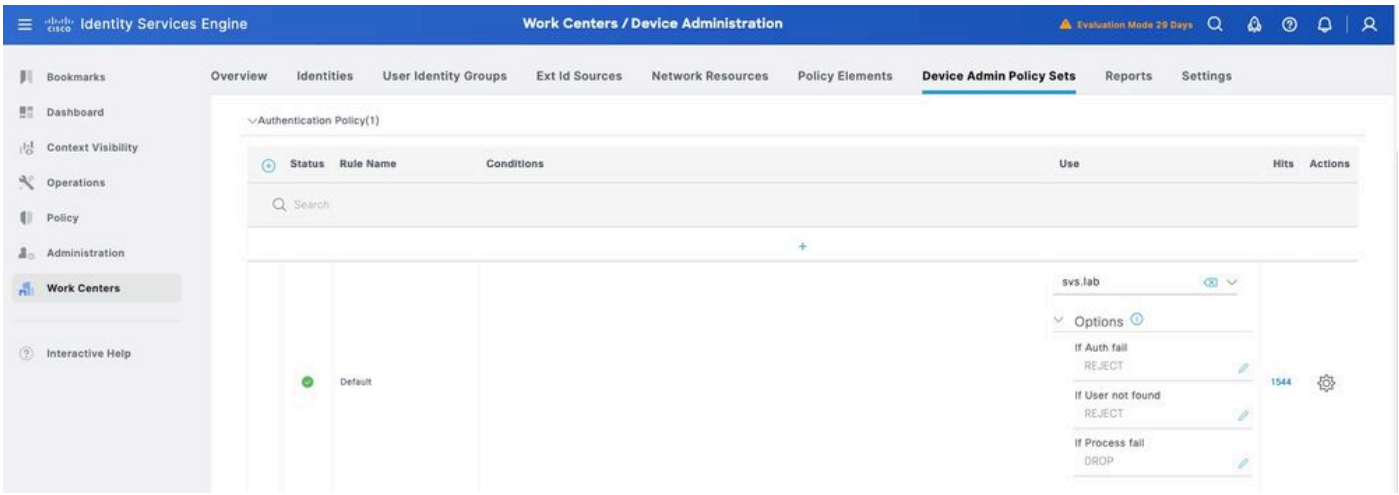
デバイス管理では、ポリシーセットはデフォルトで有効になっています。ポリシーセットは、デバイスタイプに基づいてポリシーを分割できるため、TACACSプロファイルの適用が容易になります。たとえば、Cisco IOSデバイスは特権レベルやコマンドセットを使用し、Cisco NX-OSデバイスはカスタム属性を使用します。

ステップ 1：Work Centers > Device Administration > Device Admin Policy Setsの順に移動します。新しいポリシーセットNX-OS Devicesを追加します。conditionで、DEVICE:Device Type EQUALS All Device Types#NXOSを指定します。Allowed Protocolsの下で、Default Device Adminを選択します。



ステップ 2：Saveをクリックし、右矢印をクリックしてこのポリシーセットを設定します。

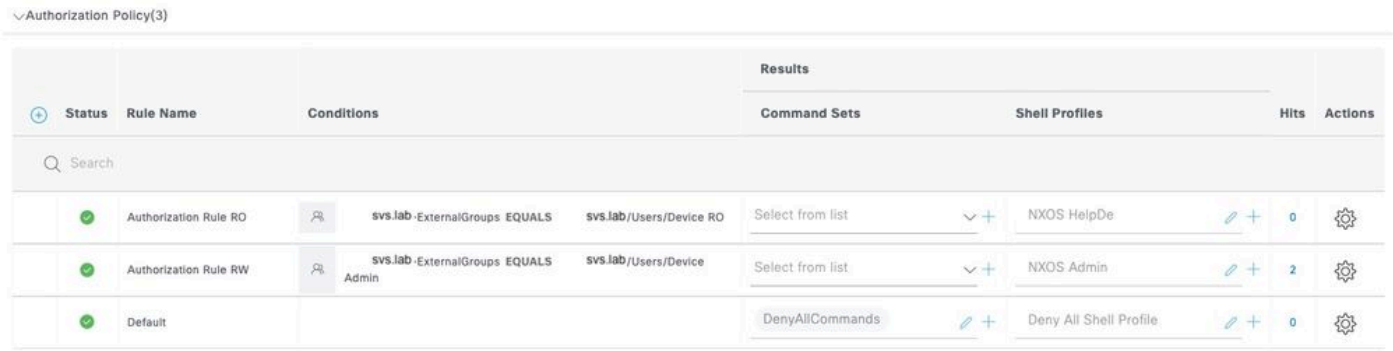
ステップ 3：認証ポリシーを作成します。認証には、ID StoreとしてADを使用します。If Auth fail, If User not foundおよびIf Process failのデフォルトオプションはそのままにします。



