

ISEを使用したIOS XE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](#)

[パート1: デバイス管理用のConfigureISE](#)

[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の作成](#)

[アイデンティティストアの設定](#)

[TACACS+プロファイルの設定](#)

[IOS XE RW – 管理者プロファイル](#)

[IOS XE RO – オペレータプロファイル](#)

[ConfigureTACACS+コマンドセット](#)

[CISCO IOS XE RW : 管理者コマンドセット](#)

[CISCO IOS XE RO : オペレータコマンドセット](#)

[デバイス管理ポリシーセットの設定](#)

[パート2: TLS 1.3を介したTACACS+のCisco IOS XEの設定](#)

[設定方法1: デバイスが生成したキーペア](#)

[TACACS+サーバの設定](#)

[トラストポイントの設定](#)

[TACACSおよびAAAとTLSの設定](#)

[設定方法2: CAが生成したキーペア](#)

[TACACSおよびAAAとTLSの設定](#)

[検証](#)

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® XE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、アカウントिंग(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 XE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 XE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 IOS XEソフトウェアバージョン17.15+

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。

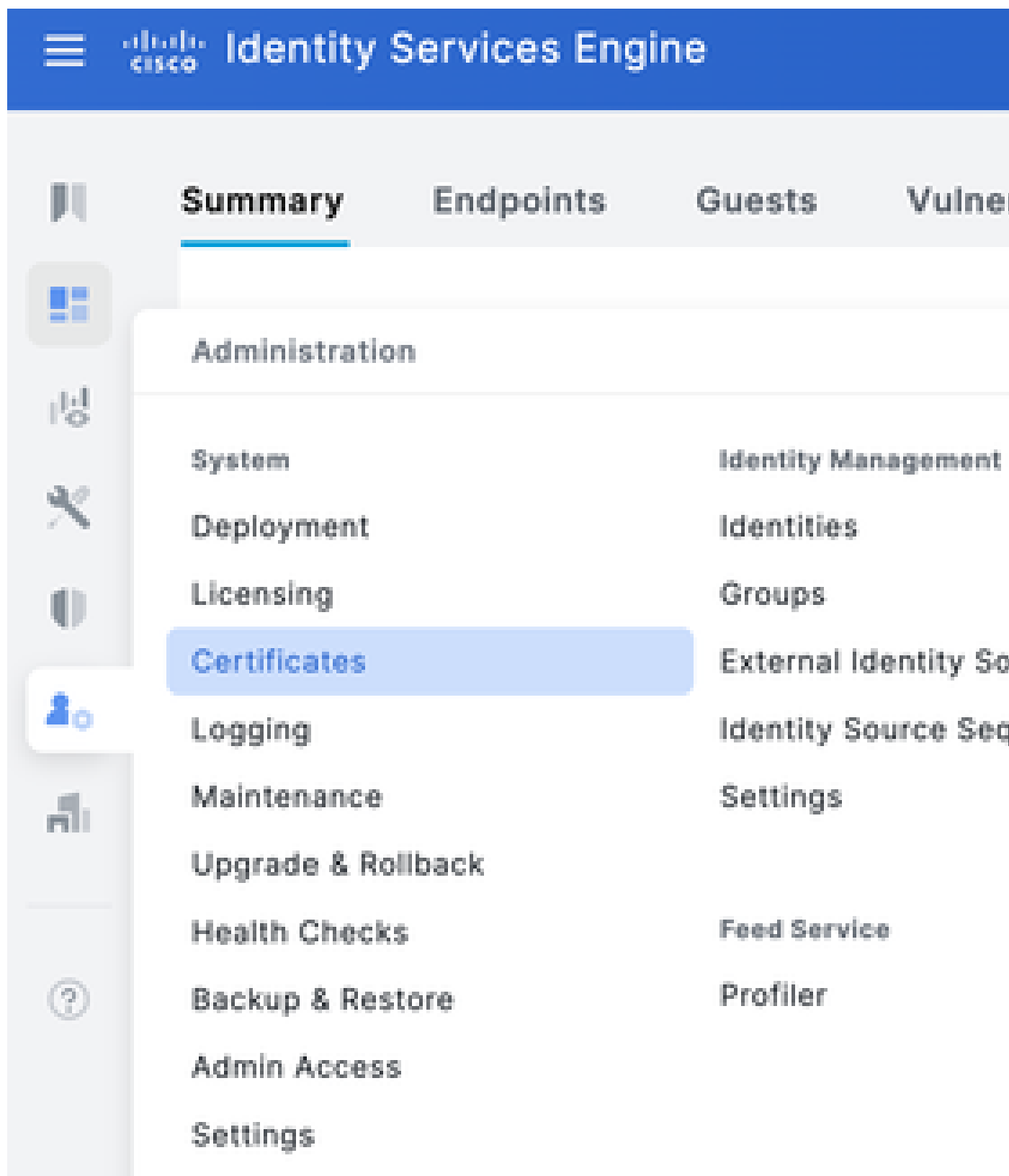
パート1：デバイス管理用のISEの設定

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の下で、Generate Certificate Signing Requestをクリックします。



ステップ4:TACACS inUsageを選択します。

Usage

Certificate(s) will be used for **TACACS** 

Allow Wildcard Certificates ☐ 

ステップ5:TACACS+を有効にするPSNを選択します。

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ ISE1	ISE1#TACACS

手順 6 : Subjectフィールドに、適切な情報を入力します。

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

Country (C)
US

ステップ7:サブジェクト代替名(SAN)の下にDNS名とIPアドレスを追加します。

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	−	+	
⋮	IP Address	✓	10.225.253.209	−	+	①

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



Successfully generated CSR(s)

Certificate Signing request(s) generated:

ISE2#TACACS

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

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の下にあるImportをクリックします。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The 'Certificates' tab is selected in the top navigation bar. On the left, the 'Trusted Certificates' link is highlighted in the sidebar. The main content area displays a table of 'Trusted Certificates'. The 'Import' button is highlighted with a red box. Below the table, there is a note: 'For disaster recovery it is recommended to export and backup all your trusted certificates.'

