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

内容

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 IOS® XR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 IOS XR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 IOS XRの設定

前提条件

要件

TACACS+ over TLSを設定するための要件：

- 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。

- ISE VMware仮想アプライアンス、リリース3.4パッチ2
- Cisco 8201ルータ、リリース25.3.1

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。

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。

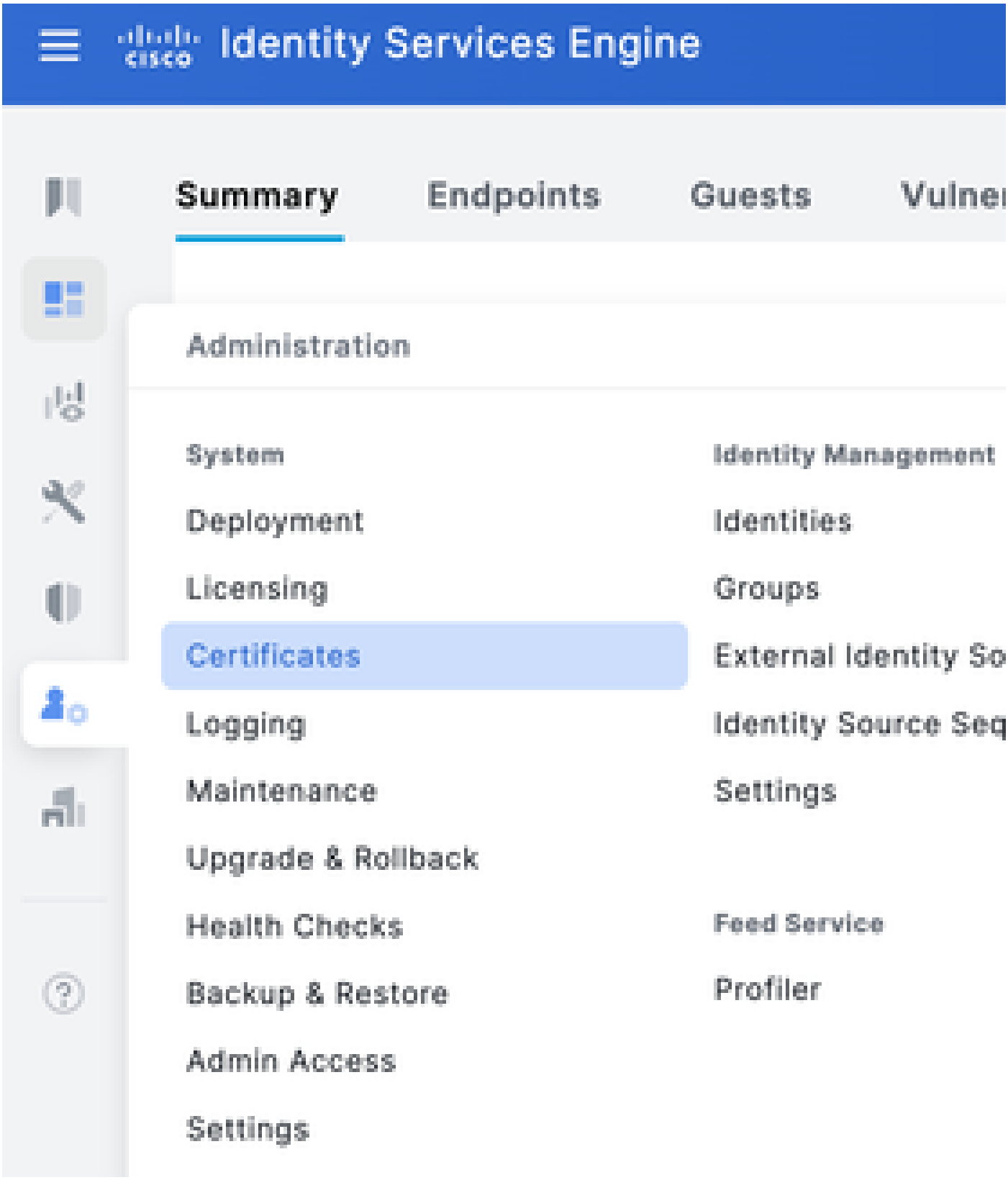
パート1：デバイス管理用のISE設定

TACACS+サーバ認証用の証明書署名要求の生成

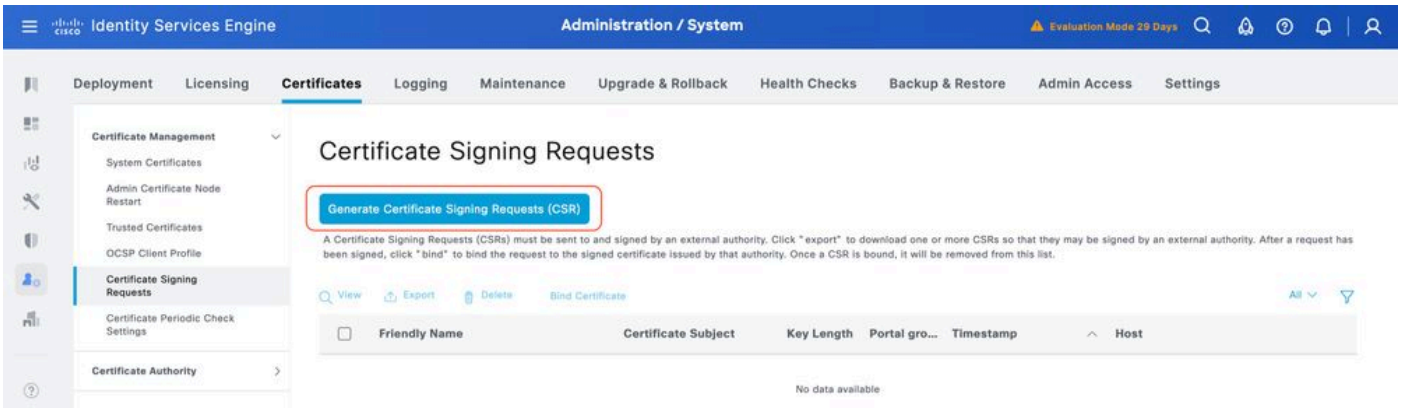
ステップ 1： サポートされているいずれかのブラウザを使用して、ISE管理Webポータルにログインします。

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の順に移動します。

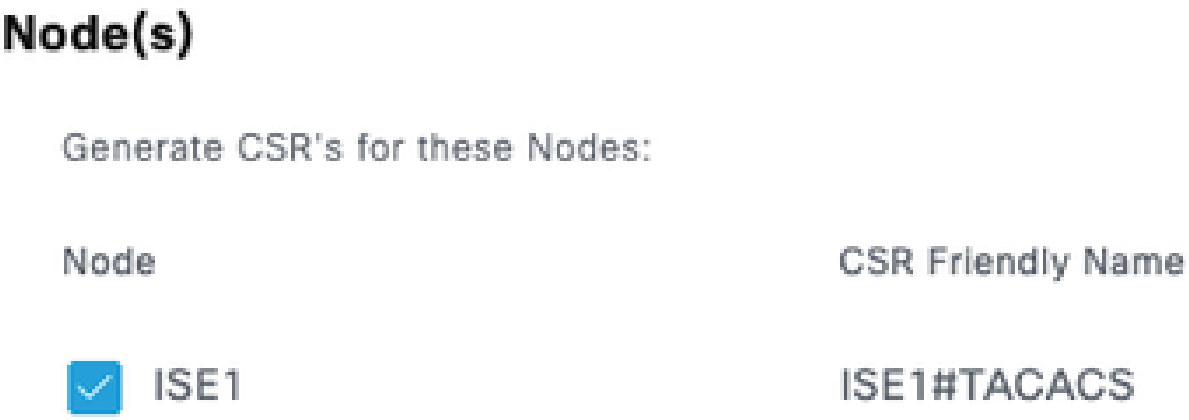


ステップ3:Certificate Signing Requestsの下で、Generate Certificate Signing Requestをクリックします。

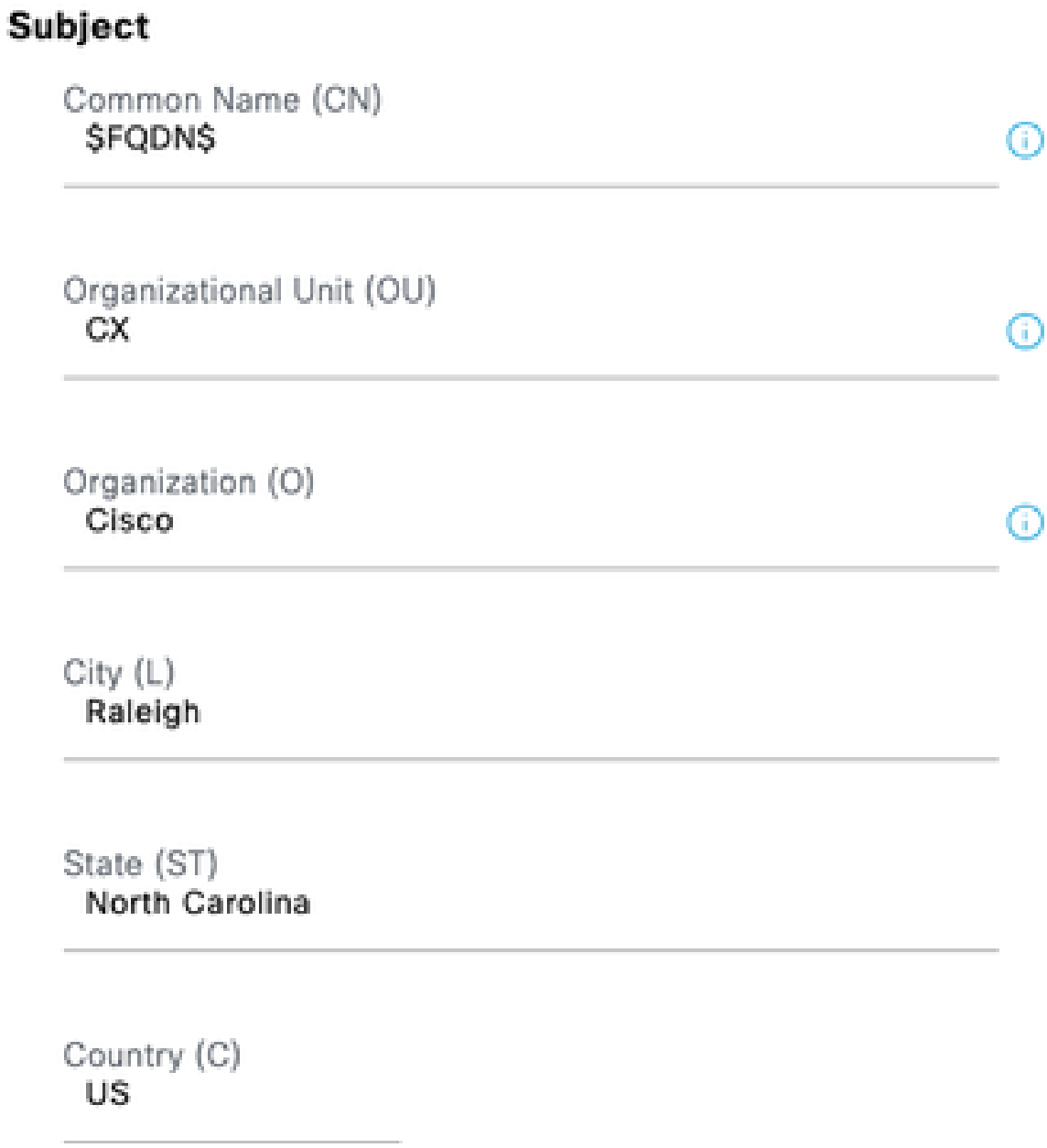


ステップ 4： inUsageのTACACSを選択します。

ステップ 5： TACACS+が有効になっているPSNを選択します。

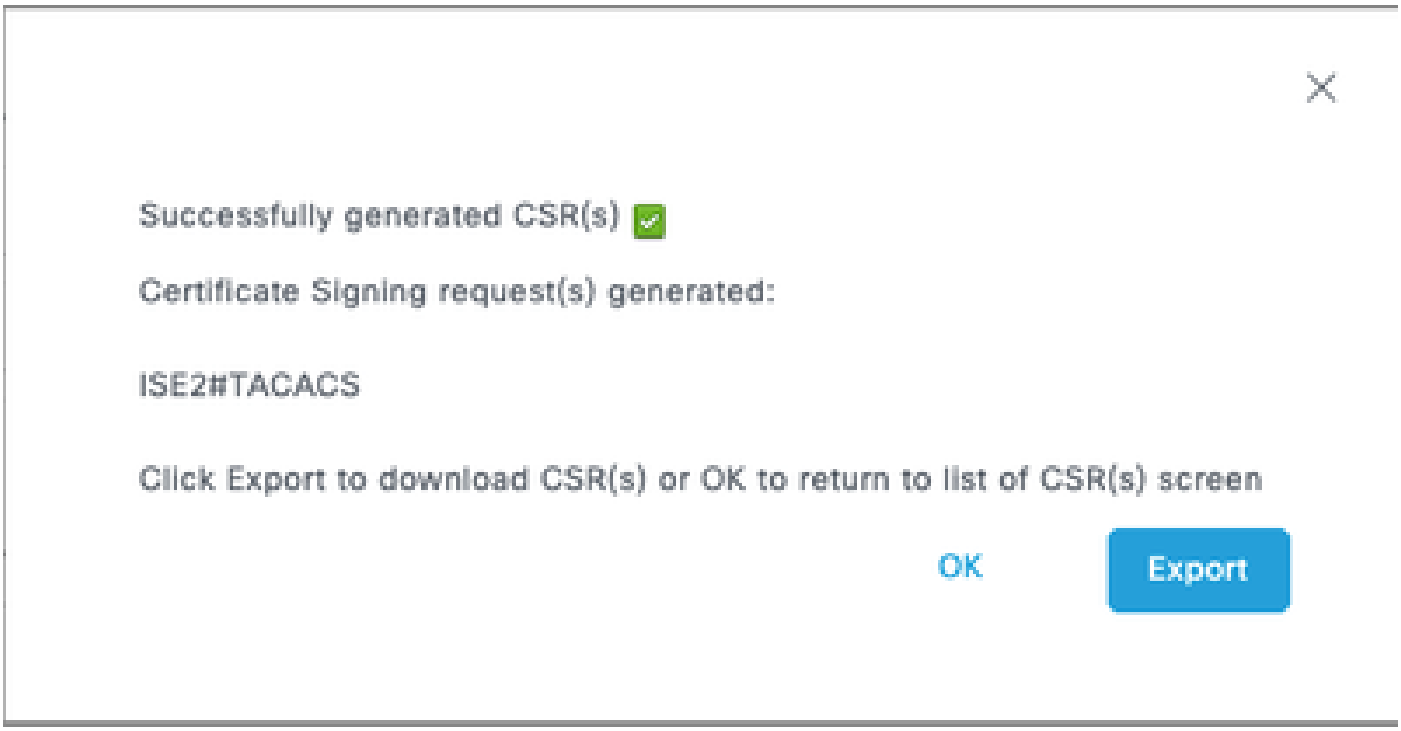


手順 6： Subjectフィールドに、適切な情報を入力します。



手順 7： Subject Alternative Name (SAN)の下にDNS名とIPアドレスを追加します。

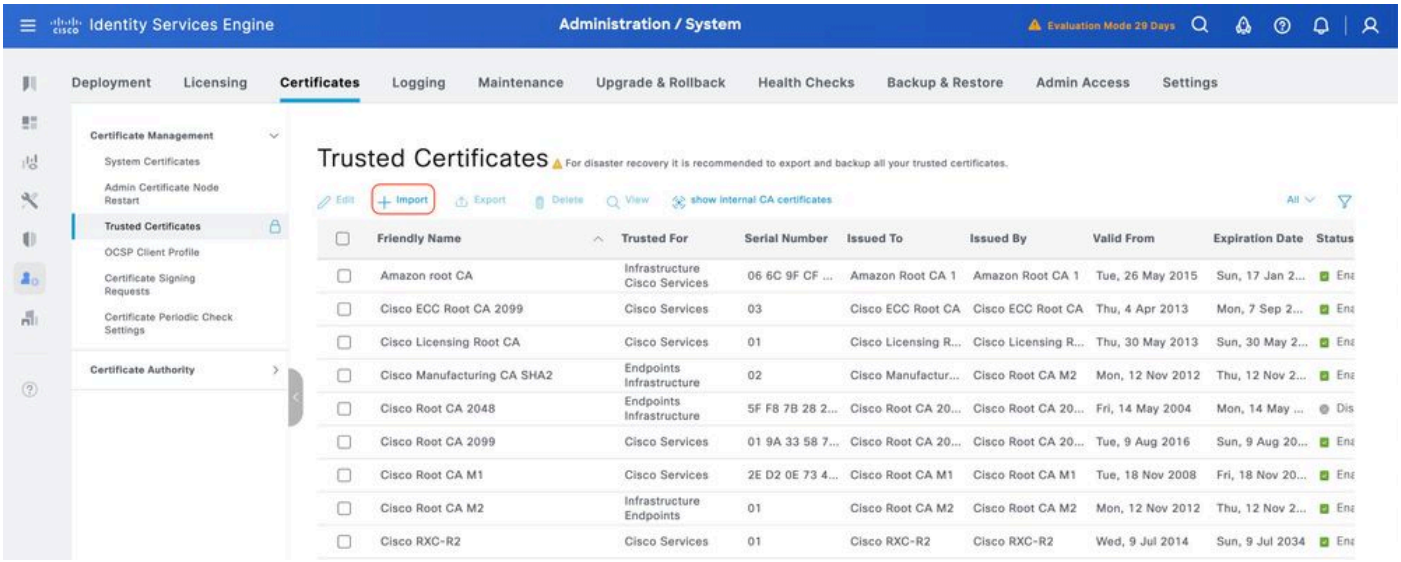
ステップ 8： Generateをクリックし、次にExportをクリックします。