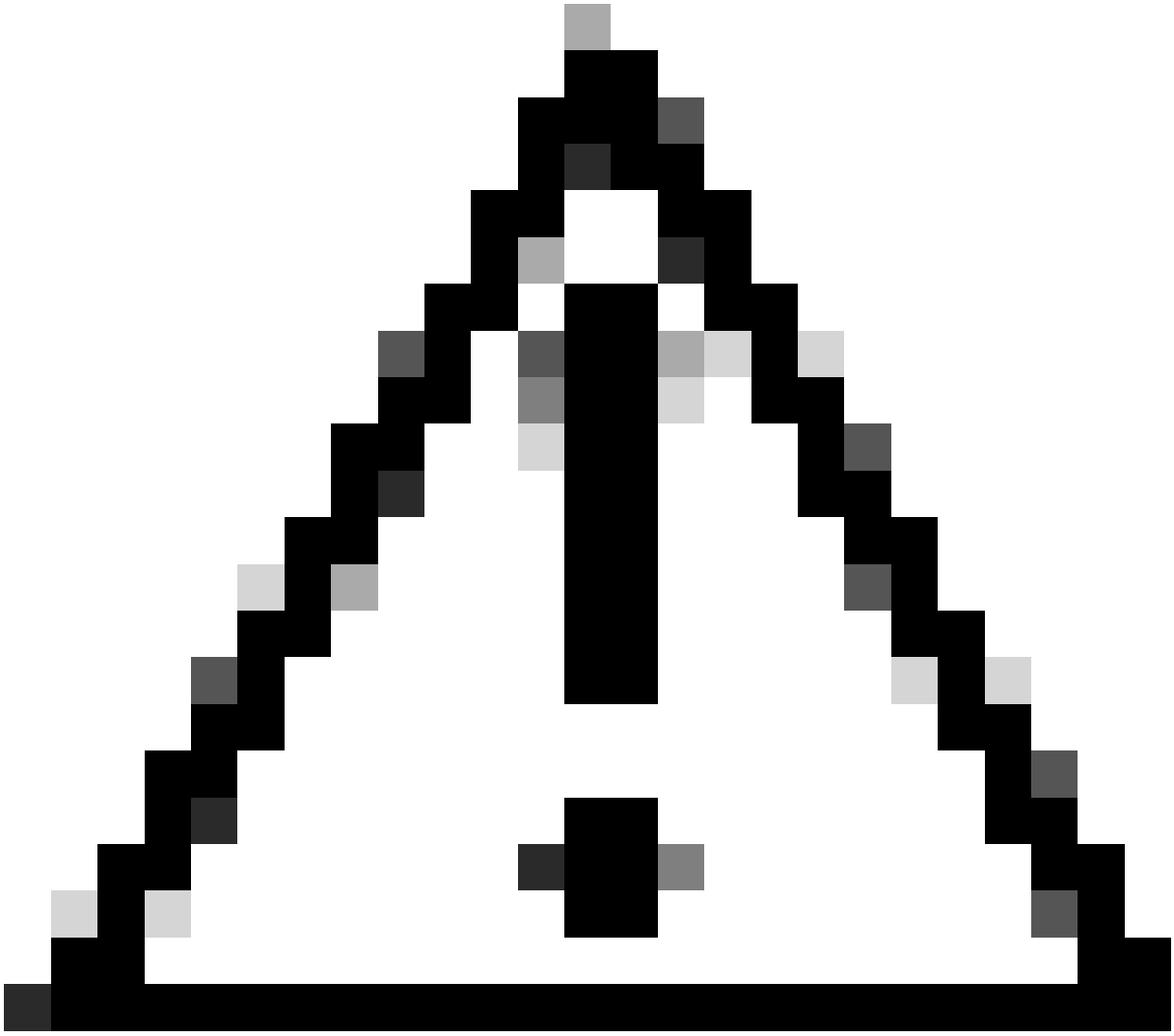
ステップ 4：許可ポリシーを定義します。

Active Directory(AD)のユーザグループに基づいて認可ポリシーを作成します。

例：
- ADグループDevice AdminのユーザにNXOS管理TACACSプロファイルが割り当てられます。
- ADグループDevice ROのユーザにNXOS HelpDesk TACACS Profileが割り当てられます。



TACACS+ over TLS用のCisco NX-OSの設定



注意：コンソール接続が到達可能で、正しく機能していることを確認してください。

ヒント：一時的なユーザを設定し、AAAの認証および認可方式を変更して、設定の変更時にTACACSの代わりにローカルクレデンシャルを使用することで、デバイスからロックアウトされないようにすることをお勧めします。

TACACS+サーバの設定

ステップ 1：初期設定.

```
POD2IPN2# sho run tacacs

feature tacacs+

tacacs-server host 10.225.253.209 key 7 "F1whg.123"
aaa group server tacacs+ tacacs2
```

```
  server 10.225.253.209
  use-vrf management
```

トラストポイントの設定

ステップ 1： キーラベルを作成します。この場合は、eccキーペアを使用します。

<#root>

```
POD2IPN2(config)#
```

crypto key generate ecc label ec521-label exportable modulus 521

ステップ 2：これをトラストポイントに関連付けます。

<#root>

```
POD2IPN2(config)#
```

crypto ca trustpoint ec521-tp

```
POD2IPN2(config-trustpoint)#
```

ecckeypair ec521-label

ステップ 3：CA公開キーをインストールします。

<#root>

```
POD2IPN2(config)#
```

crypto ca authenticate ec521-tp


```
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3sOJ/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrsOtatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBROz+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKVOARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

```
Fingerprint(s): SHA1
Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

Do you accept this certificate? [yes/no]:yes
POD2IPN2(config)#
POD2IPN2(config)#
```

show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient
POD2IPN2(config)#
```

ステップ 4： スイッチID証明書要求を生成します。

<#root>

```
POD2IPN2(config)#
```

crypto ca enroll ec521-tp

```
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:C1sco.123
 The subject name in the certificate will be the name of the switch.
 Include the switch serial number in the subject name? [yes/no]:
```

yes

```
 The serial number in the certificate will be: FDO2649OP4T
 Include an IP address in the subject name [yes/no]:
```

yes

```
ip address:10.225.253.177
 Include the Alternate Subject Name ? [yes/no]:
```

no

```
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwwIUE9EMklQTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6LzpkOhPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q42OmCe8Mef+bqJBdJ9wzpyEjhI2lIIoXt4814nBxObkIWWyR5cZN
IiXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMklQTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/44lul
+3H1y52vn4Rm4CGU3wkzXU3qGO3YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt3OhpaDDOTWzzvZY7qFflCOl5p6pvUpHigqoZNg5
9xhNdM1CQSykOg==
-----END CERTIFICATE REQUEST-----
```