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2015	Sun, 17 Jan 2...	Ent
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	Ent
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Ent
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 2004	Mon, 14 May ...	Dis
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 20...	Cisco Root CA 20...	Tue, 9 Aug 2016	Sun, 9 Aug 20...	Ent
☐	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...	Ent
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	Ent

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。

Import a new Certificate into the Certificate Store

* Certificate File ISE SVSLab CA.crt

Friendly Name

Trusted For: ⓘ

- ☒ Trust for authentication within ISE
 - ☐ Trust for client authentication and Syslog
 - ☐ Trust for certificate based admin authentication
- ☐ Trust for authentication of Cisco Services
- ☐ Trust for Native IPSec certificate based authentication
- ☐ Validate Certificate Extensions

Description

Submit

Cancel

ステップ 3 : [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。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The 'Certificates' tab is selected, and the 'Trusted Certificates' sub-tab is active. The table displays the following information:

Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
CN=SVS LabCA, OU=SVS, O=Cisco, L=...	Endpoint Infrastructure Cisco Services Endpoints AdminAuth	20 CD 74 02 ...	SVS LabCA	SVS LabCA	Mon, 28 Apr 2025	Sat, 28 Apr 2...

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。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The 'Certificates' tab is selected, and the 'Certificate Signing Requests' sub-tab is active. The table displays the following information:

Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
---------------	---------------------	------------	---------------	-----------	------

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。

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

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。



Warning

The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

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。

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

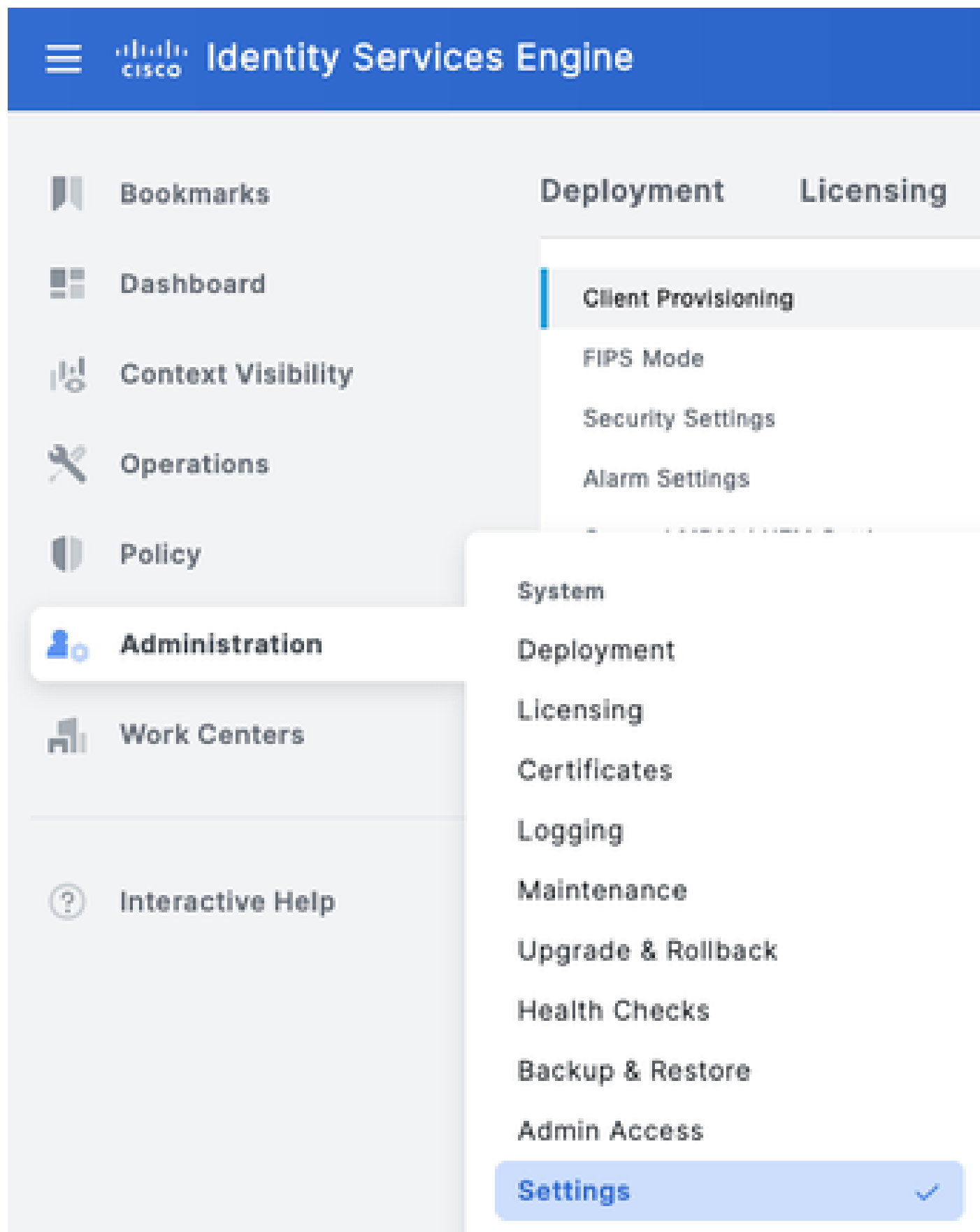
[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ISE1	C=US, ST=NC, L=Raleigh, TACACS O=Cisco, OU=SVS, CN=I SE1.lab#ISE1.lab#00010		ISE1.lab	ISE1.lab	Wed, 10 Sep 2025	Fri, 10 Sep 2027	Active