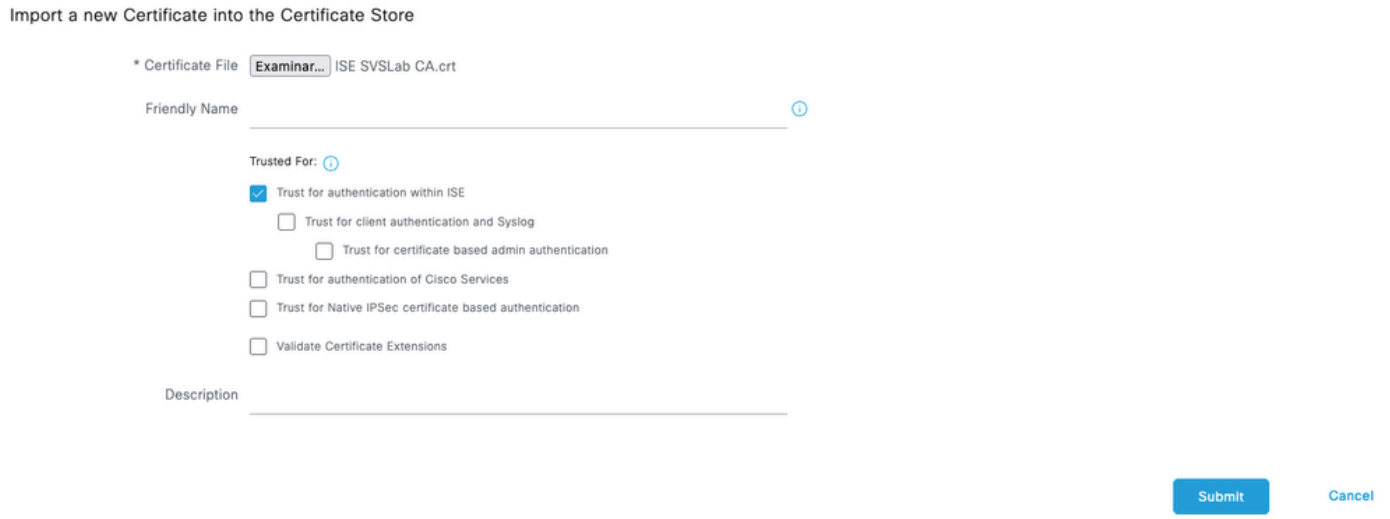
これで、認証局(CA)によって署名された証明書(CRT)を取得できます。

TACACS+サーバ認証用のルートCA証明書のアップロード

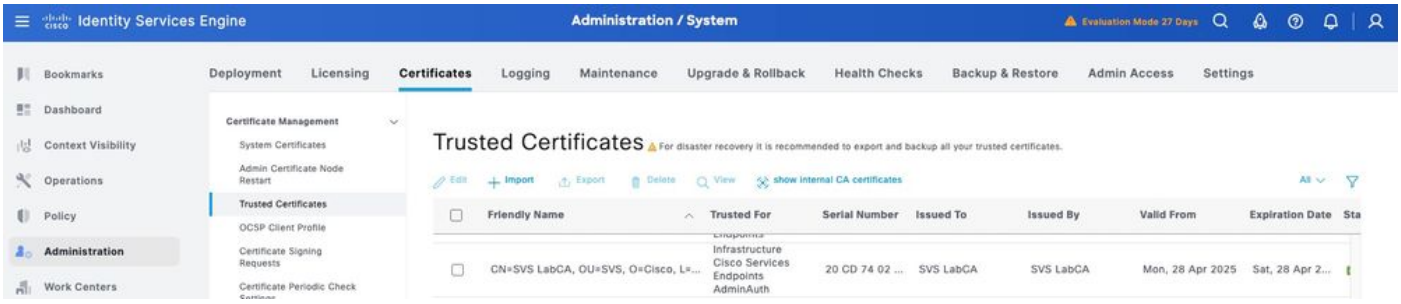
ステップ1:Administration > System > Certificatesの順に移動します。Trusted Certificatesの下にあるImportをクリックします。



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。 次のことを確認してください。 ISE内での認証の信頼性 オプションが有効になっている。



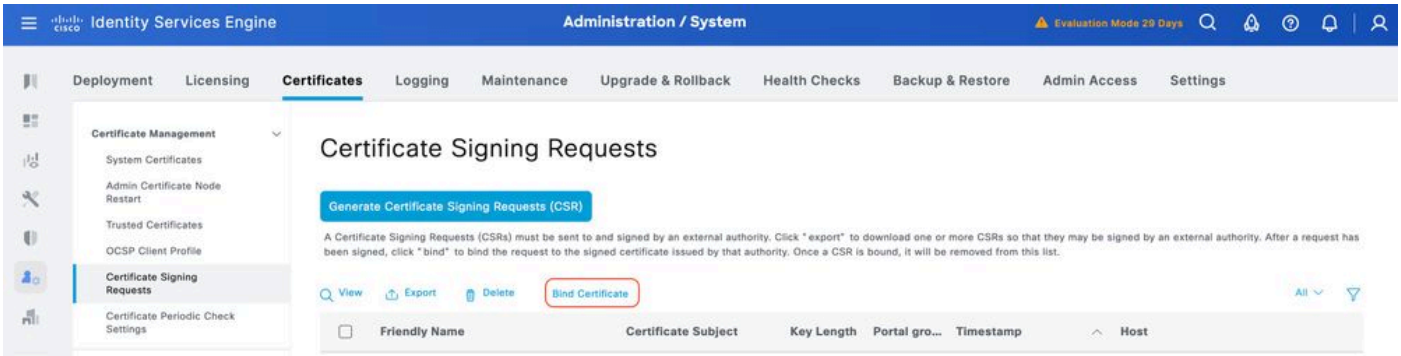
Submitをクリックします。証明書がTrusted Certificatesの下に表示されている必要があります。



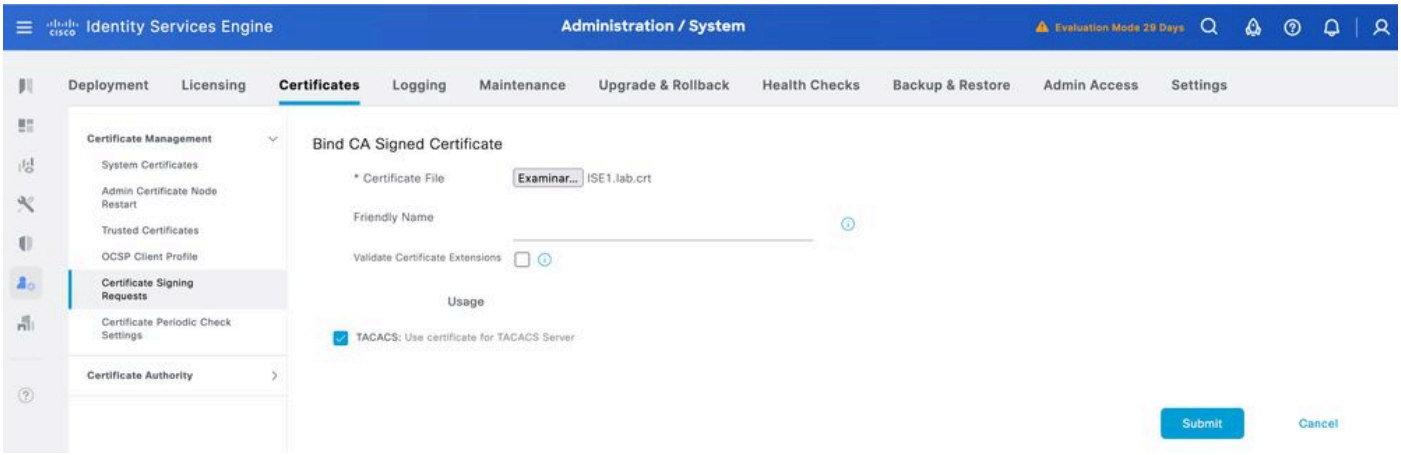
署名付き証明書署名要求(CSR)のISEへのバインド

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されたTACACS CSRを選択し、Bind Certificateをクリックします。

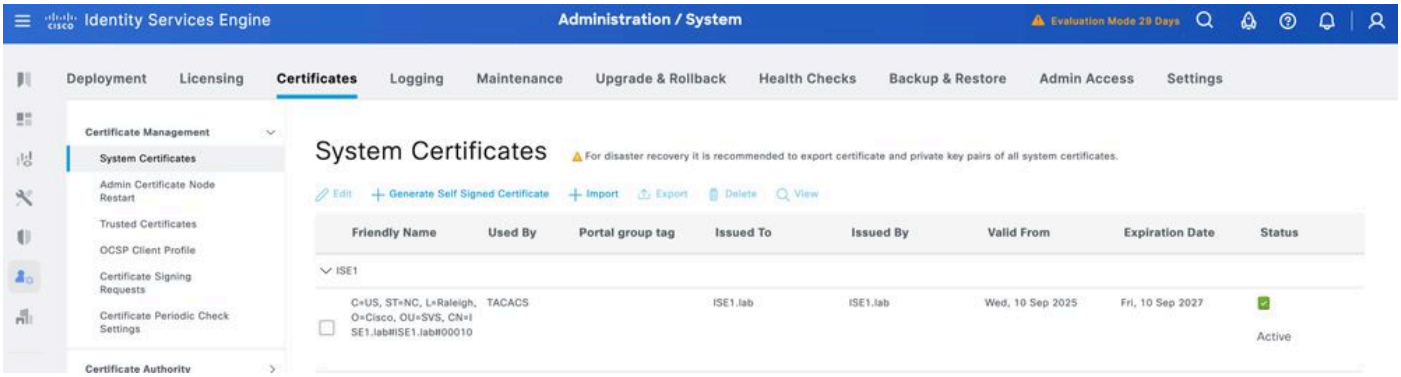


ステップ2:署名付き証明書を選択し、Usageの下のTACACSチェックボックスが選択されたままになっていることを確認します。



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。

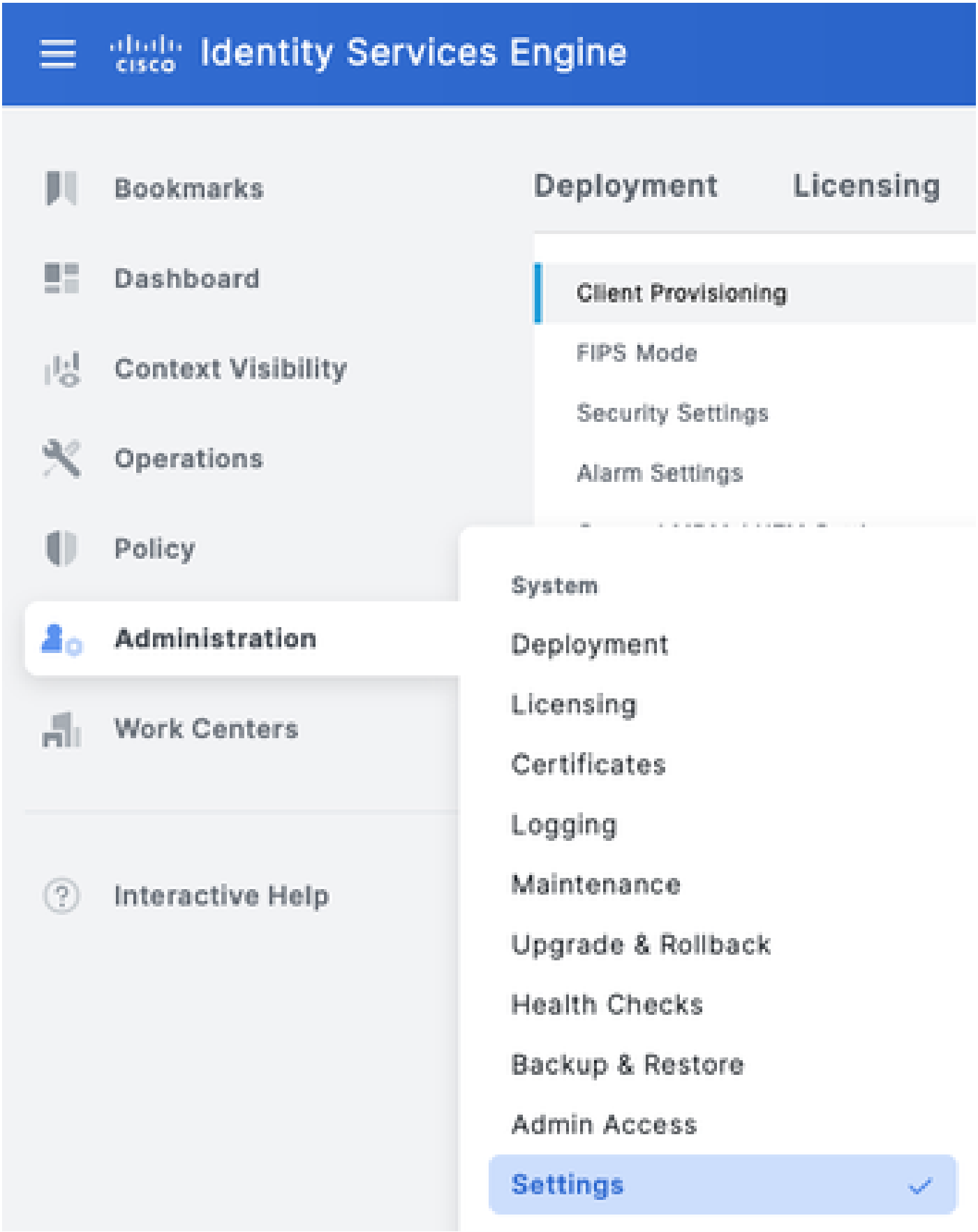
これで、証明書が正しくインストールされました。これは、「システム証明書」で確認できます。



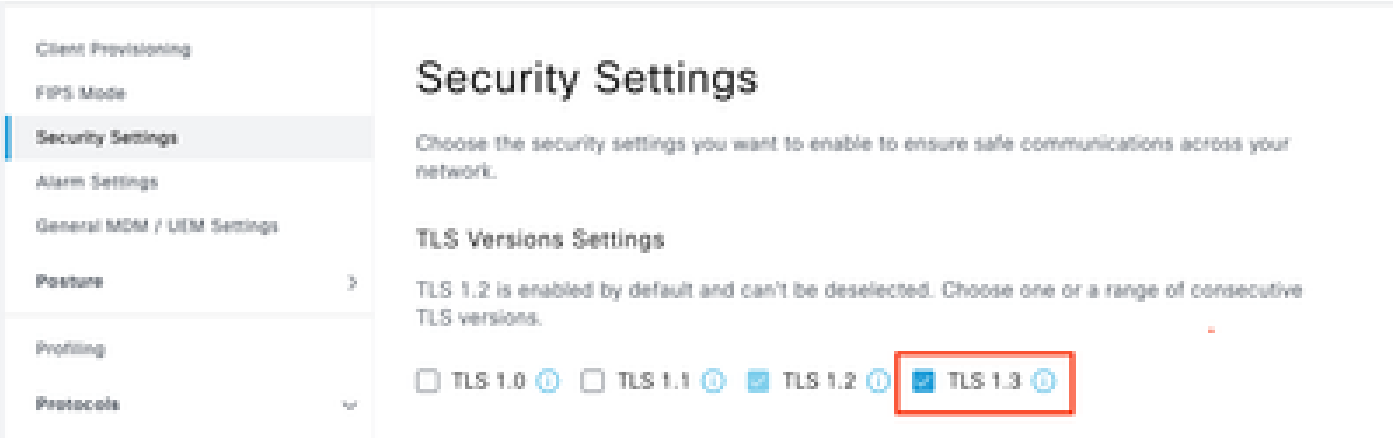
TLS 1.3を有効にする

ISE 3.4.xでは、TLS 1.3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の順に移動します。