ステップ 5：CAによって署名されたスイッチID証明書をインポートします。

<#root>

```
POD2IPN2(config)#
```

crypto ca import ec521-tp certificate

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
Q0EwHhcNMjUwNTA3MTkxMDAwWhcNMjYwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
T0QySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG94OfFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3DOn
ISOEjaUgihe3jzXicHE5uQhZbJHlxk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAcBgNVHREBAf8EEjAQgghQ
T0QySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZO1PUXNTyZidXpGd/yTrdQAl5JzpW4pEudrbCJMZEEYtqoP
wD+4OE8vKoYEgyWlDrpRZOZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
liToeYy2Q0cTesSZCKvRBv6Ewj5JuSLemURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61LnlVxhXombiS6
INoa0GvQONrl+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MWtkK1wVO16Hv7vGpSMYonD6
a271im+tJPyKnnezQ6OykzlGqsL/Ta6JOdip/fEYp8UmRq9InDh23gDjqrojWL7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJTlnuk5KCqFx//4P7mAoyZYiTIDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sgOO6Y6wIXyTP0UB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
```

```
lfKuuebdZkbwz72r7OyyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

スイッチのID証明書が登録されていることを確認します。

<#root>

```
POD2IPN2(config)#
```

```
show crypto ca certificates ec521-tp
```

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FDO2649OP4T
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=0BACD2EFA5D80E6F
notBefore=May  7 19:10:00 2025 GMT
notAfter=May  7 19:10:00 2026 GMT
SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13
purposes: sslserver sslclient

CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient

POD2IPN2(config)#
```

TACACS+ TLSの設定

注意：コンソールからローカルクレデンシャルを使用して、これらの設定変更を行います。

ステップ 1： global tacacs tlsを設定します。

<#root>

```
POD2IPN2(config)#
tacacs-server secure tls
```

ステップ 2：ISEサーバが設定されているTLSポートにISEポートを変更します。

<#root>

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

ステップ 3：スイッチのISEサーバ設定をTLS接続用のトラストポイントに関連付けます。

<#root>

```
POD2IPN2(config)#
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

ステップ 4：tacacsサーバグループを作成します。

<#root>

```
POD2IPN2(config)#
aaa group server tacacs+ tacacs2

POD2IPN2(config-tacacs+)#
server 10.225.253.209

POD2IPN2(config-tacacs+)#
use-vrf management
```

ステップ 5：設定を確認します。

<#root>

```
POD2IPN2#
sho run tacacs

feature tacacs+

tacacs-server secure tls
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
aaa group server tacacs+ tacacs2
    server 10.225.253.209
    use-vrf management
```