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の順に選択します。



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、Saveをクリックします。

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

General MDM / UEM Settings

Posture

Profiling

Protocols

Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

☐ TLS 1.0

☐ TLS 1.1

☒ TLS 1.2

☒ TLS 1.3

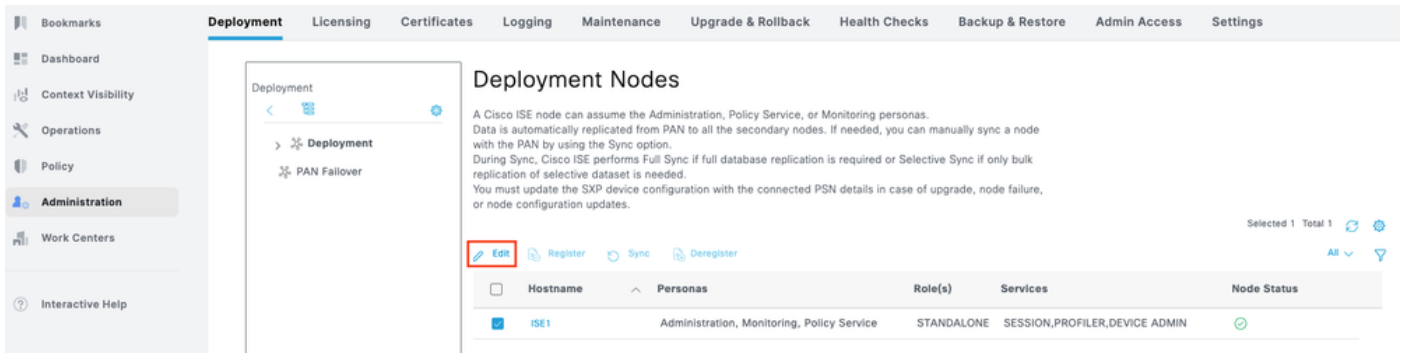


警告:TLSバージョンを変更すると、Cisco ISEアプリケーションサーバがすべてのCisco ISE導入マシンで再起動します。

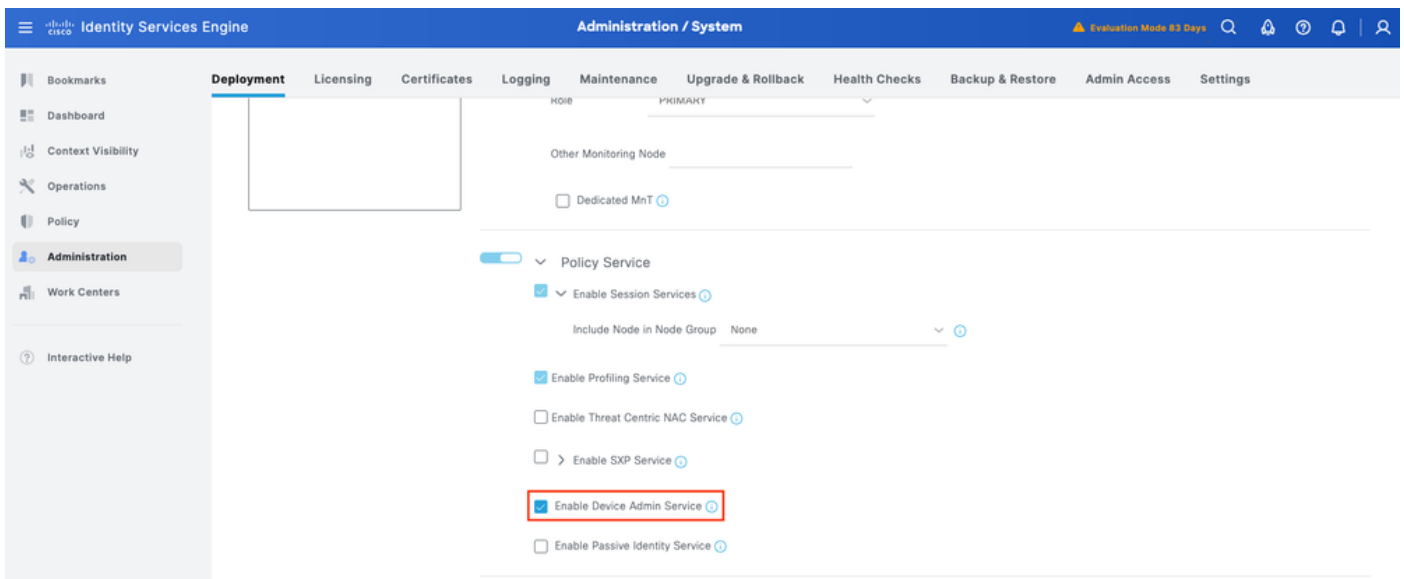
ISEでのデバイス管理の有効化

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の順に選択します。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。