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。

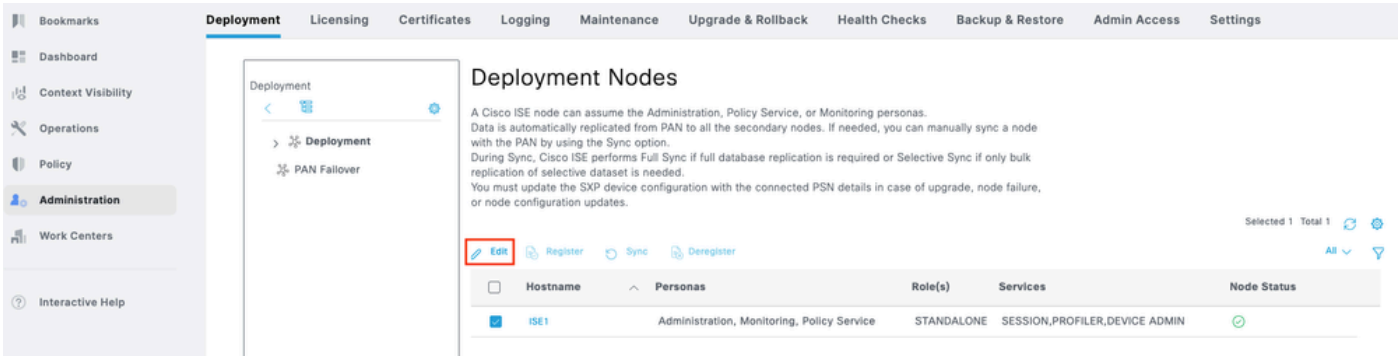


警告:TLSバージョンを変更すると、Cisco ISEアプリケーションサーバがすべてのCisco ISE導入マシンで再起動します。

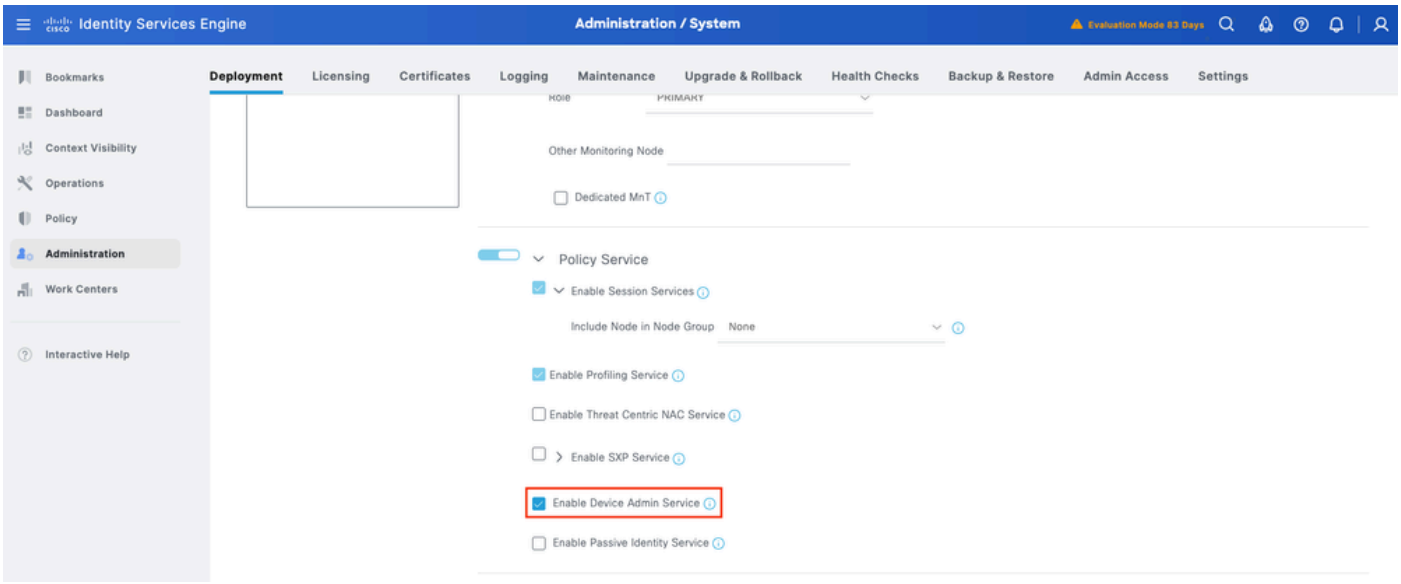
ISEでのデバイス管理の有効化

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+を有効にするには、次の手順を実行します。

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て、Editをクリックします。



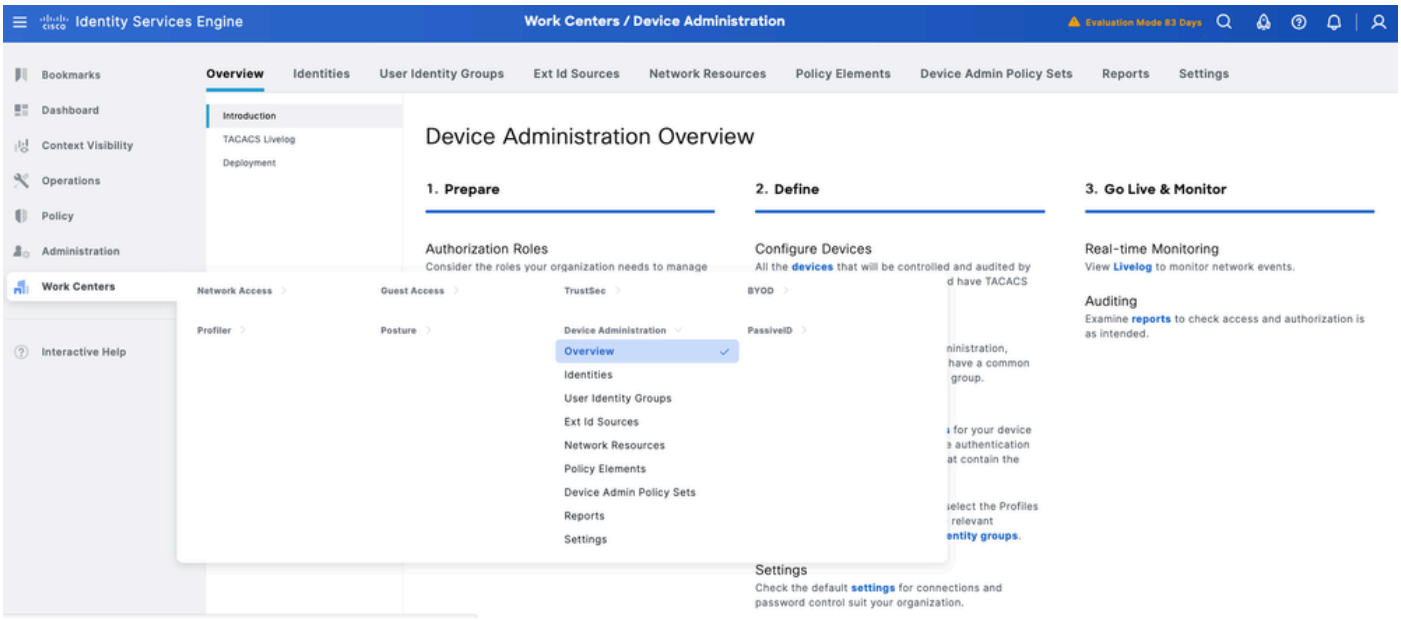
ステップ2:GeneralSettingsで、下にスクロールしてEnable Device Admin Serviceの横にあるチェックボックスをオンにします。



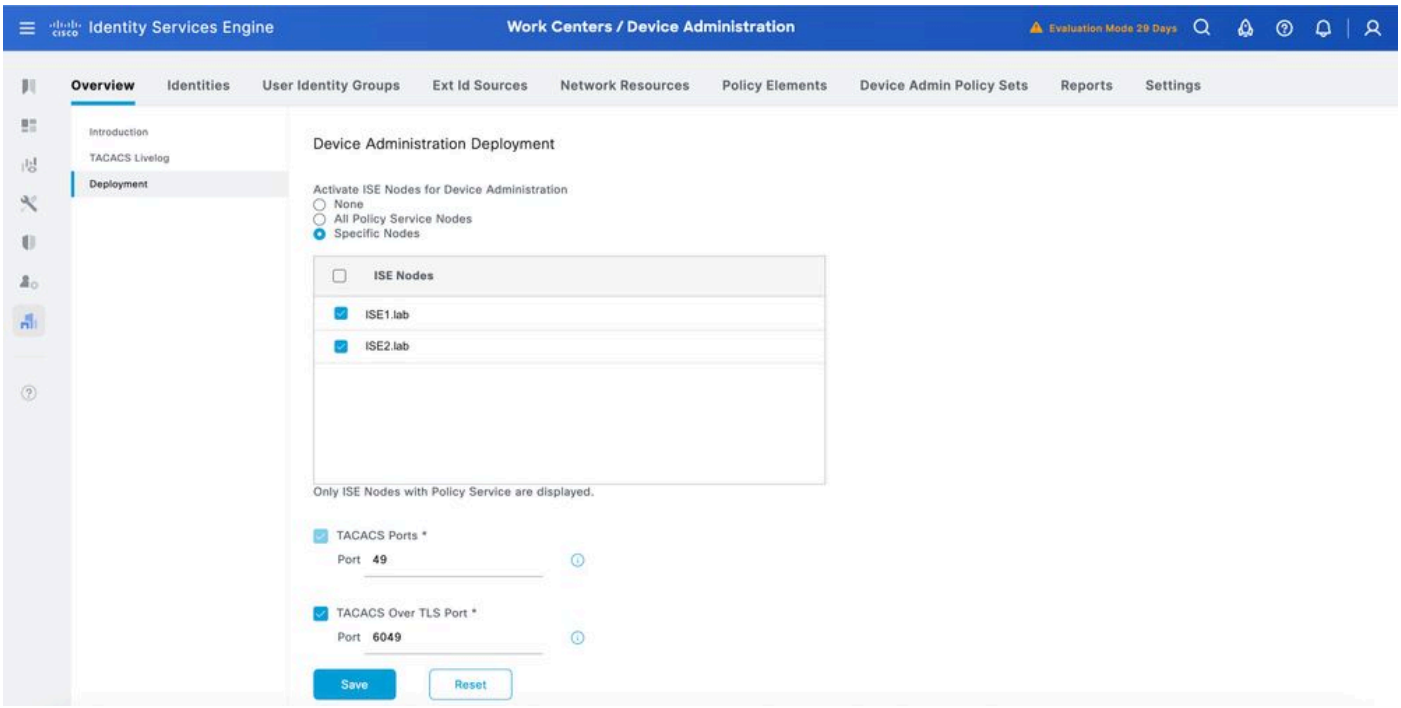
ステップ 3： 設定を保存します。Device Admin ServiceがISEで有効になりました。

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。

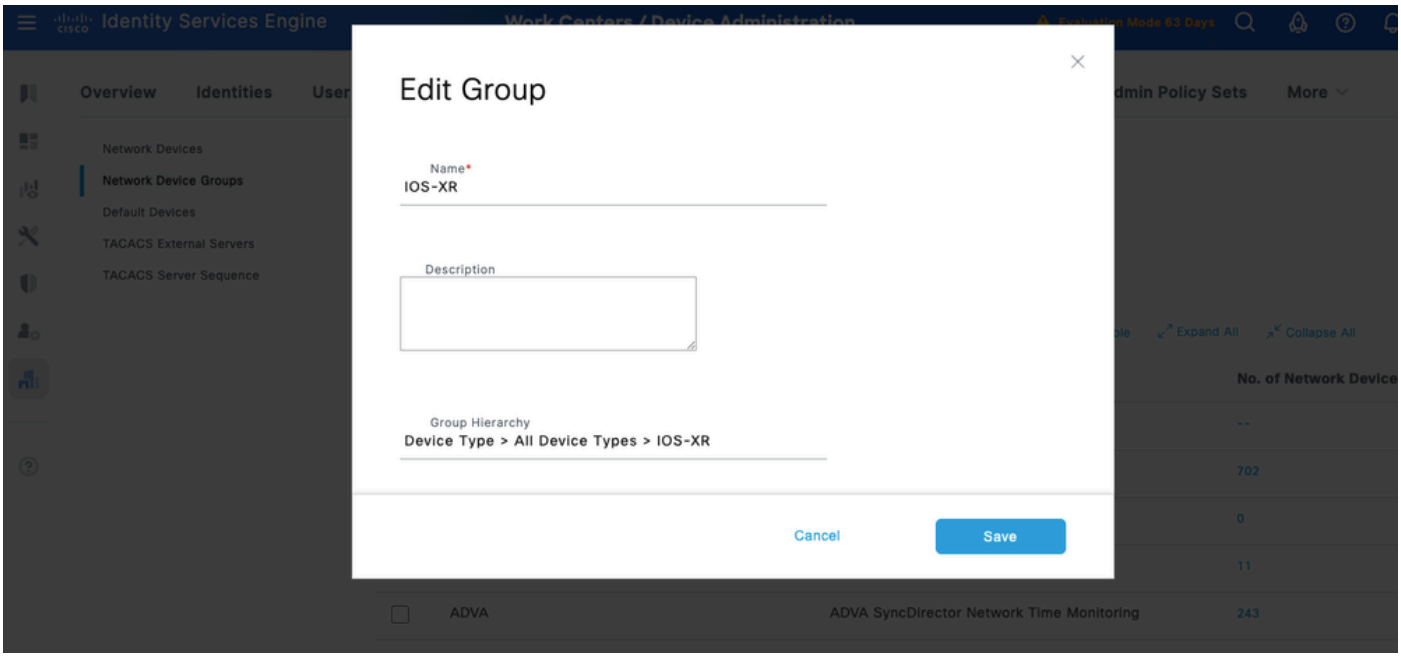


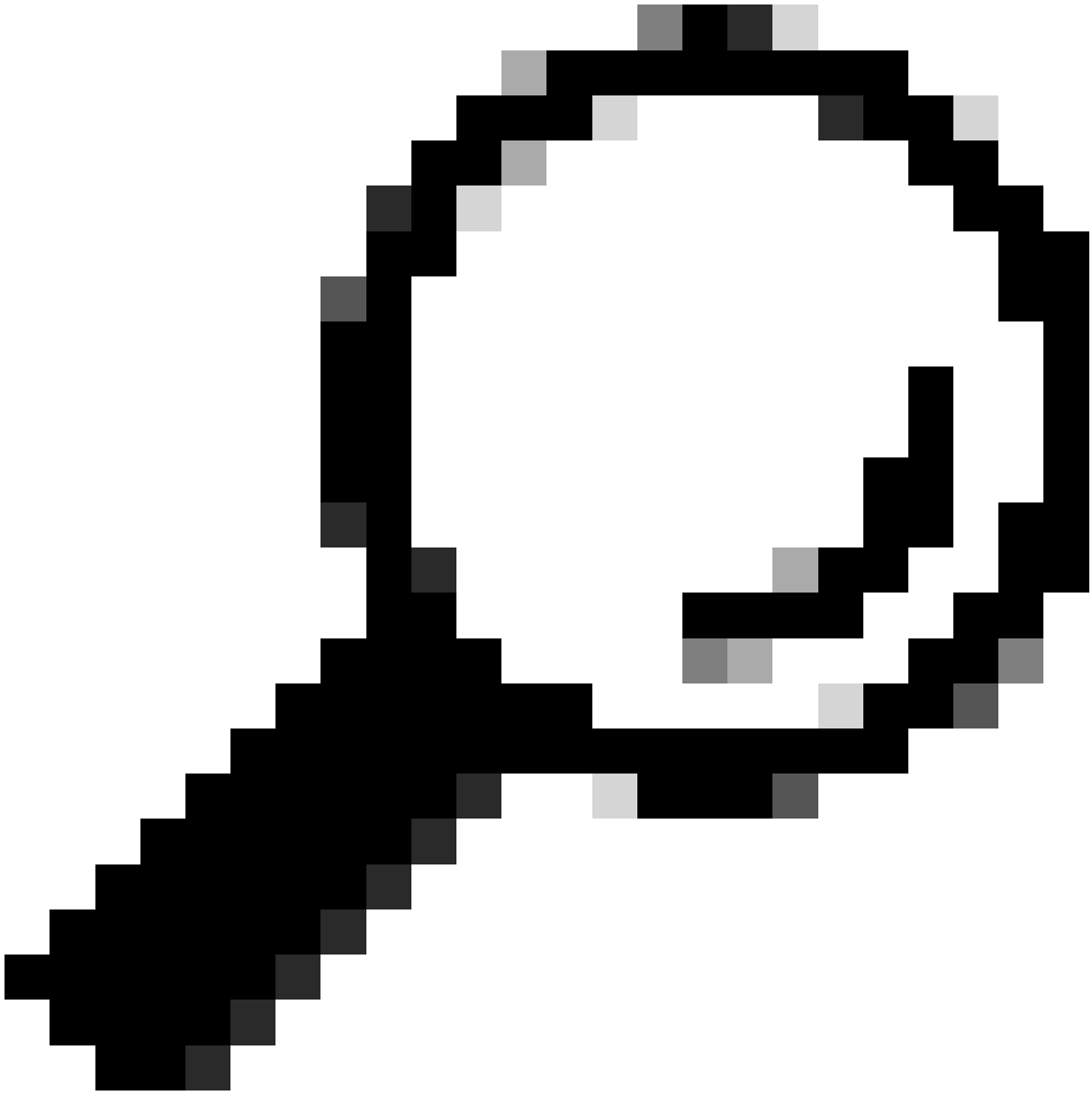
ステップ3：デフォルトのポート6049をそのまま使用するか、TACACS over TLSに別のTCPポートを指定して、Saveをクリックします。

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の作成

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。

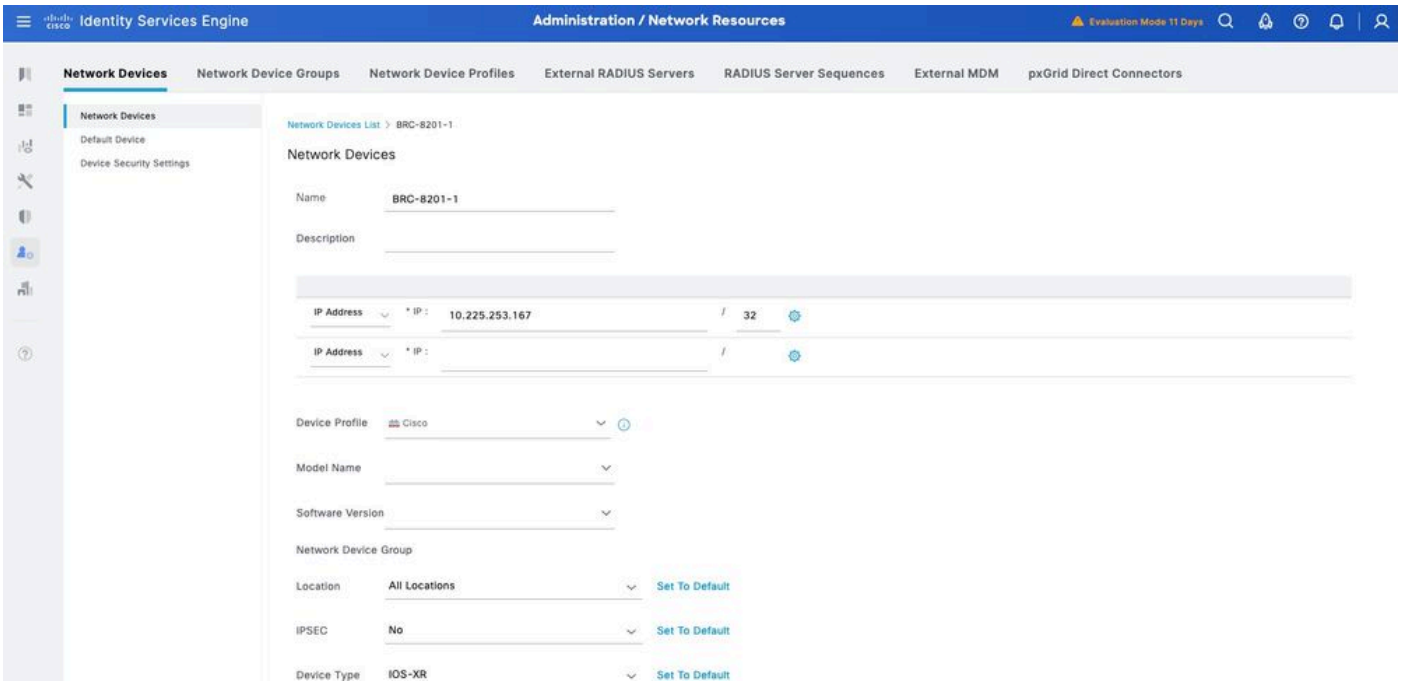
ステップ1:Work Centers > Device Administration > Network Resourcesの順に移動します。Network Device Groups をクリックし、IOS XRという名前でグループを作成します。


Identity Services Engine
Work Centers / Device Administration
Overview
Identities
User
Admin Policy Sets
More
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Expand All
Collapse All
No. of Network Device
Edit Group
Name*
IOS-XR
Description
Group Hierarchy
Device Type > All Device Types > IOS-XR
Cancel
Save
ADVA
ADVA SyncDirector Network Time Monitoring
243