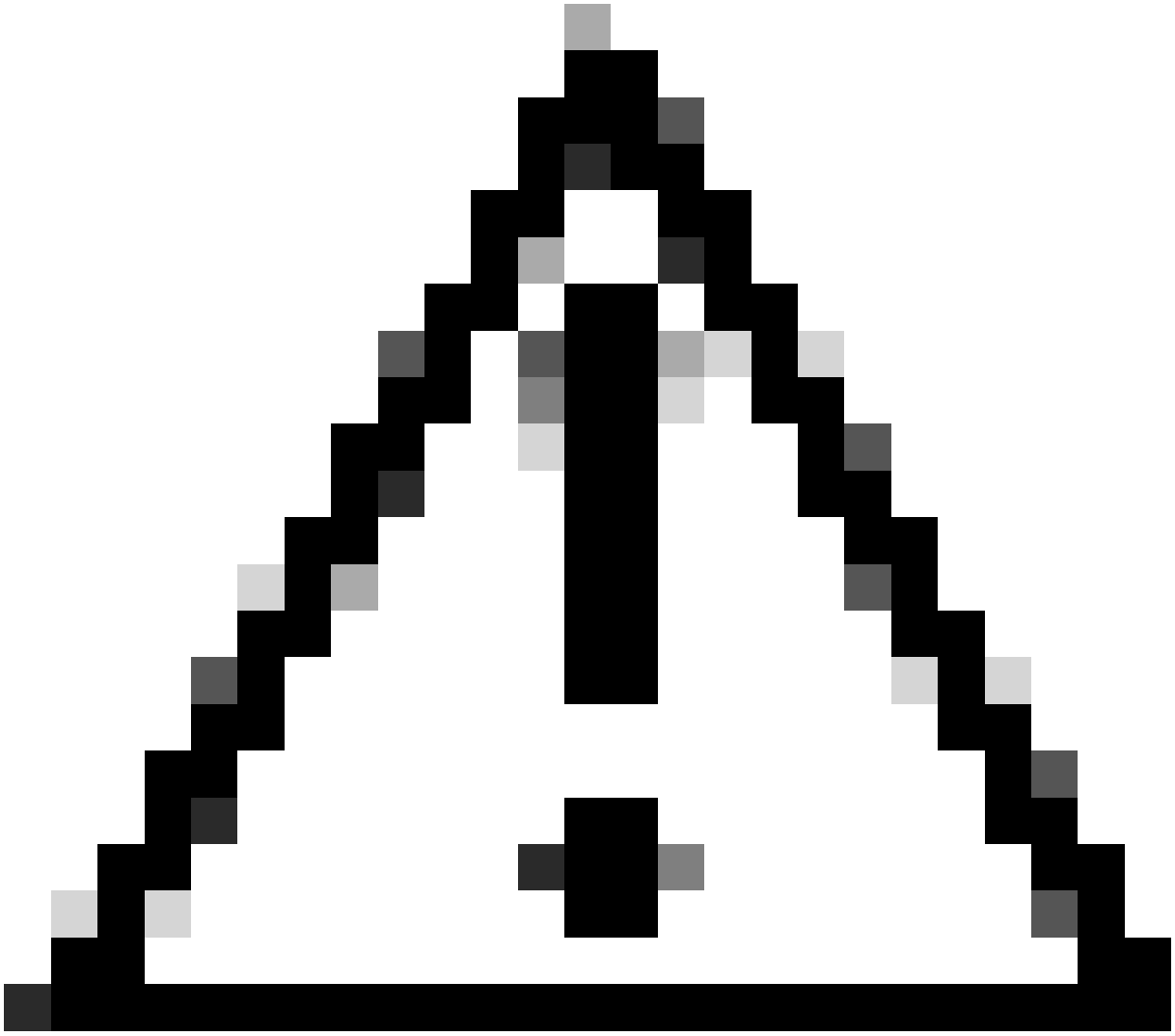
手順 6：AAA認証を設定する前に、リモートユーザをテストします。

<#root>

```
POD2IPN2#
test aaa group tacacs2
```

```
user has been authenticated
POD2IPN2#
```