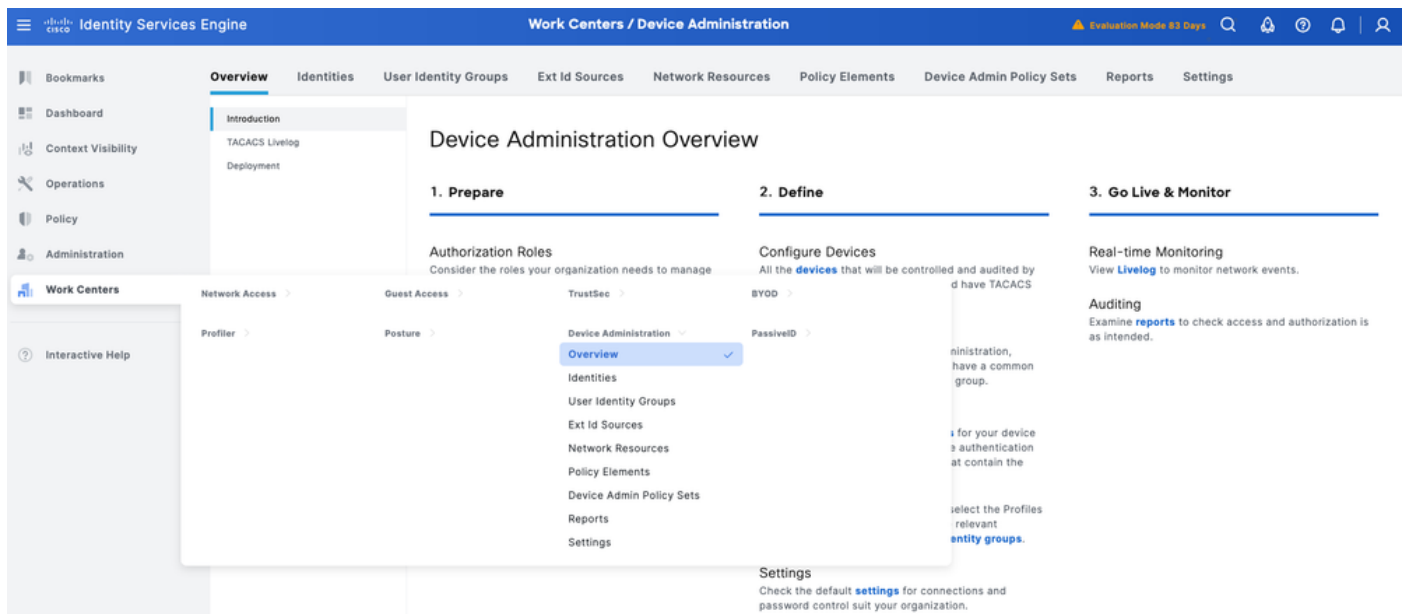
ステップ2:GeneralSettingsで、スクロールダウンしてEnable Device Admin Serviceの横にあるチェックボックスをオンにします。



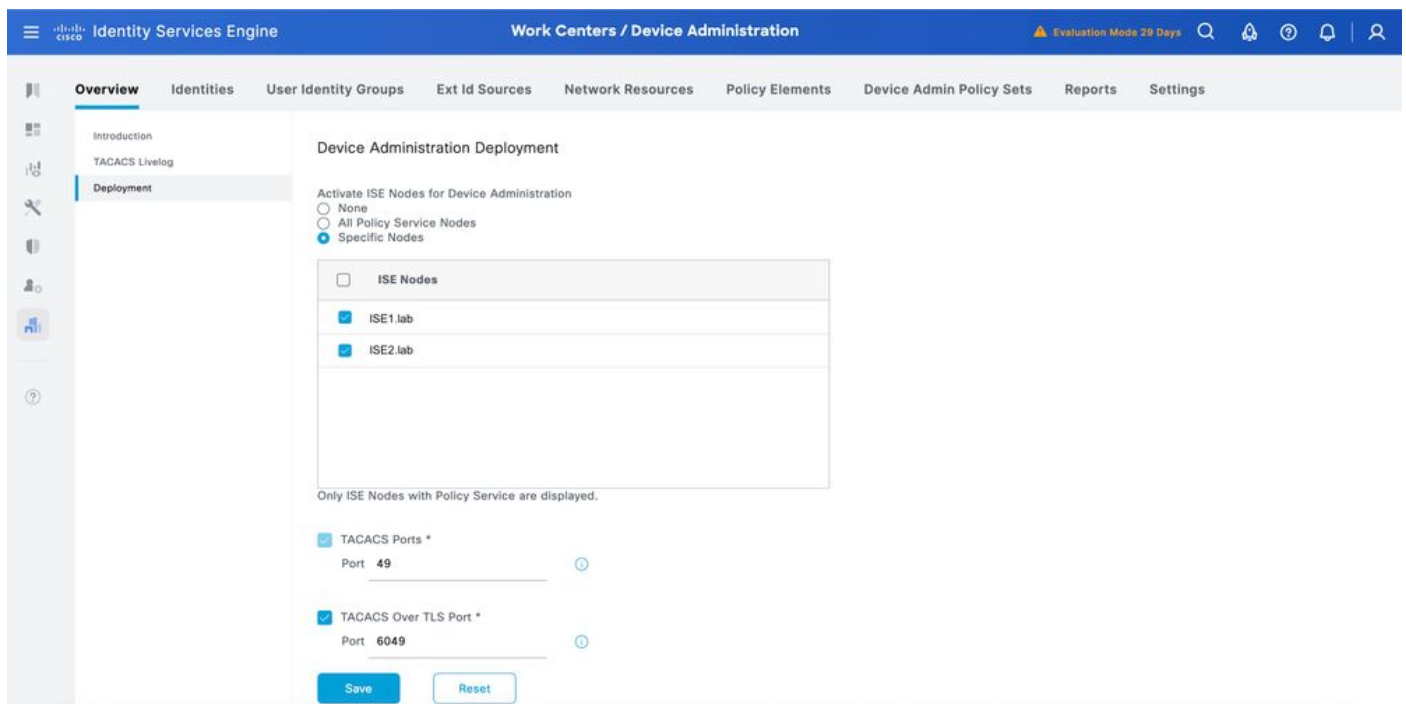
ステップ3：設定を保存します。Device Admin ServiceがISEで有効になりました。

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、Network Device Groupsをクリックして、IOS XEという名前のグループを作成します。