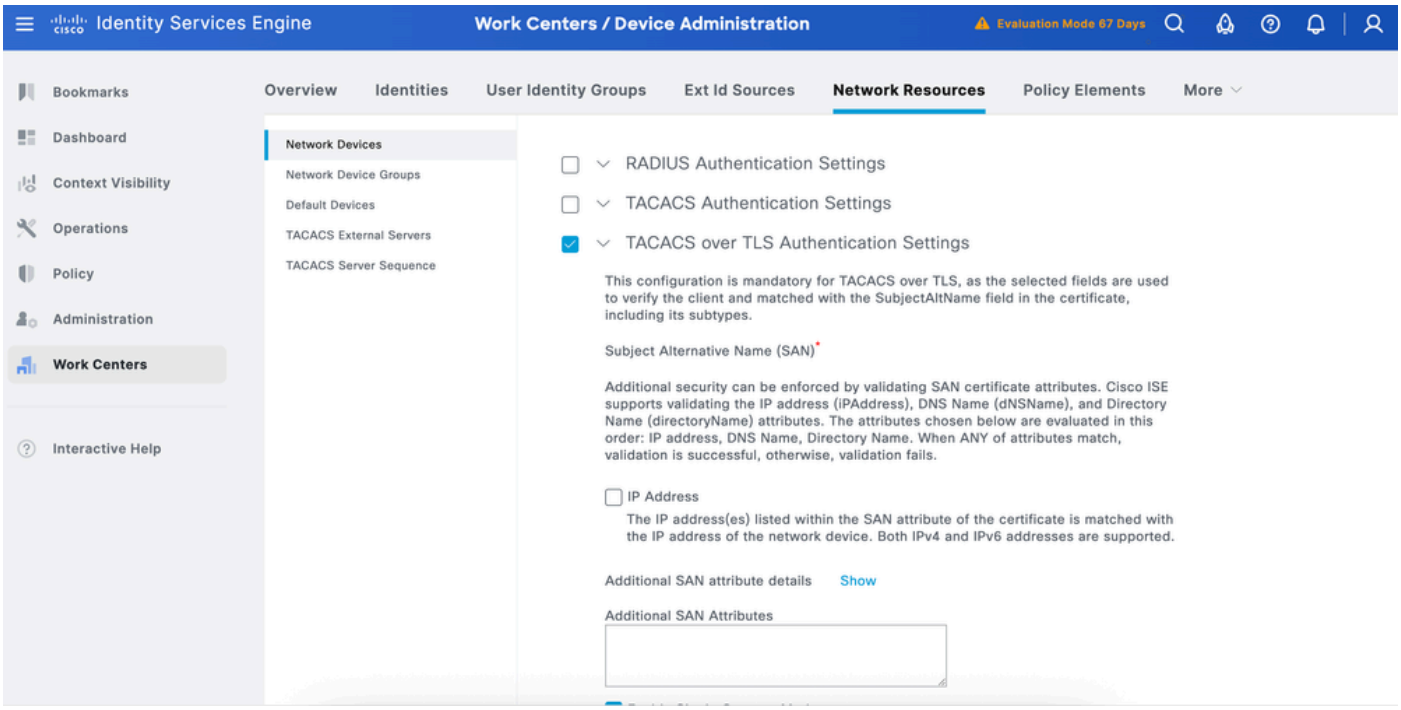


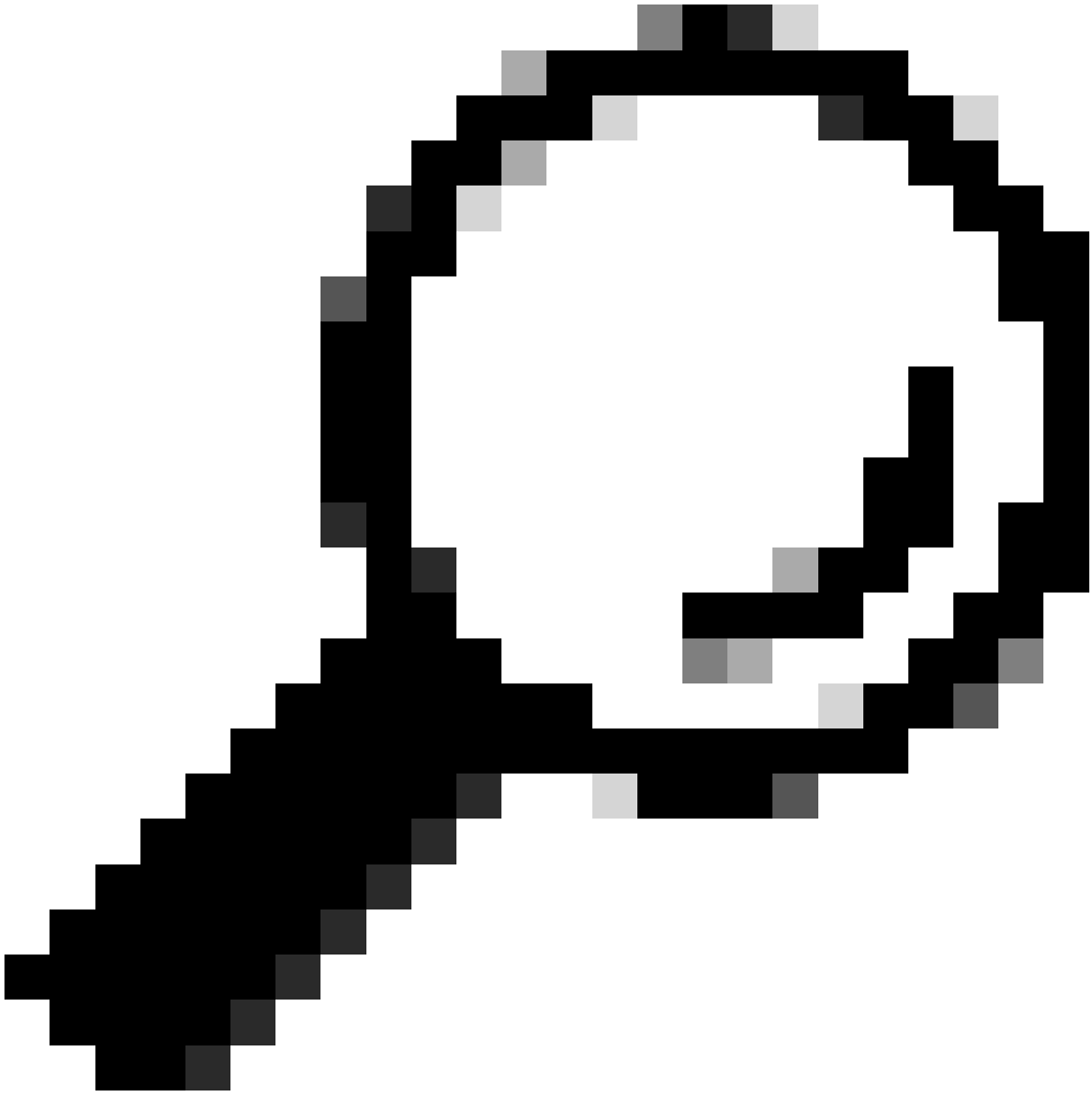
ヒント：すべてのデバイスタイプとすべての口ケーションは、ISEが提供するデフォルトの階層です。独自の階層を追加し、ポリシー条件で後から使用できるネットワークデバイスの識別でさまざまなコンポーネントを定義できます

ステップ 2： 次に、Cisco IOS XR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] > [Network Devices] 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(IOS XR)を必ずマッピングします。最後に、TACACS+ over TLS認証設定を有効にします。



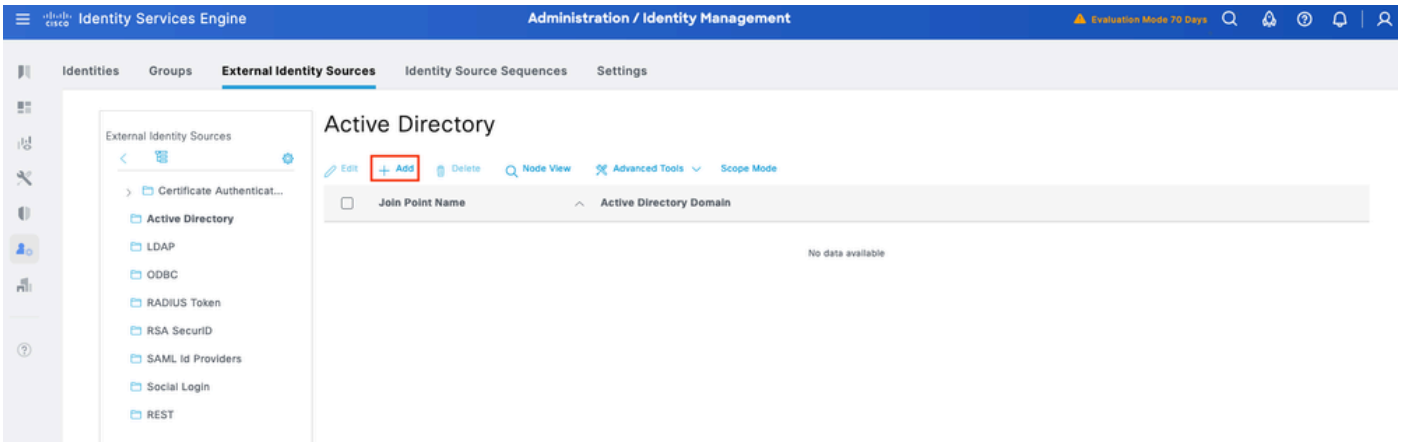


ヒント：デバイスにコマンドが送信されるたびにTCPセッションが再起動しないように、シングルコネクトモードを有効にすることを推奨します。

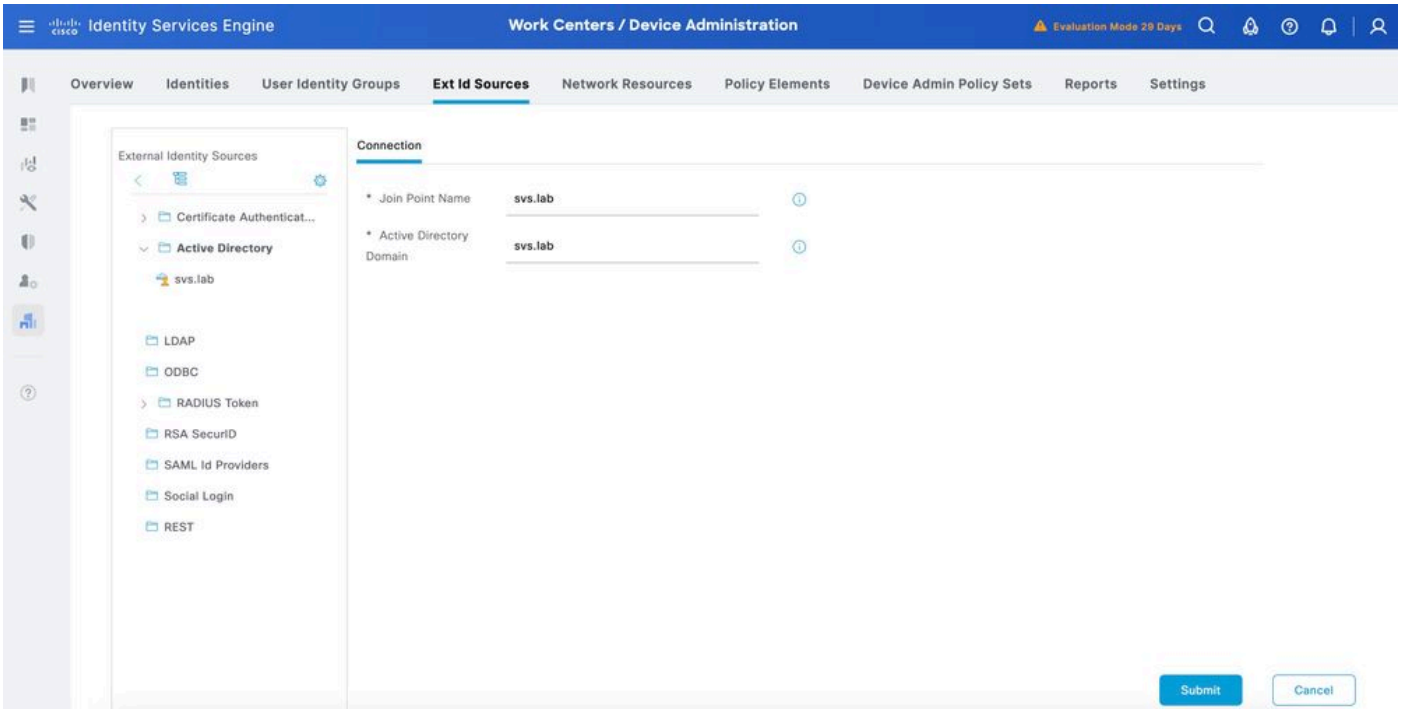
アイデンティティストアの設定

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。

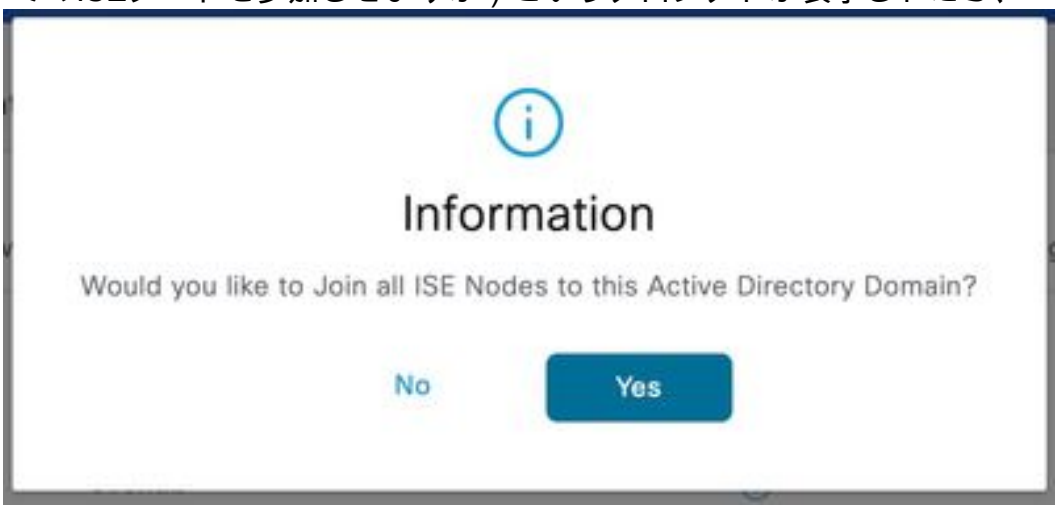
ステップ 1： Administration > Identity Management > External Identity Stores > Active Directoryの順に移動します。Addをクリックして、新しいADジョイントポイントを定義します。