AAA 設定



注意:AAAの設定に進む前に、リモートユーザ認証が成功していることを確認してくださ

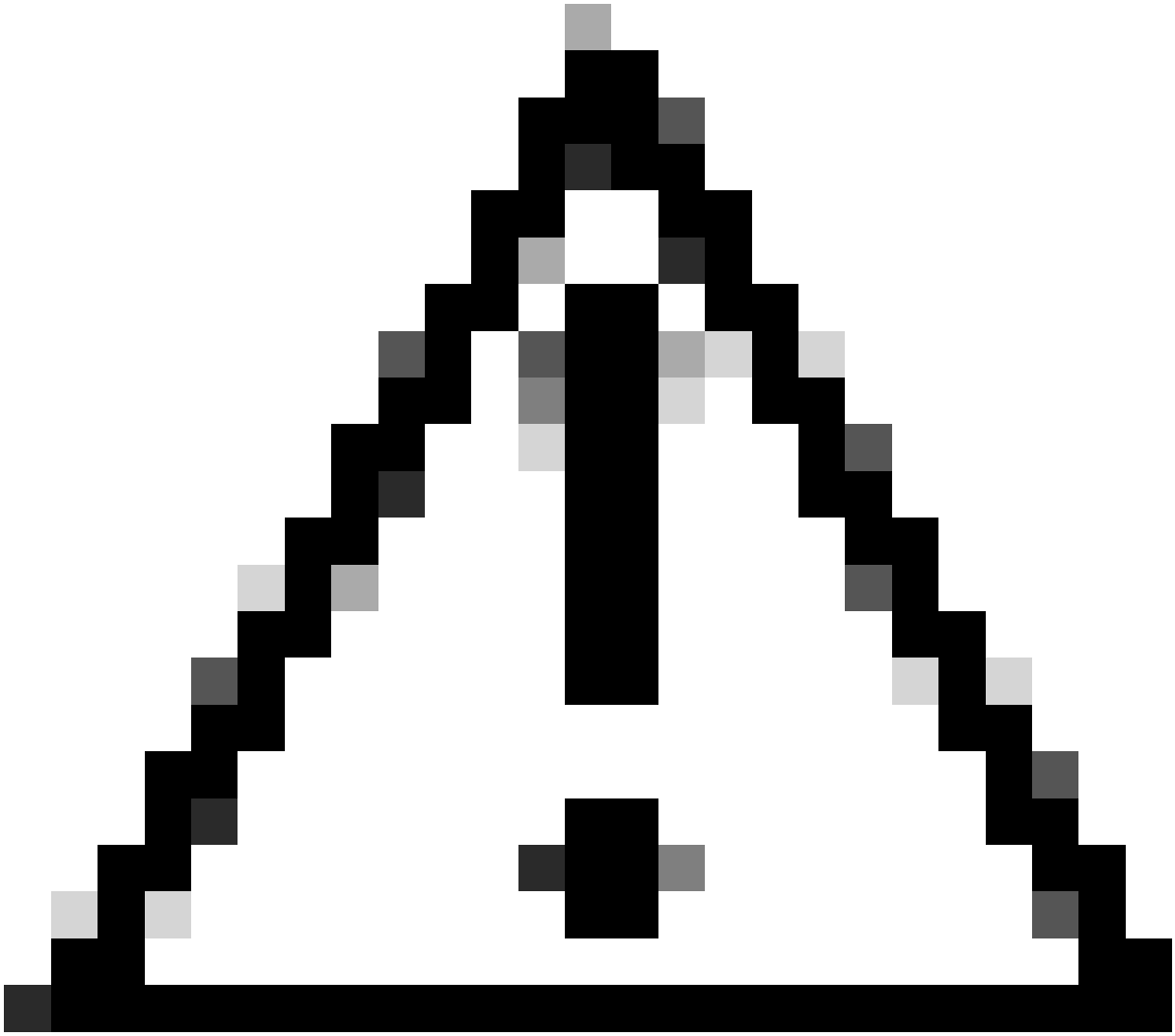
い。

ステップ 1：AAAリモート認証を設定します。

<#root>

```
POD2IPN2(config)#
aaa authentication login default group tacacs2
```

ステップ 2：コマンドのテスト後に、AAAリモート認可を設定します。



注意: authorization-statusが「AAA_AUTHOR_STATUS_PASS_ADD」と表示されていることを確認してください。

<#root>

```
POD2IPN2#
test aaa authorization command-type config-commands default user
```

```
        command "feature bgp"
```

```
sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD
```

ステップ 3：AAAコマンドとconfig-command認可を設定します。

<#root>

```
POD2IPN2(config)#
aaa authorization config-commands default group tacacs2 local
```

```
POD2IPN2(config)#
aaa authorization commands default group tacacs2 local
```

NX-OSのユーザアクセスのテストとトラブルシューティング

検証

Cisco NX-OSのデバイス管理の設定が完了しました。設定を検証する必要があります。

ステップ 1：SSHを実行し、さまざまなロールとしてNX-OSデバイスにログインします。

ステップ 2：デバイスのコマンドラインインターフェイス(CLI)で、ユーザが適切なコマンドにアクセスできることを確認します。たとえば、ヘルプデスクユーザは通常のIPアドレス（10.225.253.129など）にpingできるが、実行コンフィギュレーションを表示することを拒否される必要があります。

```
POD2IPN1# ping 10.225.253.129 vrf management
PING 10.225.253.129 (10.225.253.129): 56 data bytes
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms
```

```
--- 10.225.253.129 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.638/0.692/0.817 ms
POD2IPN1#
POD2IPN1# show running-config
% Permission denied for the role
```