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

×

Add Group

Name*

IOSXE

Description

Parent Group*

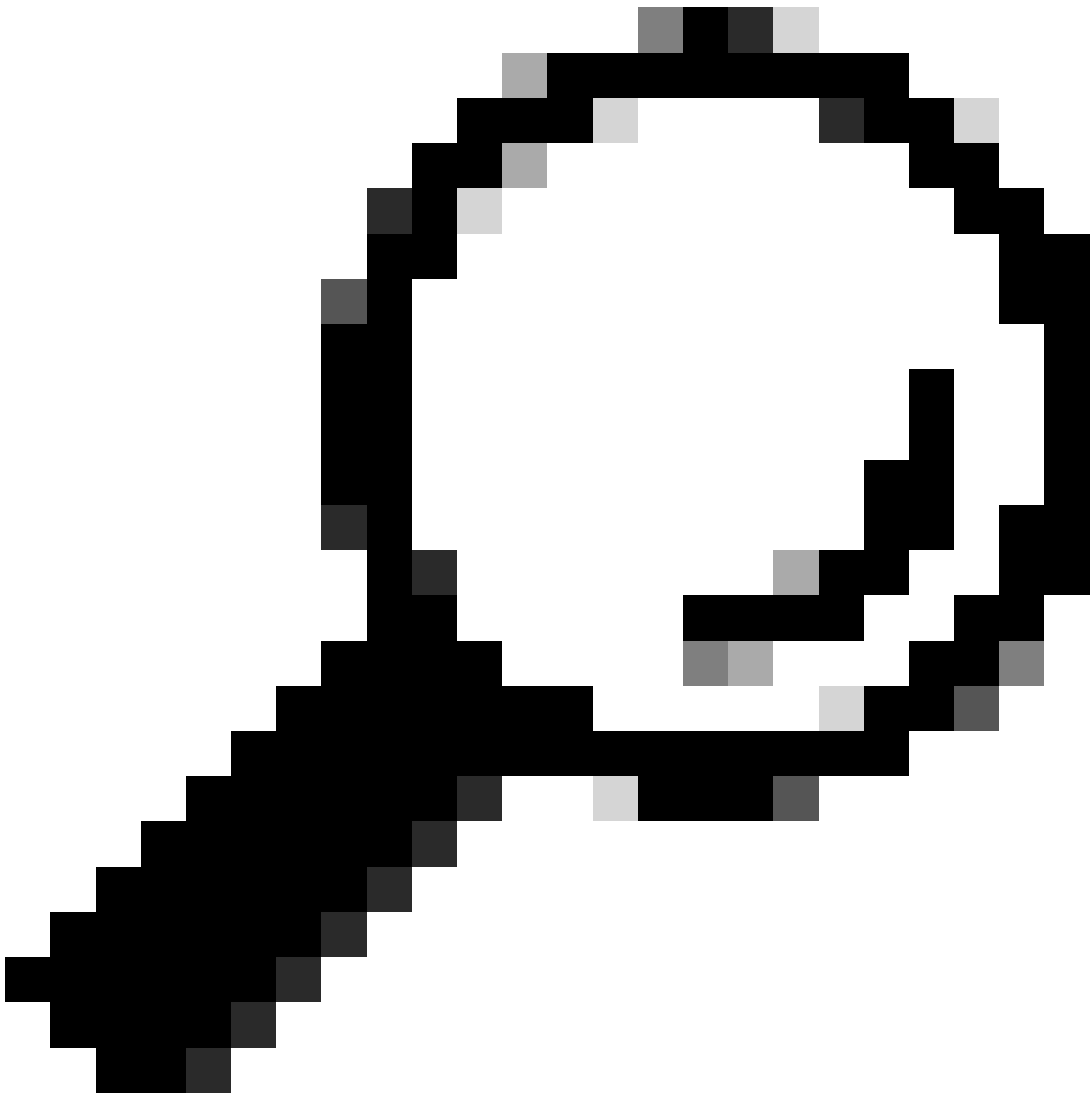
Select Group or Add as root group

Cancel

Save

☐

IOSXR



ヒント：すべてのデバイスタイプとすべてのロケーションは、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 XE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。このテストでは、SVS_BRPASR1Kとなります。

Identity Services Engine

Work Centers / Device Administration

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices List > SVS_BRPASR1K

Network Devices

NameSVS_BRPASR1K

Description

IP Address

* IP : 10.225.253.180

/ 32

Device ProfileCisco

Model Name

Software Version

Network Device Group

LocationAll Locations

Set To Default

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 XE)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。

Identity Services Engine

Work Centers / Device Administration

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

☐

>

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)^{*}

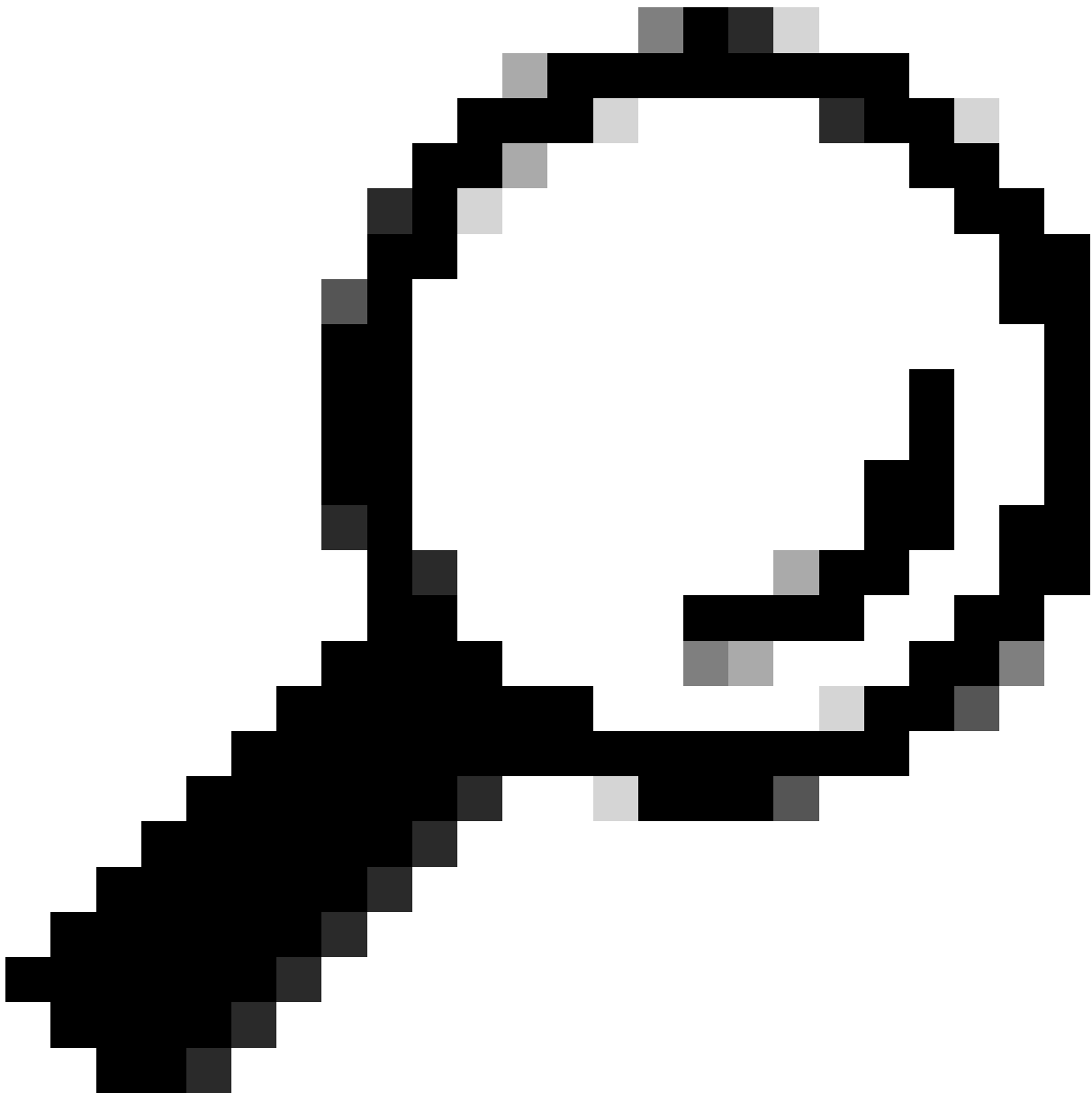
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When 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