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。

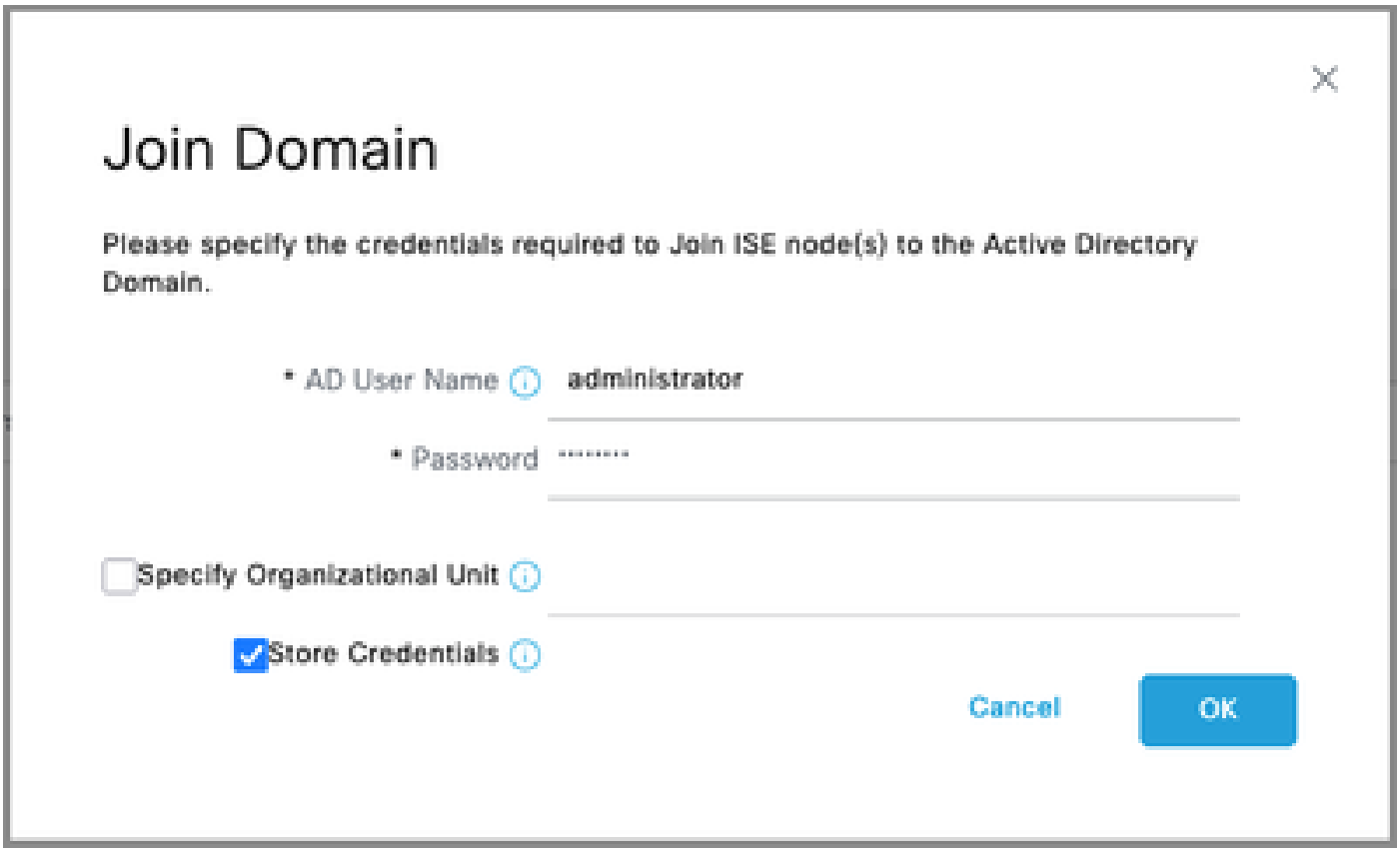


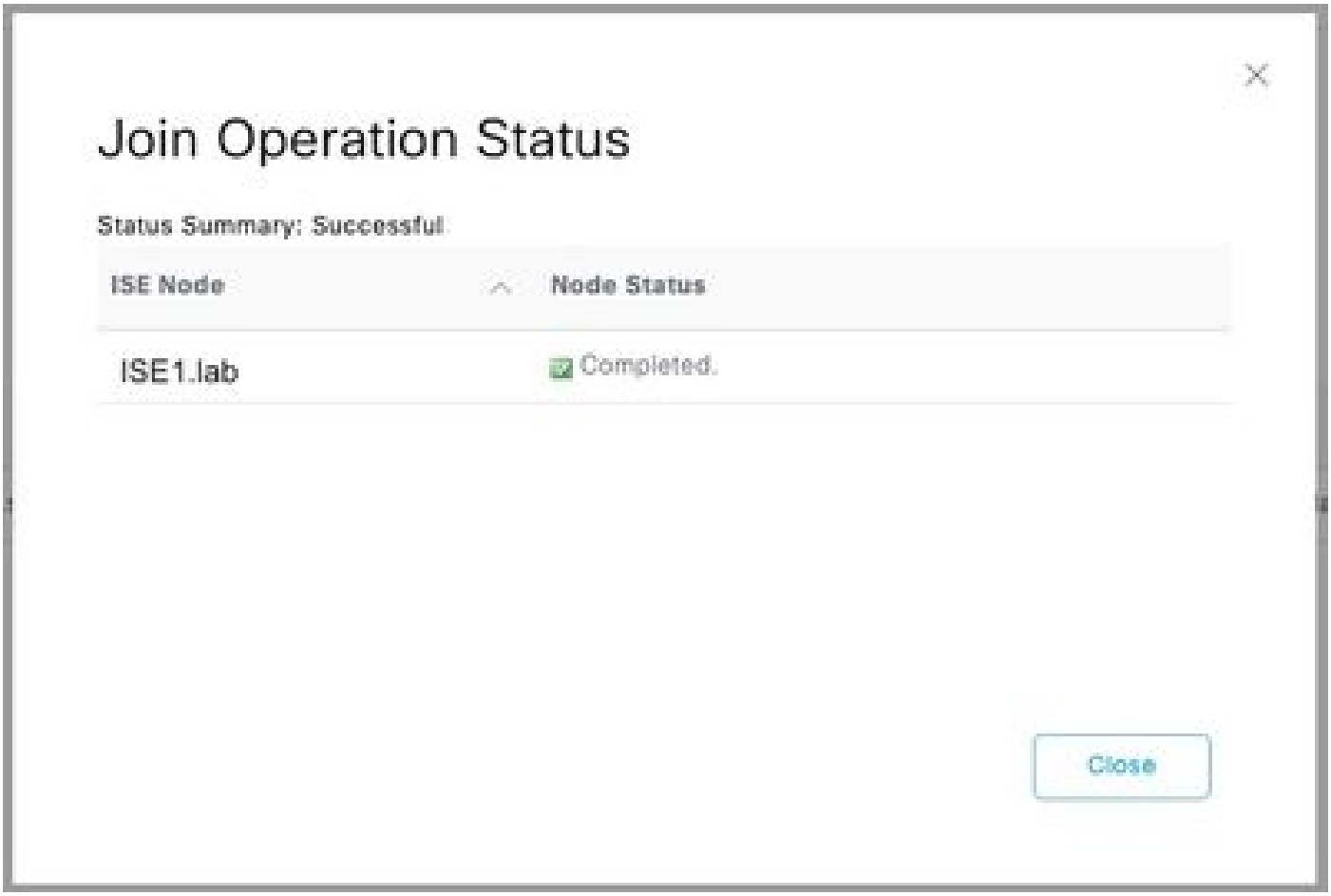
ステップ3:Would you like to Join all ISE Nodes to this Active Directory Domain?（このActive Directoryドメインにすべてのノードを参加させますか）というプロンプトが表示されたら、Yesをクリックします。



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

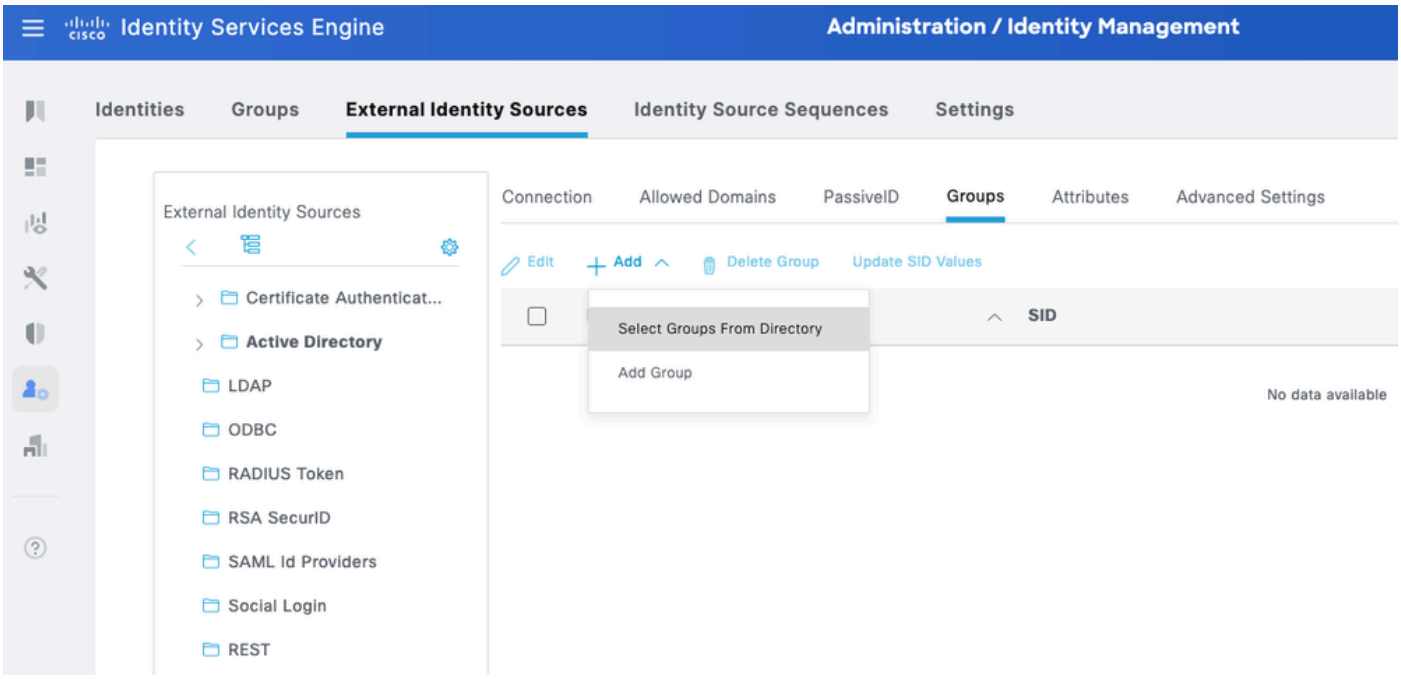
チェックして、動作していることを確認します。

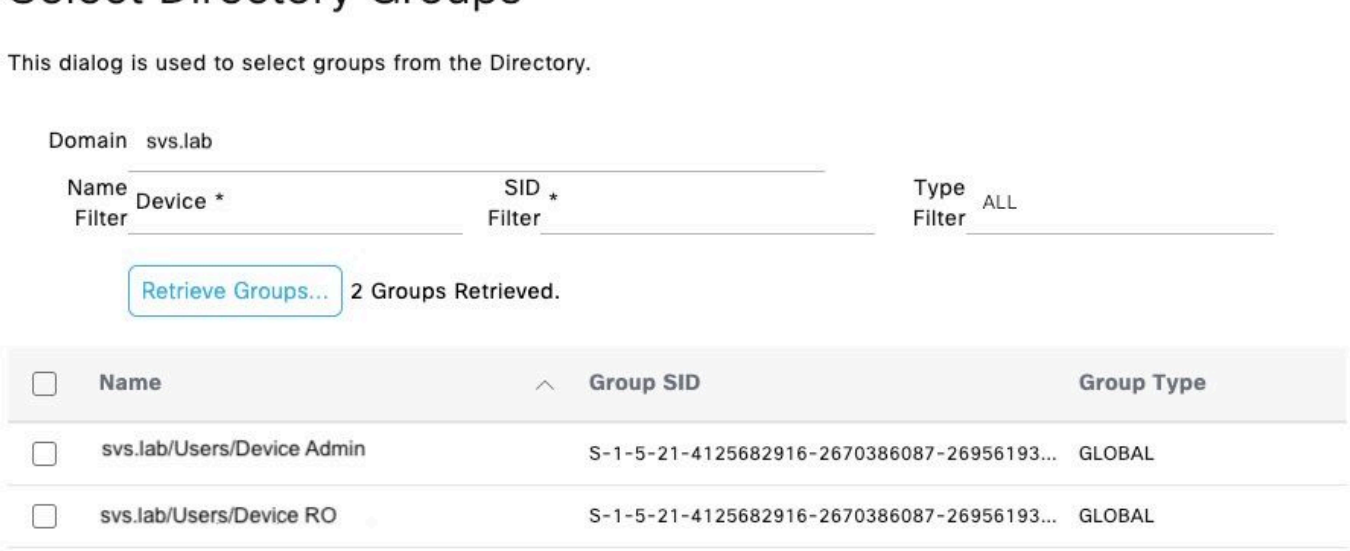


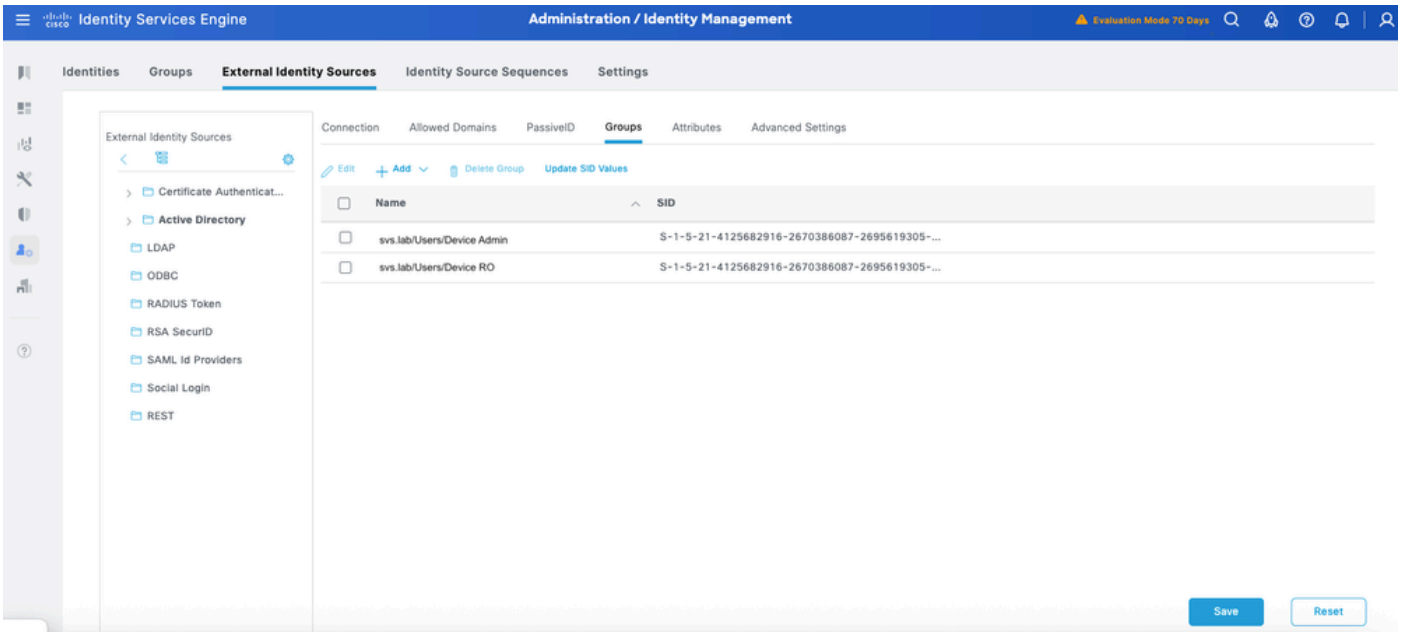


ステップ5:Groupsタブに移動し、Addをクリックして、ユーザにデバイスアクセスの権限を付与

したユーザに基づいて、必要なすべてのグループを取得します。次の例は、認可ポリシーで使用されるグループを示しています。







TACACS+プロファイルの設定

TACACS+プロファイルをCisco IOS XRデバイスのユーザロールにマッピングします。この例では、次のように定義されています。

- ルートシステム管理者 – これは、デバイス内で最も高い権限を持つロールです。root system管理者の役割を持つユーザーは、すべてのシステムコマンドと構成機能に対する完全な管理アクセス権を持ちます。
- オペレータ：このロールは、監視およびトラブルシューティングのためにシステムへの読み取り専用アクセスを必要とするユーザを対象としています。

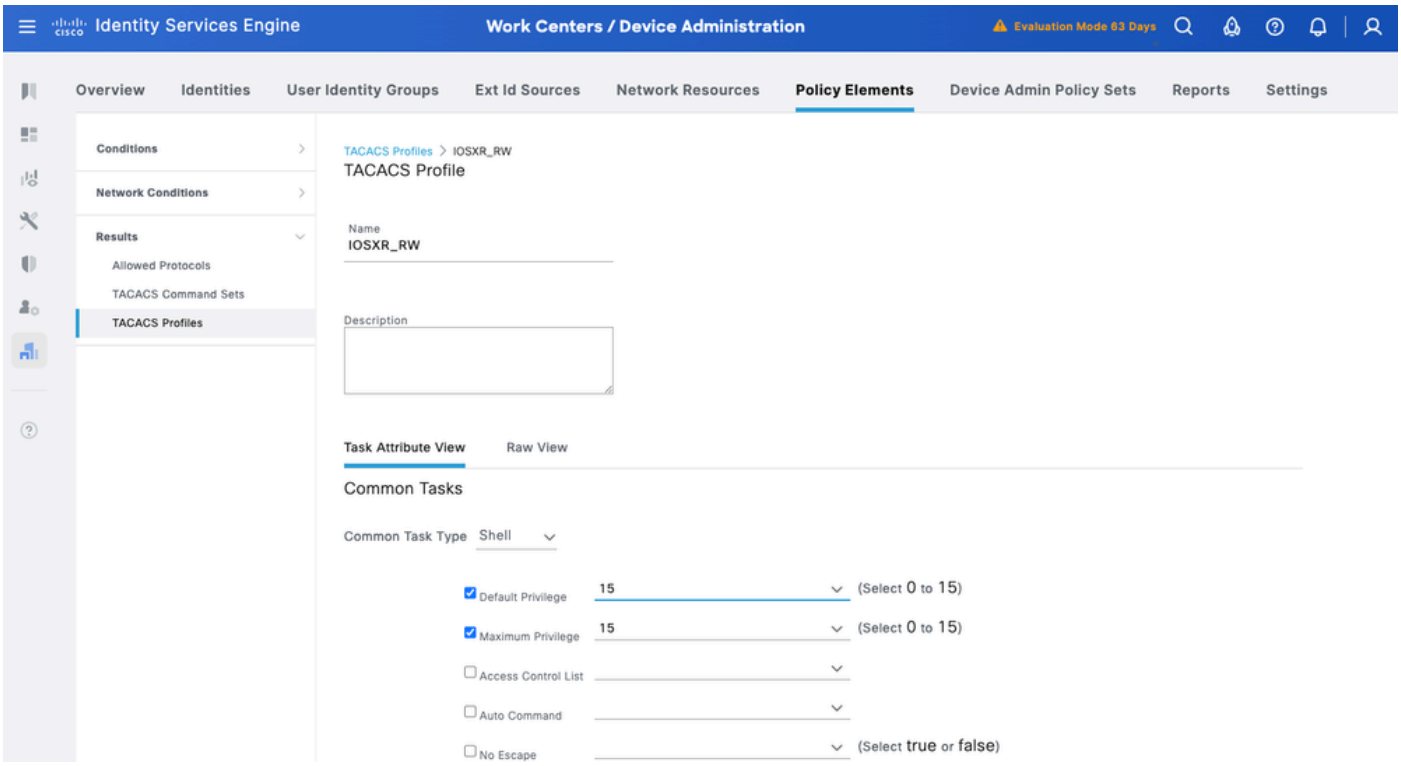
IOSXR_RWとIOSXR_ROの2つのTACACS+プロファイルを定義します。