トラブルシューティング

NX-OS構成の検証。

```
POD2IPN2# show crypto ca certificates
POD2IPN2# show crypto ca trustpoints
POD2IPN2# show tacacs-server statistics <server ip>
```

ユーザの接続とロールを表示するには、次のコマンドを使用します。

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
NAME LINE TIME IDLE PID COMMENT
Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh *
POD2IPN1# show user-account Admin-ro
user:Admin-ro
roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

TACACS+のトラブルシューティングでは、次のデバッグが役立ちます。

```
debug TACACS+ aaa-request
2016 Jan 11 03:03:08.652514 TACACS[6288]:  process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]:  process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]:  process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]:  process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]:  state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]:  is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]:  is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]:  debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]:  35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]:  36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]:  36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 TACACS[6288]:  debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]:  tplus_encrypt(659):key is configured for this aaa sessin.
2016 Jan 11 03:03:08.655054 TACACS[6288]:  num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]:  non_blocking_connect(259):interface ip_type: IPV4
```

```
2016 Jan 11 03:03:08.656023 TACACS[6288]:  non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]:  non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 TACACS[6288]:  non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]:  tplus_decode_authen_response: copying hostname into context
```

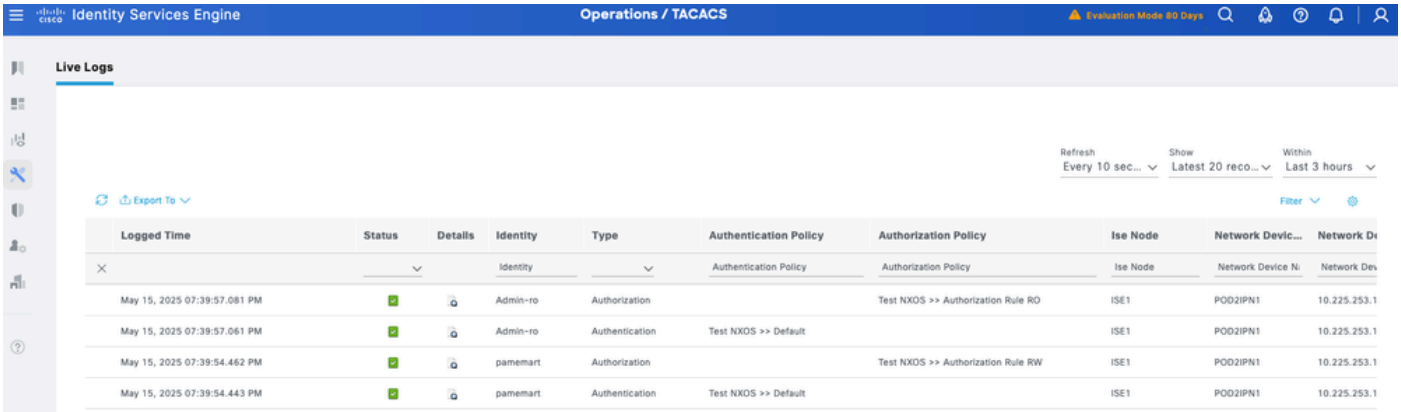
SSLデバッグを有効にします。

```
touch '/bootflash/.enable_ssl_debugs'
```