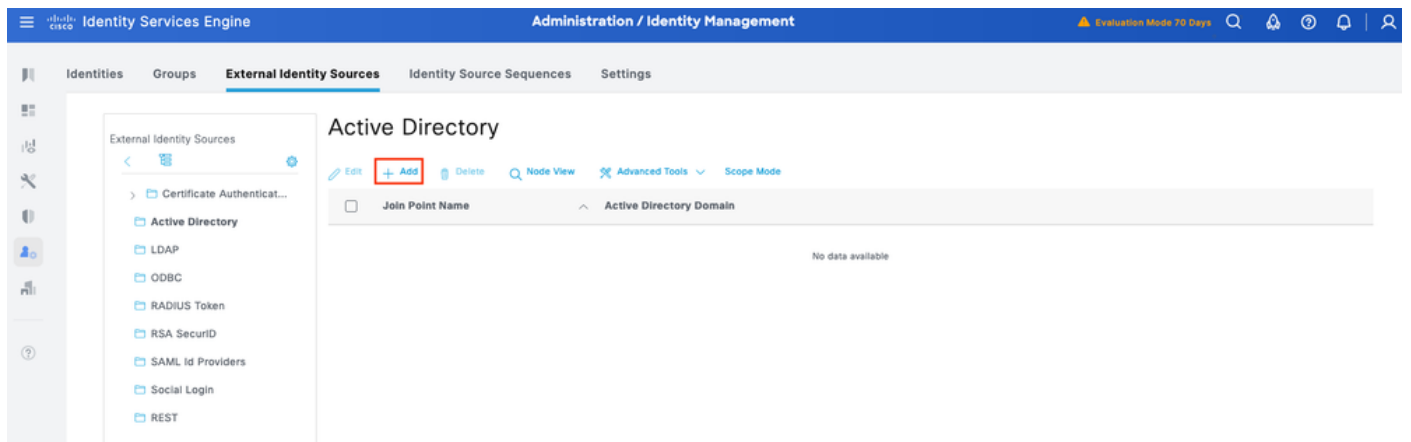


ヒント：デバイスにコマンドが送信されるたびにTCPセッションが再起動しないように、シングルコネクトモードを有効にすることを推奨します。

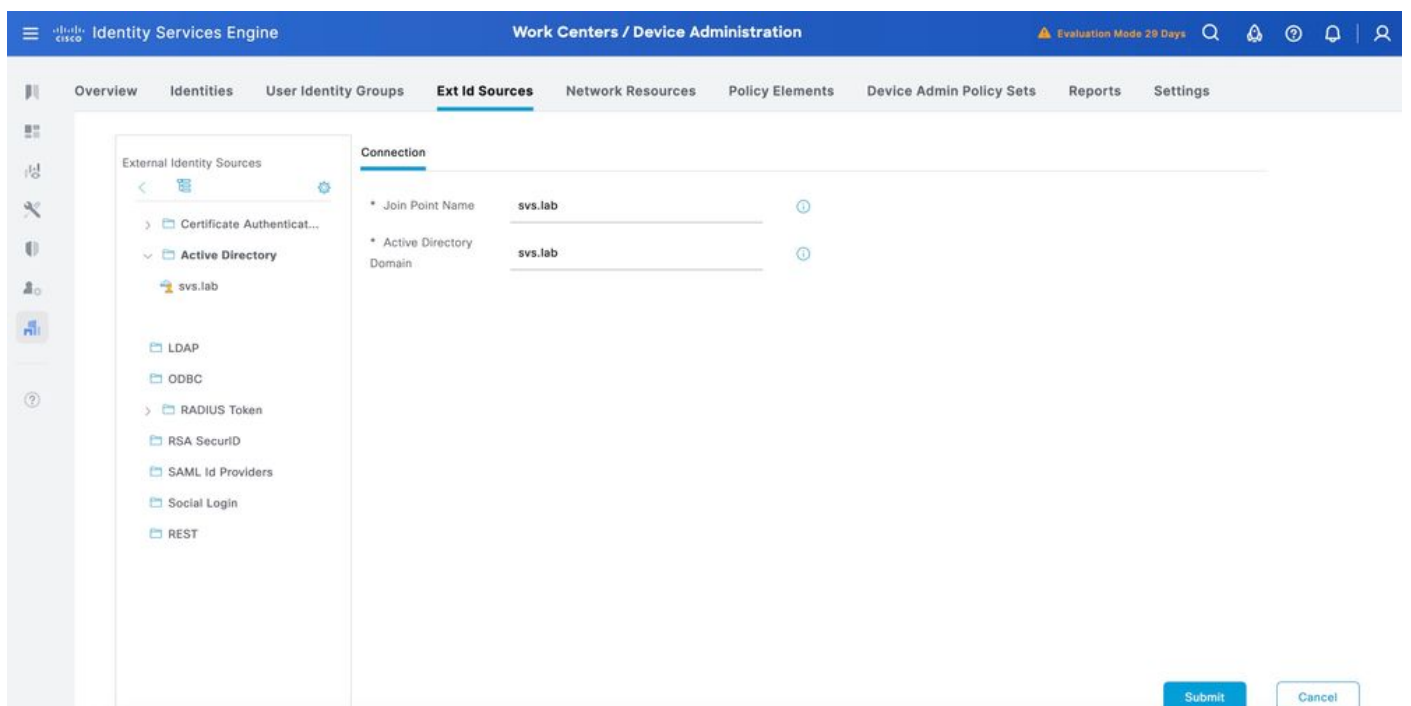
アイデンティティストアの設定

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。

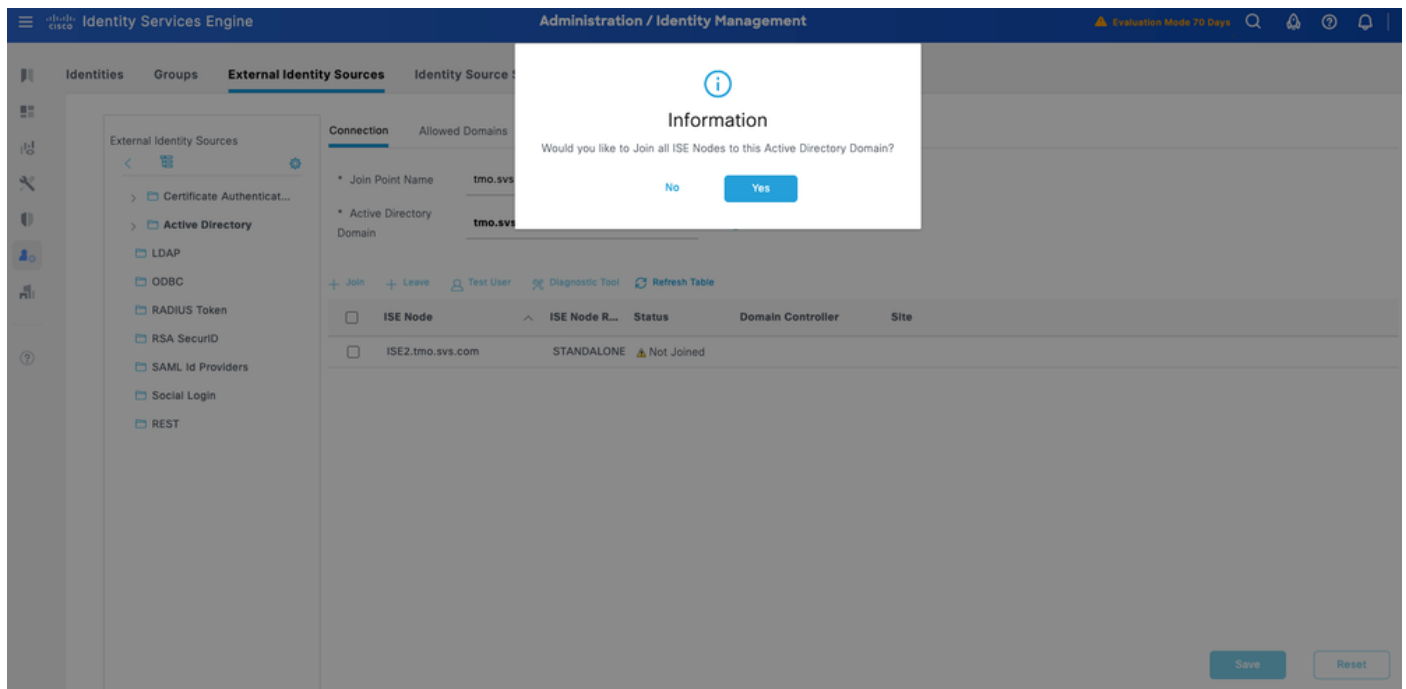
手順 1：Administration > Identity Management > External Identity Stores > Active Directoryの順に移動します。Addをクリックして、新しいADジョイントポイントを定義します。



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?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。