IOS XR_RW – 管理者プロファイル

ステップ 1：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、IOSXR_RWという名前を付けます。

ステップ 2： デフォルト権限と最大権限を15に設定します。

ステップ 3： 設定を確認して保存します。

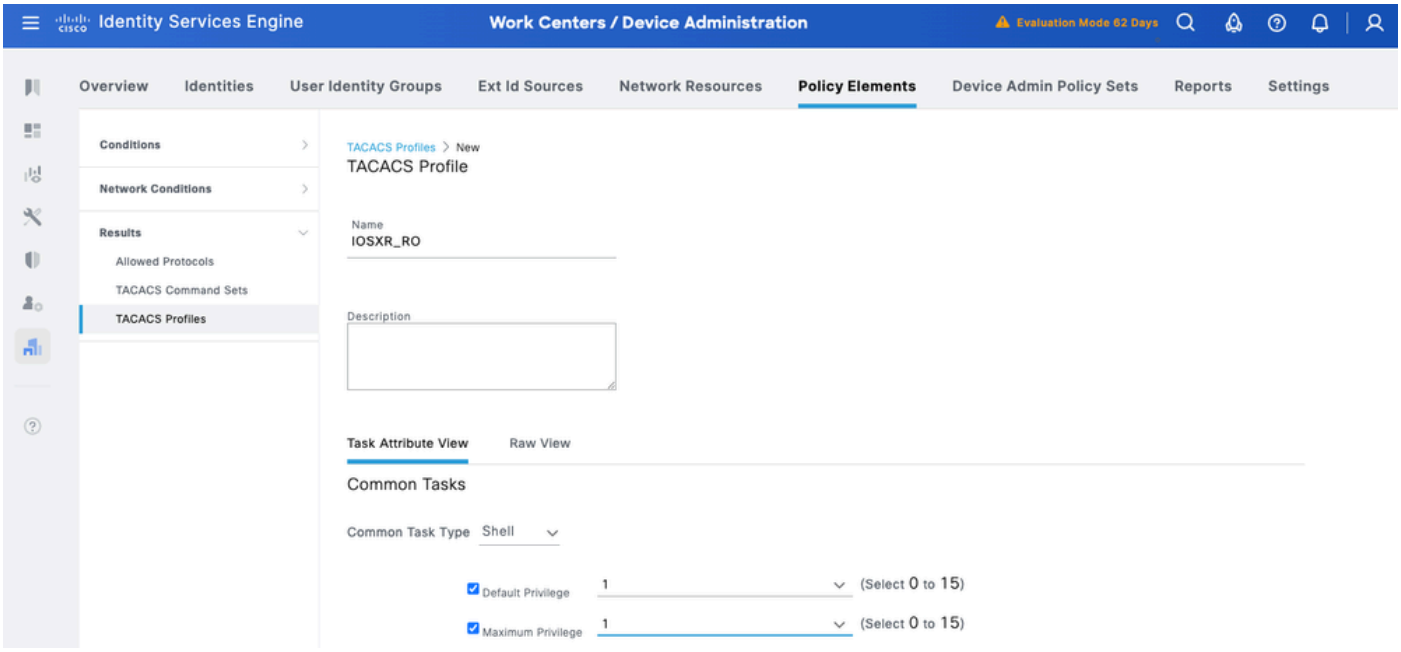


IOS XR_RO – オペレータプロファイル

ステップ 1：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、IOSXR_ROという名前を付けます。

ステップ 2： デフォルト権限と最大権限を1に設定します。

ステップ3：設定を確認し、保存します。



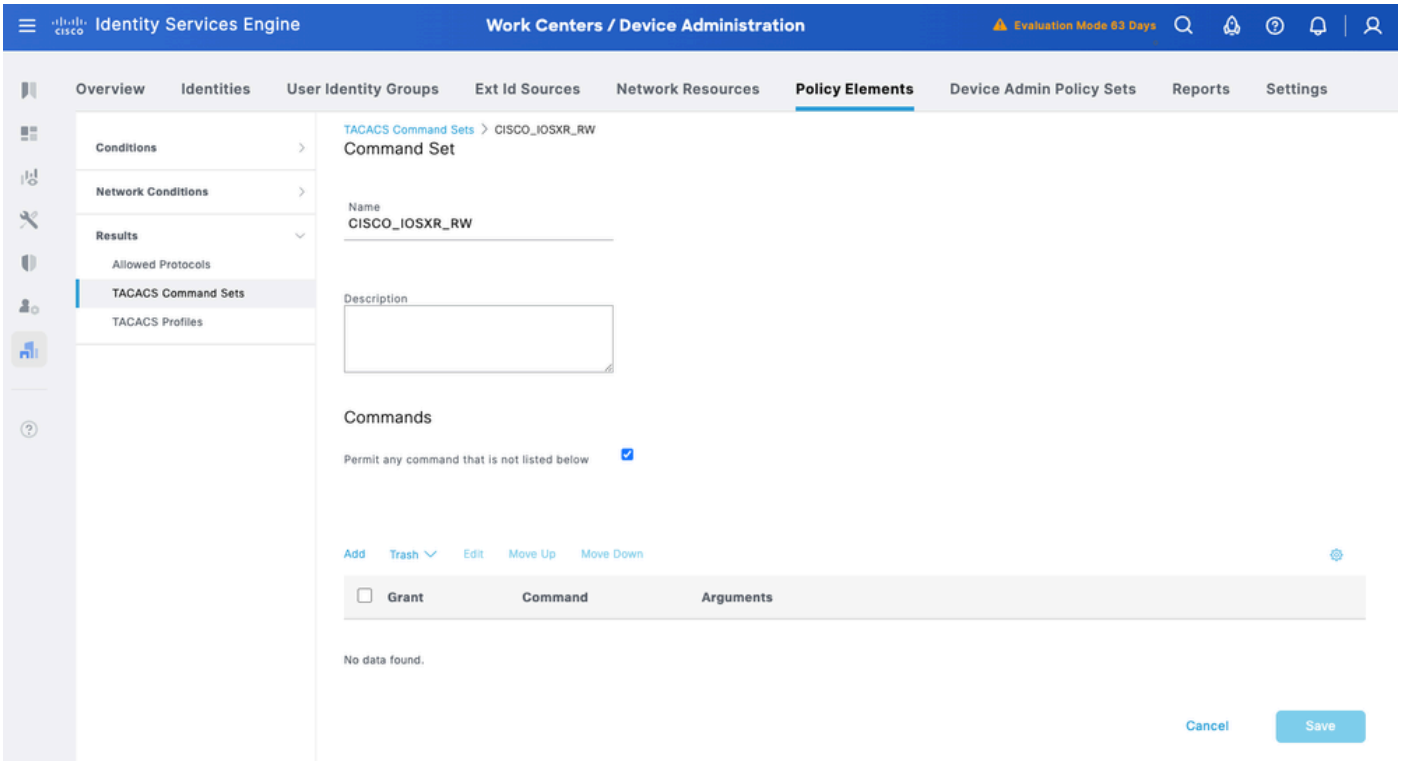
ConfigureTACACS+コマンドセット

TACACS+コマンドセットの定義：この例では、CISCO_IOSXR_RWおよびCISCO_IOSXR_ROが定義されています。

CISCO IOS XR RW：管理者コマンドセット

ステップ 1：Work Centers > Device Administration > Policy Elements > Results > TACACS Command Setsの順に移動します。 新しいTACACSコマンドセットを追加し、CISCO_IOSXR_RWという名前を付けます。

ステップ 2： Permit any command that is not listed belowチェックボックスにチェックマークを付け（これにより、管理者ロールのすべてのコマンドが許可されます）、Saveをクリックします。



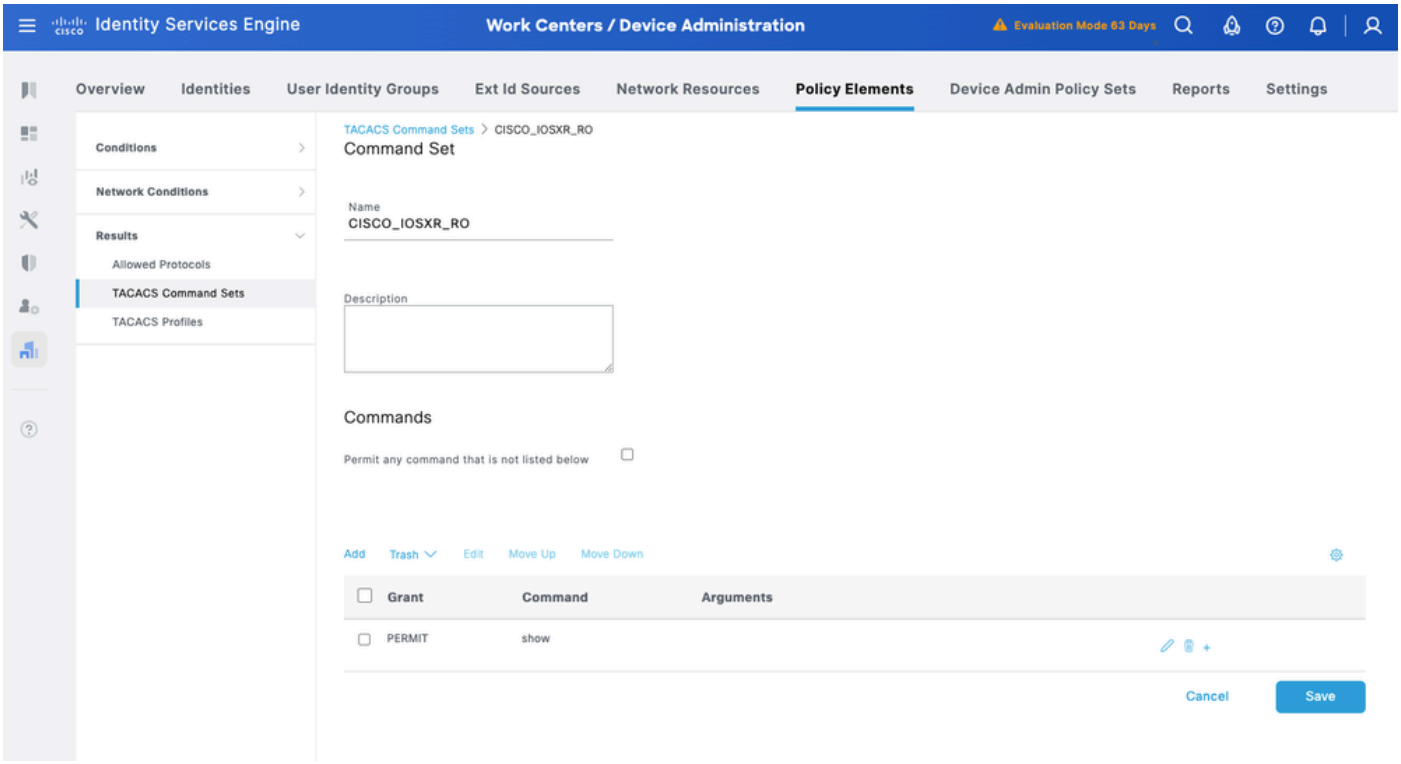
CISCO IOS XR RO：オペレータコマンドセット

ステップ 1： ISE UIから、Work Centers > Device Administration > Policy Elements > Results > TACACS Command Setsの順に移動します。 新しいTACACSコマンドセットを追加し、CISCO_IOSXR_ROという名前を付けます。

ステップ 2： コマンドセクションに、新しいコマンドを追加します。

ステップ 3： ドロップダウンリストからGrant 列のPermitを選択し、Command 列にshow と入力し、チェック矢印をクリックします。

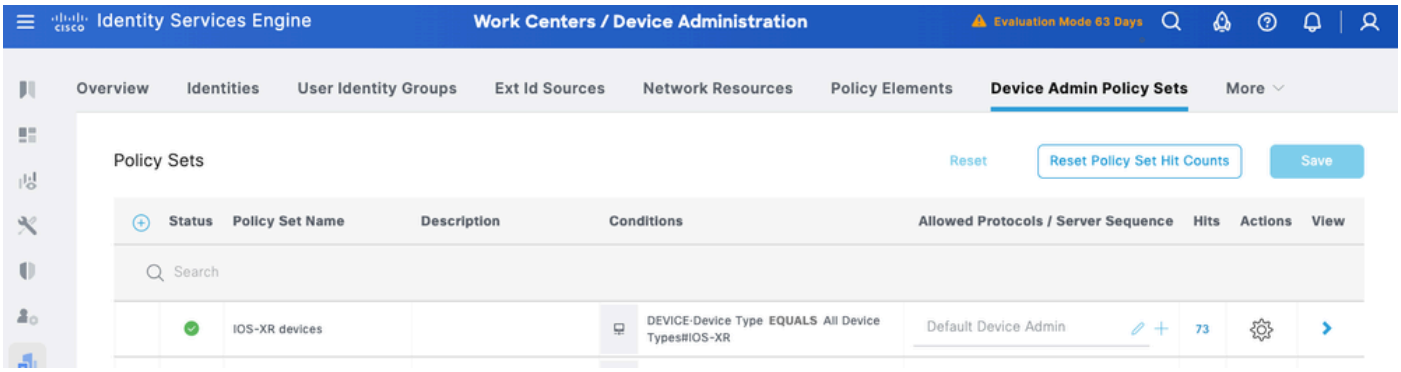
ステップ 4： データを確認して、保存をクリックします。



デバイス管理ポリシーセットの設定

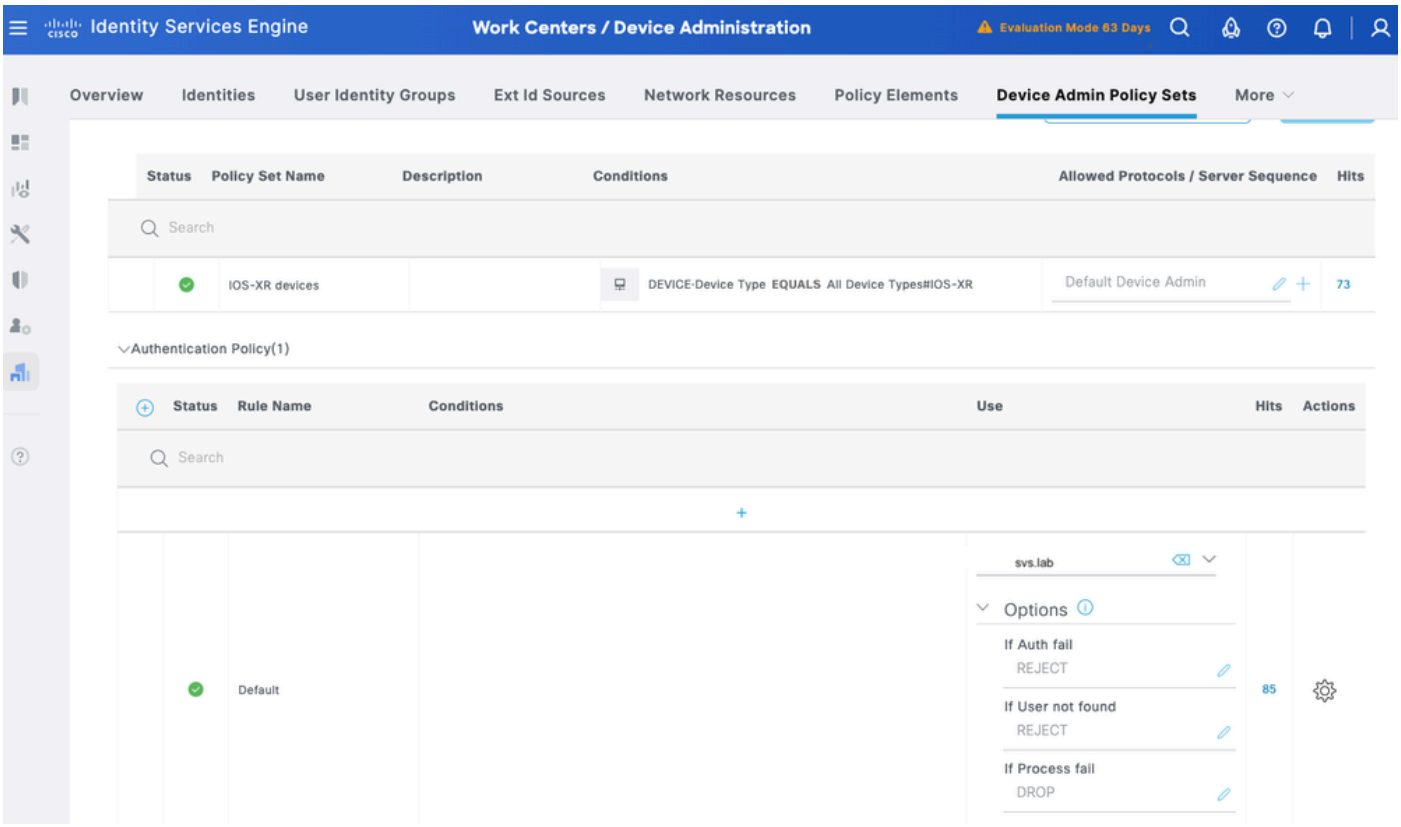
デバイス管理では、ポリシーセットはデフォルトで有効になっています。ポリシーセットは、デバイスタイプに基づいてポリシーを分割できるため、TACACSプロファイルの適用が容易になります。

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IOS XRデバイスを追加します。条件でDEVICE:Device Type EQUALS All Device Types#IOS XR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： このポリシーセットを設定するには、Saveをクリックし、右矢印をクリックします。

ステップ 3： 認証ポリシーを作成します。認証用に、ID StoreとしてADを使用します。If Auth fail, If User not foundIf process failの下にデフォルトオプションのままにします。