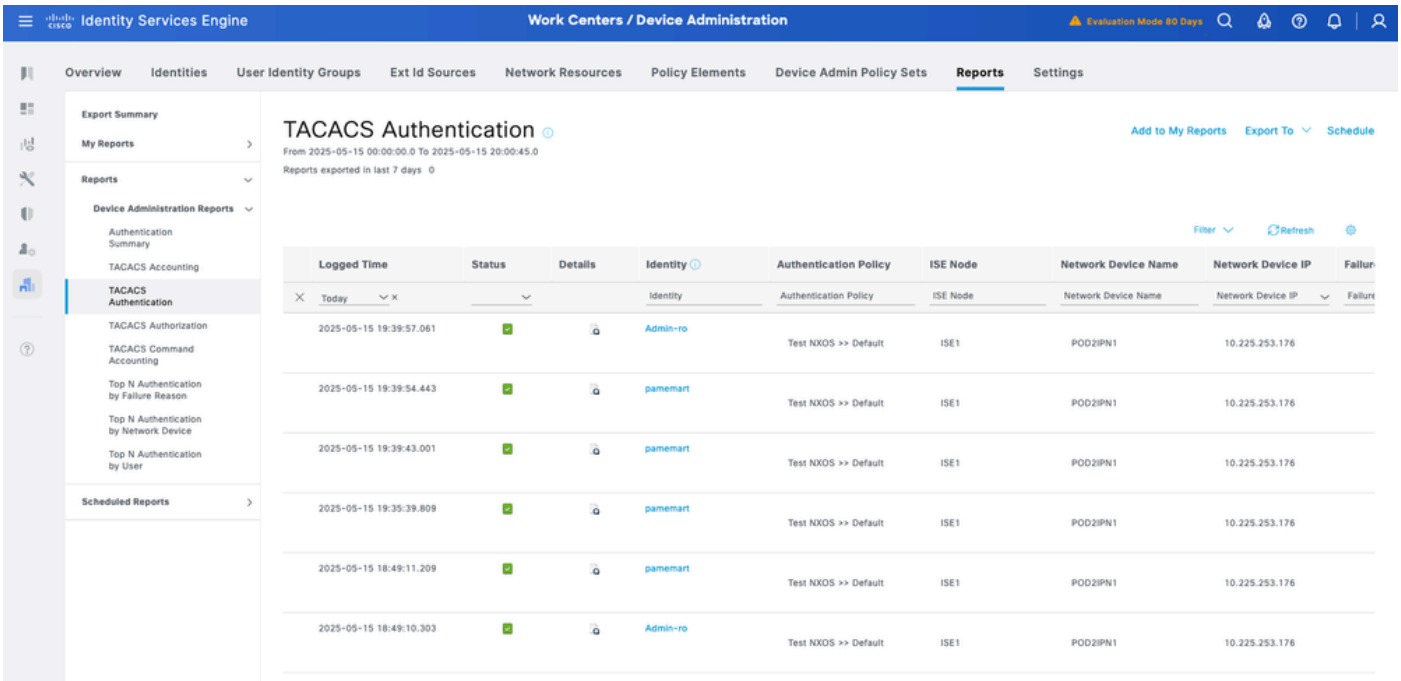
デバッグファイルの内容を表示します。

```
cat /tmp/ssl_wrapper.log.*
```

ISEのGUIで、Operations > TACACS Livelogの順に移動します。すべてのTACACS認証要求と認可要求がここにキャプチャされます。詳細ボタンには、特定のトランザクションが成功/失敗した理由に関する詳細情報が表示されます。



履歴レポートの場合：Work Centers > Device Administration > Reports > Device Administrationの順に移動して、認証、認可、アカウンティング(AAA)レポートを取得します。


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 80 Days
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Export Summary
My Reports
Reports
Device Administration Reports
Authentication Summary
TACACS Accounting
TACACS Authentication
TACACS Authorization
TACACS Command Accounting
Top N Authentication by Failure Reason
Top N Authentication by Network Device
Top N Authentication by User
Scheduled Reports
TACACS Authentication
From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0
Reports exported in last 7 days 0
Add to My Reports
Export To
Schedule
Filter
Refresh
Logged Time
Status
Details
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
Today
2025-05-15 19:39:57.061
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:54.443
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:43.001
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:35:39.809
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:11.209
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:10.303
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176

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。