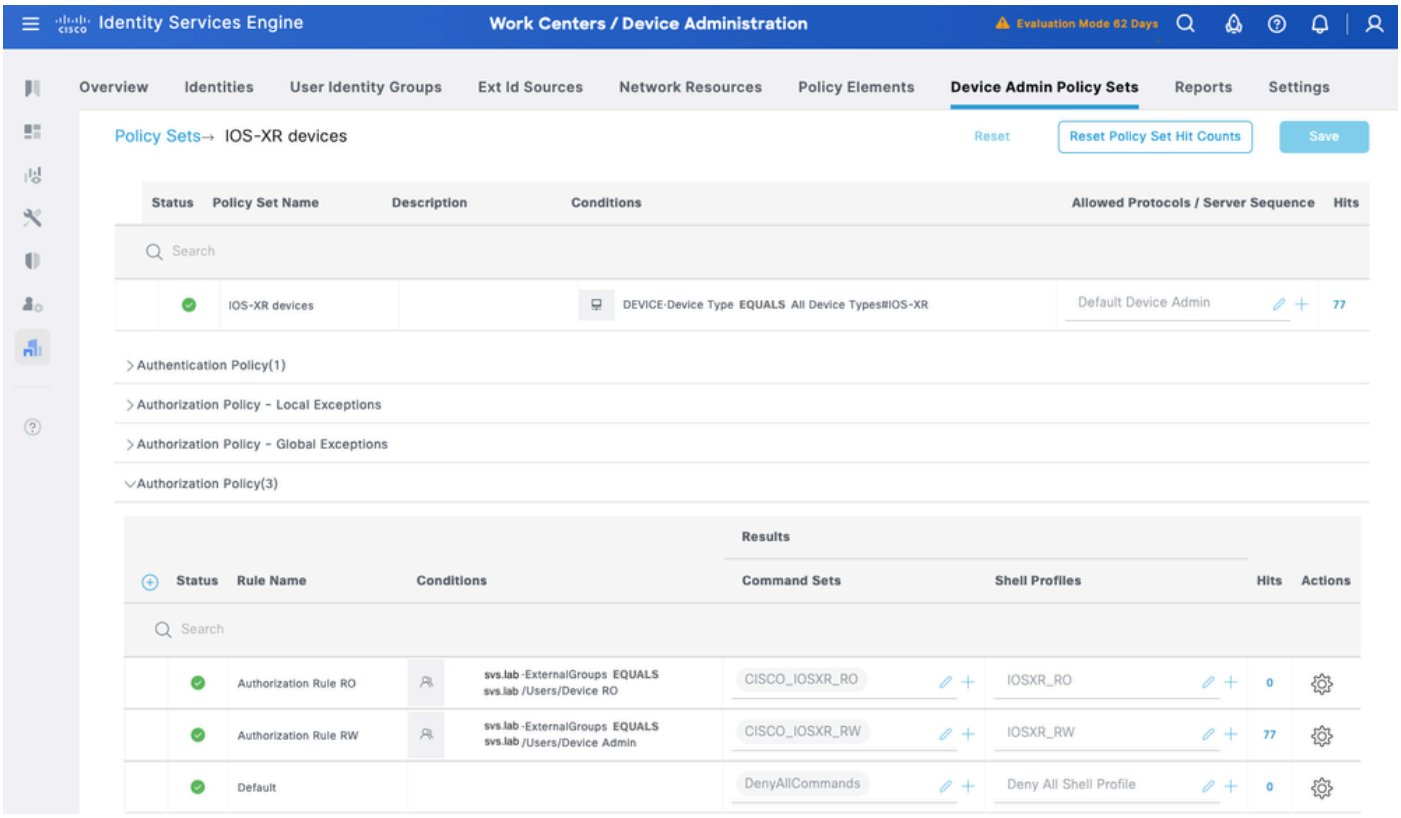


ステップ 4： 許可ポリシーを定義します。

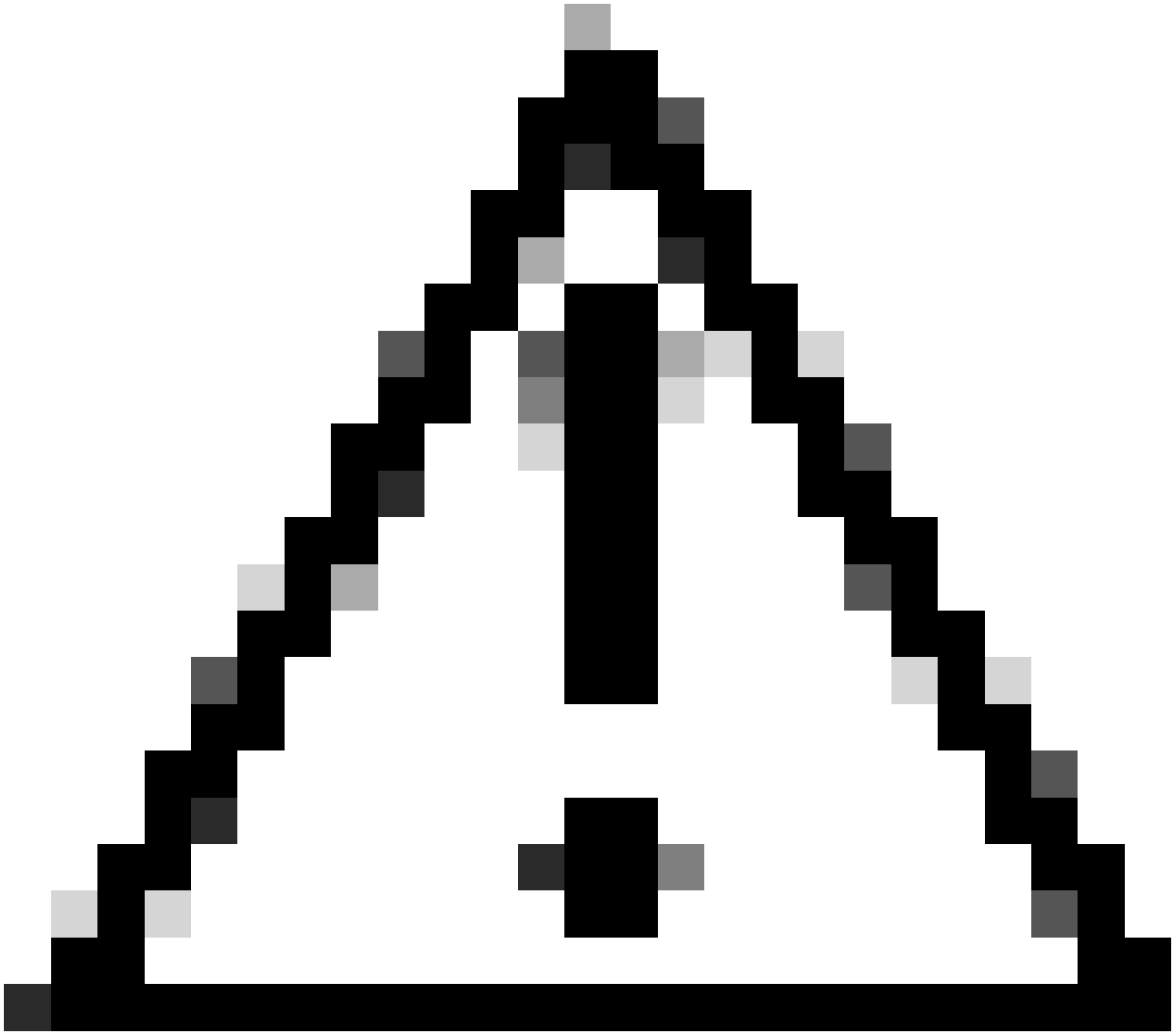
Active Directory(AD)のユーザグループに基づいて認可ポリシーを作成します。

例：

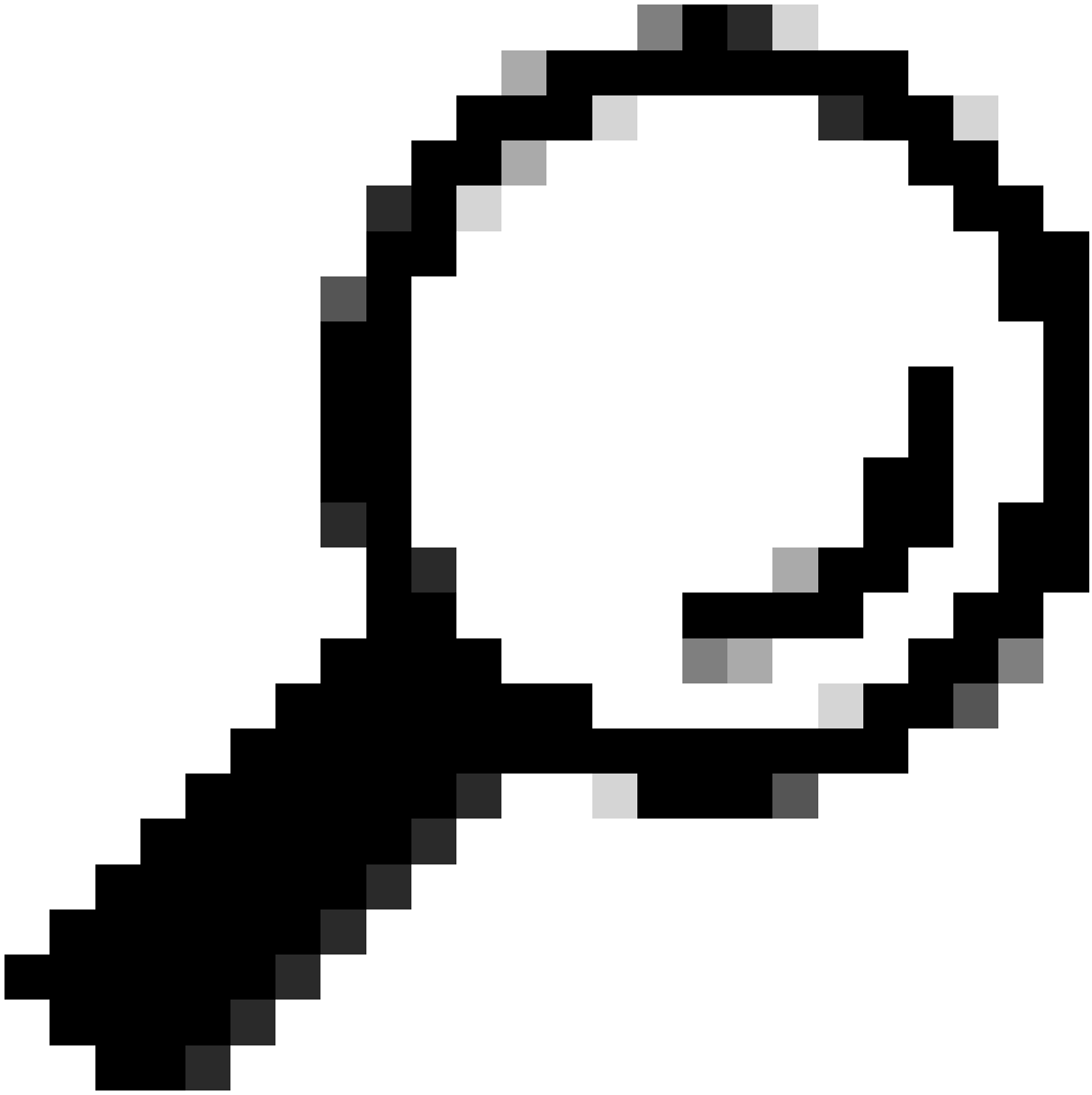
- ADグループDevice ROのユーザには、CISCO_IOSXR_RO コマンドセットとIOSXR_RO シェルプロファイルが割り当てられます。
- ADグループDevice Admin のユーザには、CISCO_IOSXR_RW コマンドセットとIOSXR_RW シェルプロファイルが割り当てられます。



パート2:TACACS+ over TLS 1.3用のCisco IOS XR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。

初期設定

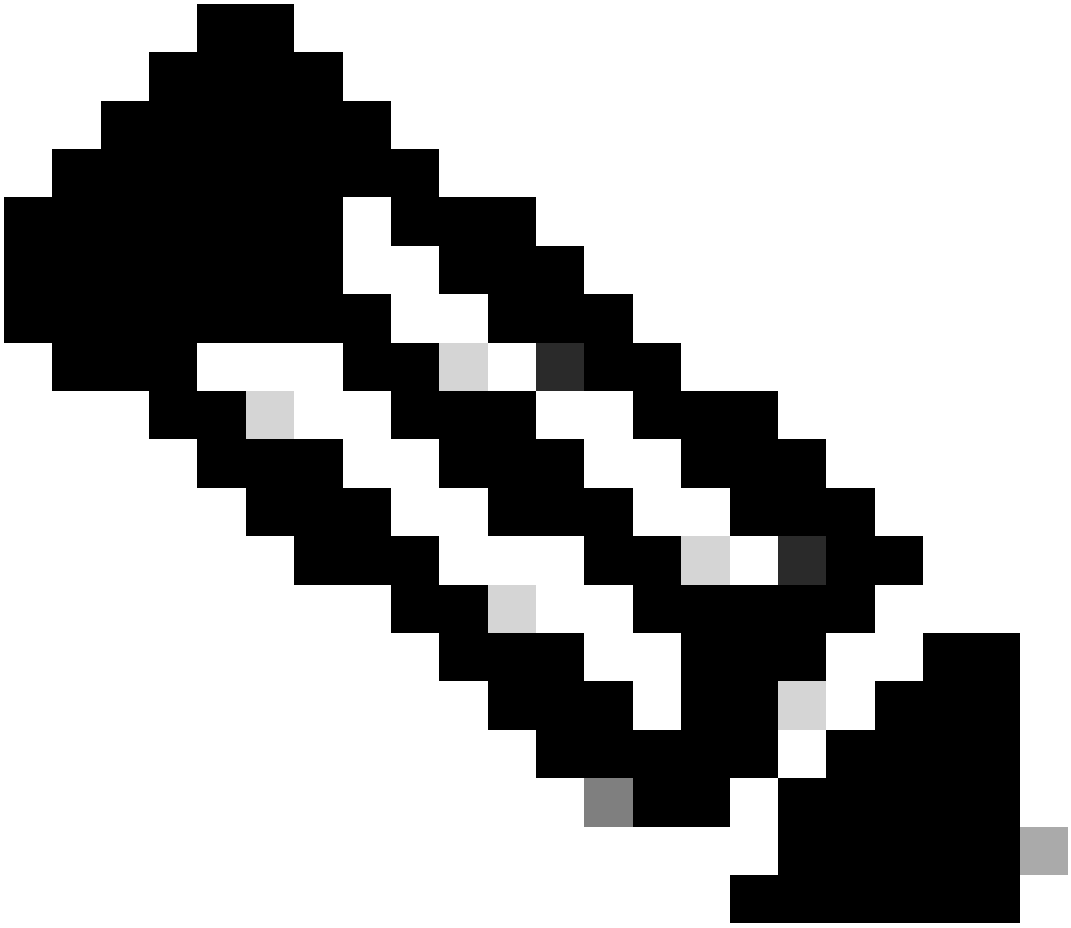
ステップ 1： name-server(DNS)が設定されており、ルータがFrequently Qualified Domain Name（FQDN；高頻度ドメイン名）を正常に解決できることを確認します。特に、ISEサーバのFQDNが有効であることを確認します。

```
domain vrf mgmt name svs.lab
domain vrf mgmt name-server 10.225.253.247
no domain vrf mgmt lookup disable
```

```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

ステップ 2： 古い/未使用のトラストポイントと証明書をすべてクリアします。 古いトラストポイントと証明書が存在していないことを確認します。古いエントリが表示された場合は、その エントリを削除またはクリアします。

```
show crypto ca trustpoint
show crypto ca certificates

(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



注：新しいRSAキーペアを手動で作成し、トラストポイントに添付できます。キーペアを作成しない場合は、デフォルトのキーペアが使用されます。トラストポイントでのECCキーペアの定義は、現在サポートされていません。

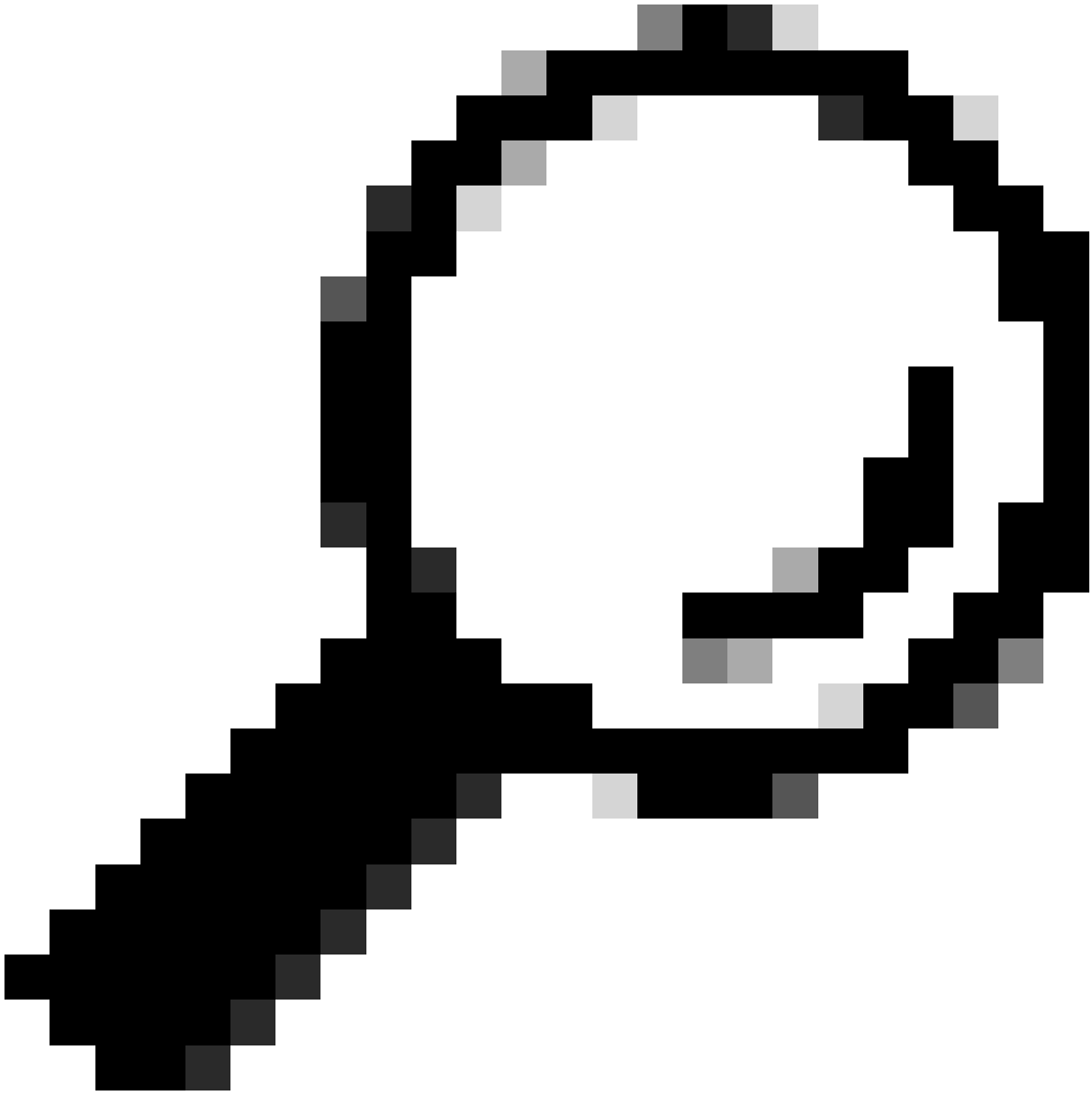
トラストポイントの設定

ステップ 1：キーペア設定（オプション）。

```
<#root>

RP/0/RP0/CPU0:BRC-8201-1(config)#

crypto key generate rsa

          4096
```

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint


RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair
```

ステップ 2：トラストポイントを作成します。

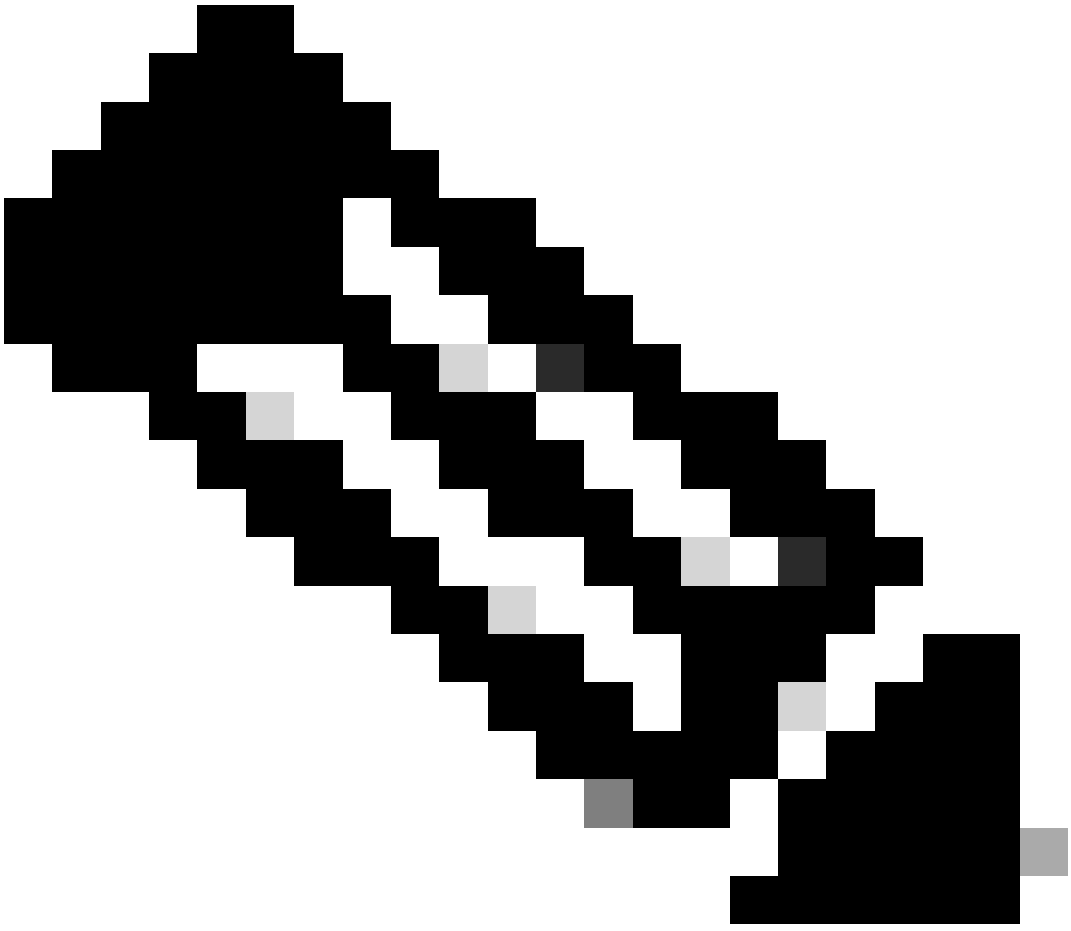


ヒント：サブジェクト代替名(SAN)のDNS設定はオプションですが（ISEで有効になっている場合）、設定することをお勧めします。

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint svs

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
vrf mgmt

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
crl optional
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
enrollment url terminal
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair svs-4096

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
commit
```



注:OまたはOUでカンマを使用する必要がある場合は、カンマの前にバックスラッシュ(\)を付けることができます。例：O=Cisco Systems\, Inc.

ステップ 3： CA証明書をインストールしてトラストポイントを認証します。

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca authenticate svs

```
Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
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
xDrmo7e0XPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

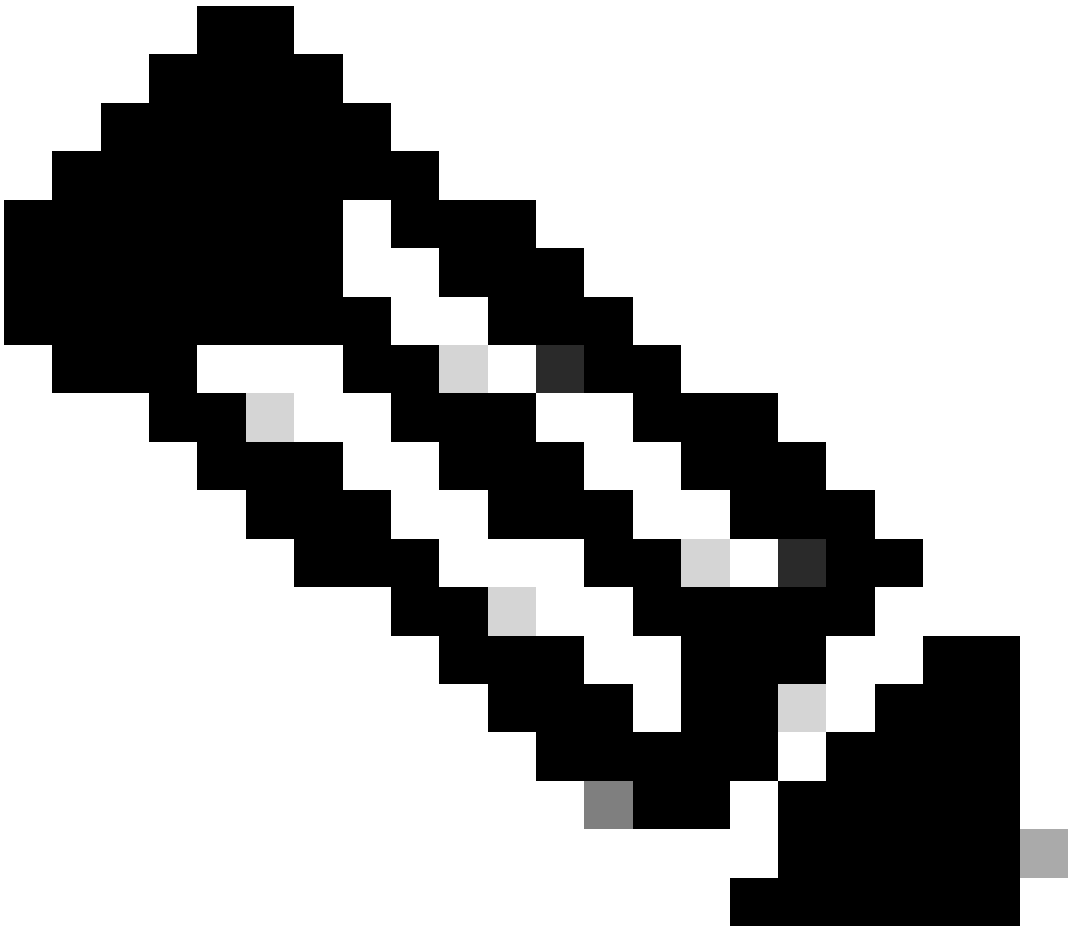
quit

```
   Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5
   Subject:
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
   Issued By :
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
   Validity Start : 17:05:00 UTC Mon Apr 28 2025
   Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
   SHA1 Fingerprint:
      0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
```

yes

```
RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated
```



注：下位CAシステムがある場合は、ルートCA証明書と下位CA証明書の両方をインポートする必要があります。同じコマンドを、上に下位CA、下にルートCAを指定して使用します。

ステップ 4： 証明書署名要求(CSR)を生成します。

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca enroll svs

```
Fri May 9 14:52:44.030 UTC
% Start certificate enrollment ...
% 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:

Re-enter Password:

```
% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167
% The subject name in the certificate will include: BRC-8201-1.svs.lab
% Include the router serial number in the subject name? [yes/no]:
```

yes

```
% The serial number in the certificate will be: 4090843b
% Include an IP address in the subject name? [yes/no]:
```

yes

```
Enter IP Address[]
```

10.225.253.167

```
Fingerprint: 36354532 38324335 43434136 42333545
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANTVlMxFzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQclZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaiMGqETnO0LKpwmtx10IqXL7UYMHHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkWkwI0cb1X2HgtbVQdCXTAwJDmr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAaCBiTAYBgkqhkiG
9w0BCQcxCxMJQzFzY28uMTIzMG0GCSqGSIb3DQEJDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBBXOeWF5ZUz7O1GFjuQHBBDgYb+3lhFOxbYm9psIWfv1uwjkKoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswjlYpO+IxkUM971Ejwg2rj+jABDR7I8SU
O6YO6mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTIljdgVxB+XyzOFJMckIO5US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f9OA+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4lizO5Zj2NJbUKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZNOO
```

```
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

ステップ 5： CA署名付き証明書をインポートします。

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca import svs certificate

```
Fri May 9 15:00:35.426 UTC

Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA5MTQ1NzAwWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEOMAwGA1UECgwFQ2lzY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOdO2uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7ispmoBnXEOGJ
qIwaoROc7QsqnCa3HXQipcvtRgwcfAX29EgjnbOiaRYDxrrdbHrpSQTFpeh5dp/k
eQuioO7rxfzdTss+8x7WwzC+artGbLYMC7fQcH8l9iVAIeZNUXPczl8G3zrHHi3W
fFMVT/iVFYwLvdROvlhOokuMykFPaOOTemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTAjRxvVfYeC1tVBOJdMDAkOavY73N3ZkJrl6dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJOaWZpY2F0
ZTAOBgNVHQ8BAf8EBAMCBaAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMAkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjI1LjI1My4xNjeHBArh/acw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+ojO121O6WxedDQ8VduObBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8YOO7HR/2jf7gfhoRvwcR5QNOEHv4o6l
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV8lRGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr5lM4Ysvoltx1k9AeLjzb2syv5/fG6QuOZdWwTaaQhOY2h/cVDiV97wg
ODlmEfdSv6QrxQSujZr22RzVyKKHltuiV2B74pthUuGRBtfHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDplrf1ZIrPmv3ZPP7woTB22yWzydOuse+5IalbOw7OtwN4t/IIw
8CJu6HfnDXLDPZOjsC8steffrSlopwGccp3j6aZKPFz+I/Purb44a9WxEWa2TA7H
+rloynBcGMetOHxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF537Ow+uNHoK8Bdt8mqadUT4OoUSqY8ArVOBomO5tzbemreVPmQAZ/IahZ7TqKo
3dGNonTAfFTESM1iujQ81iRKsikDHySnwcCM2nilCKZrhVq5IB8NK6jKRJZOeQAX
vMt1
-----END CERTIFICATE-----
```

quit

```
Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792
```

ルータID証明書が登録されていることを確認します。

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

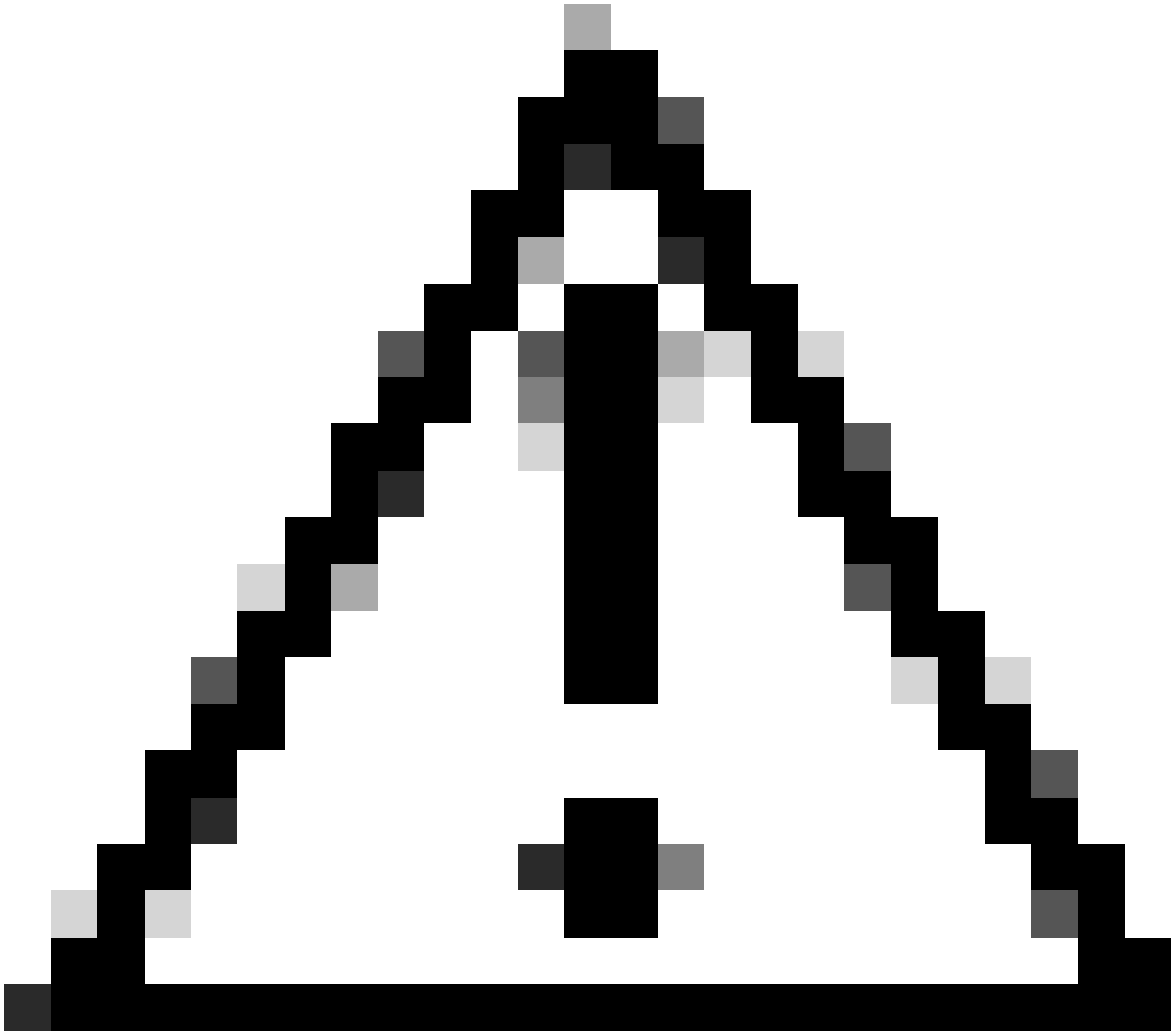
show crypto ca trustpoint svs detail

```
Trustpoint        :svs-new
================================================================
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1#
```

show crypto ca certificates svs

```
Wed May 14 14:55:58.173 UTC

Trustpoint       : svs-new
================================================
CA certificate
  Serial Number  : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
         0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
        serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
         AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs
```

TLSを使用したTACACSおよびAAAの設定



注意：ローカルクレデンシャルを使用し、コンソール経由で設定変更を実行してください。

ステップ 1： TACACS+サーバを設定します。

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
  key 7 072C705F4D0648574453

aaa group server tacacs+ tacacs2
 server 10.225.253.209
 vrf mgmt
```

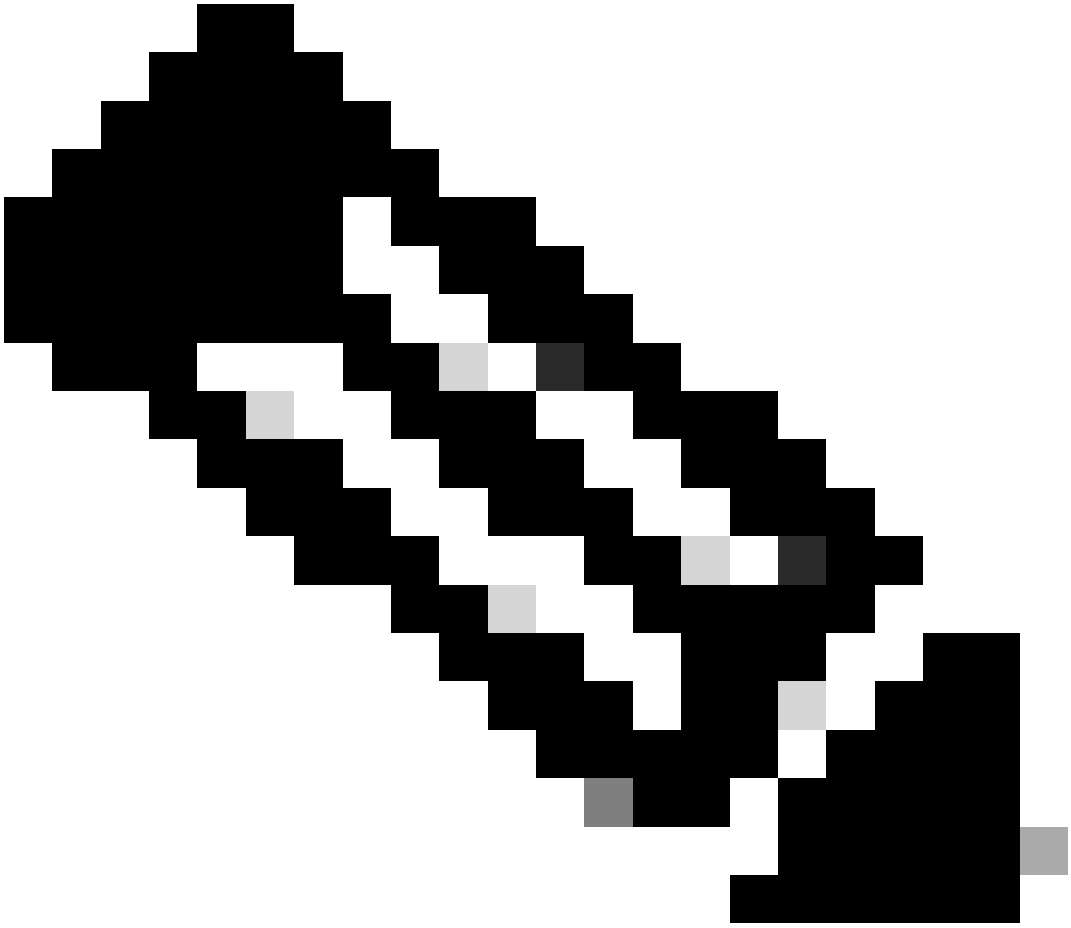
ステップ 2：AAAグループを設定します。

```
aaa group server tacacs+ tac_tls_sc
 vrf mgmt
 server-private 10.225.253.209 port 6049
  timeout 10
  tls
   trustpoint svs
  !
  single-connection
```

ステップ 2：AAA の設定.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

証明書の更新



注：更新中にTACACS+設定からトラストポイントを削除する必要はありません。

ステップ 1： 現在の証明書の有効期間を確認します。

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svs-new
Thu Aug 14 15:13:37.465 UTC

Trustpoint : svs-new
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point
```

```
http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5Gv0AZM

  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 16:38:36 UTC Wed Jul 30 2025
  Validity End : 16:38:35 UTC Thu Jul 30 2026
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svs-new
```

ステップ 2：既存のトラストポイント証明書を削除します。

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database update
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

ステップ 3：「トラストポイントの設定」の手順に従って、トラストポイントを再認証し、登録します。

ステップ 4： 証明書の有効期間が更新されていることを確認します。

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC

Trustpoint : KF_TP
================================================
```

```
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5Gv0AZM
  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 15:17:29 UTC Thu Aug 14 2025
  Validity End : 15:17:28 UTC Fri Aug 14 2026

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP
```

検証

設定を確認します。

```
show crypto ca certificates [detail]
show crypto ca trustpoint detail
show tacacs details
```

TACACS+のデバッグ

```
debug tacacs tls
```

TLSのデバッグ

```
debug ssl error
debug ssl events
```

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>

test aaa group tacacs2

```
user has been authenticated
```

トラブルシューティング

証明書を消去しています（信頼ポイントに関連付けられているすべての証明書が削除されます）。

```
clear crypto ca certificate <trustpoint name>
```

TACACSプロセスの再起動（必要な場合）

```
process restart tacacsd
```

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。