×

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name ⓘ

administrator

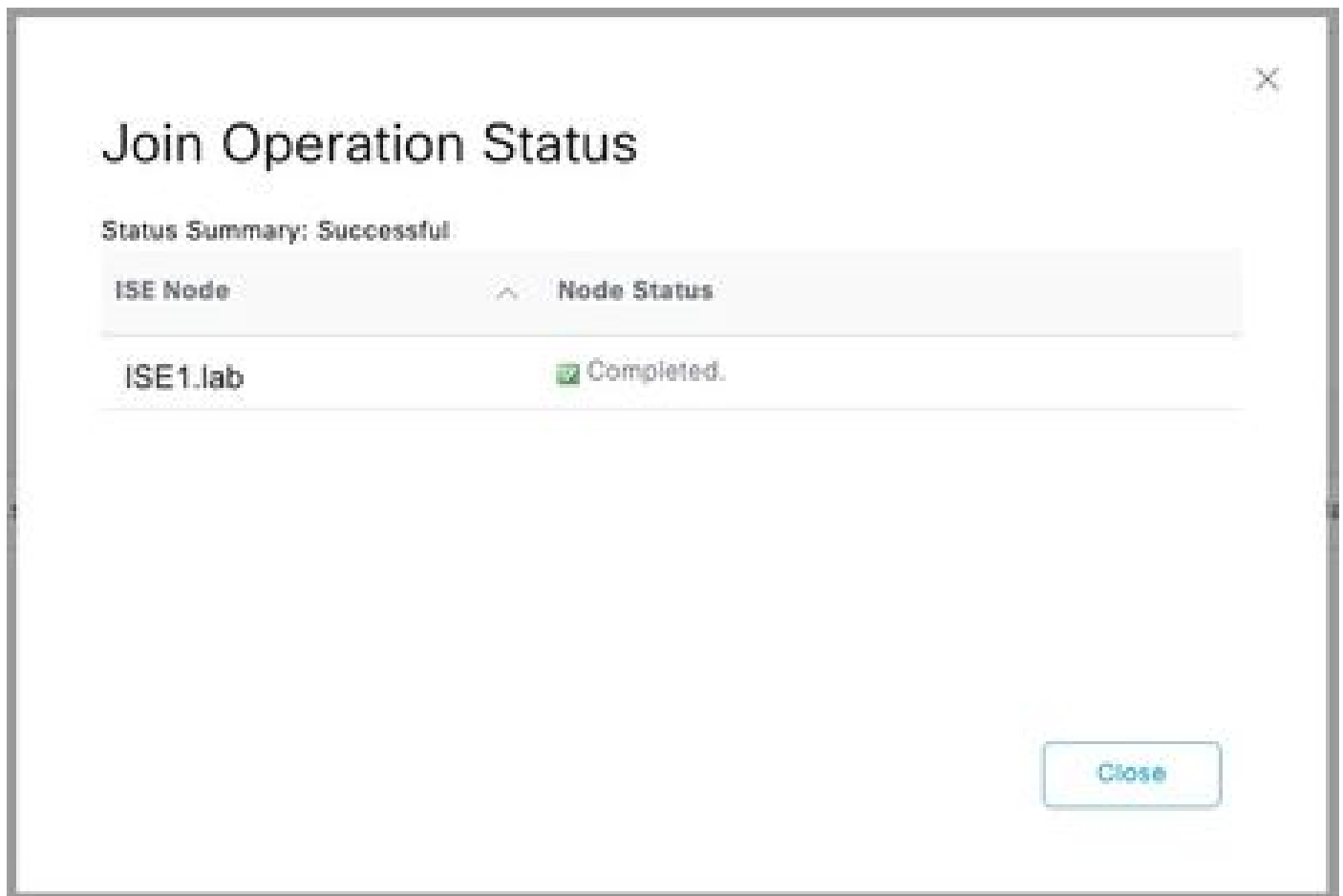
* Password ⓘ

☐ Specify Organizational Unit ⓘ

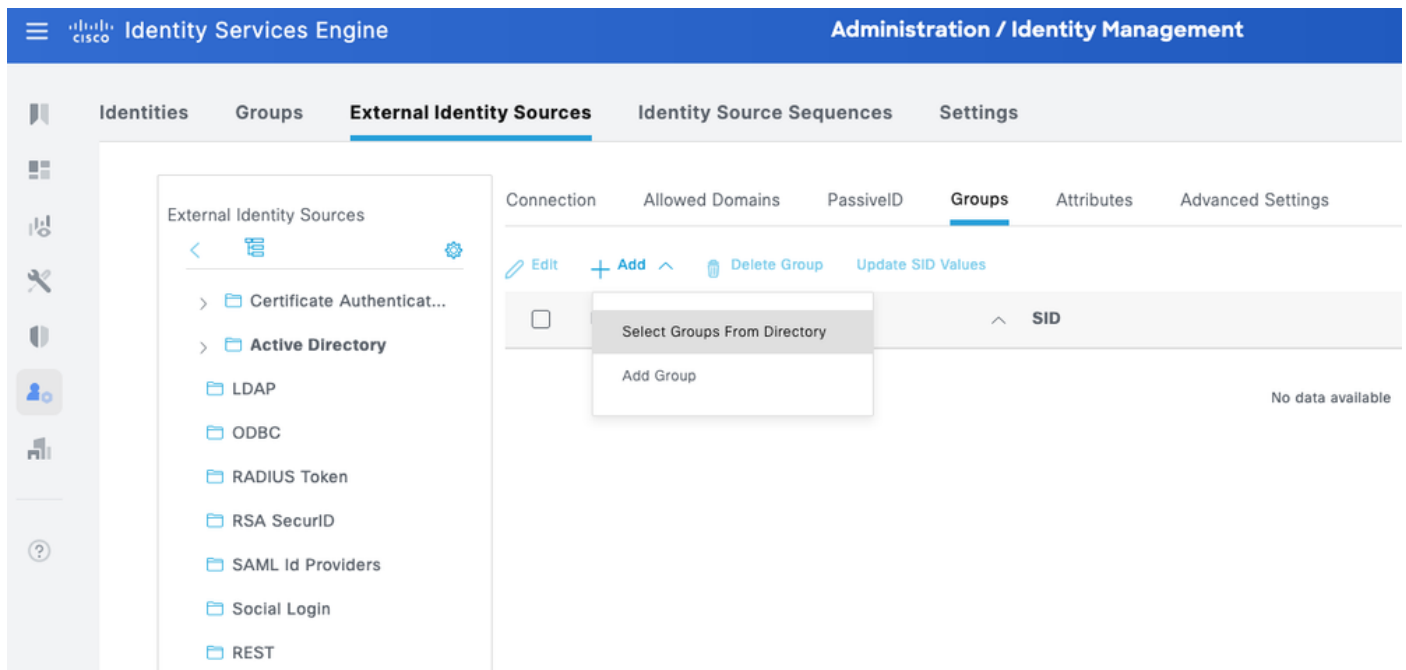
☒ Store Credentials ⓘ

Cancel

OK



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するグループを示します



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain svs.lab

Name
Filter Device *

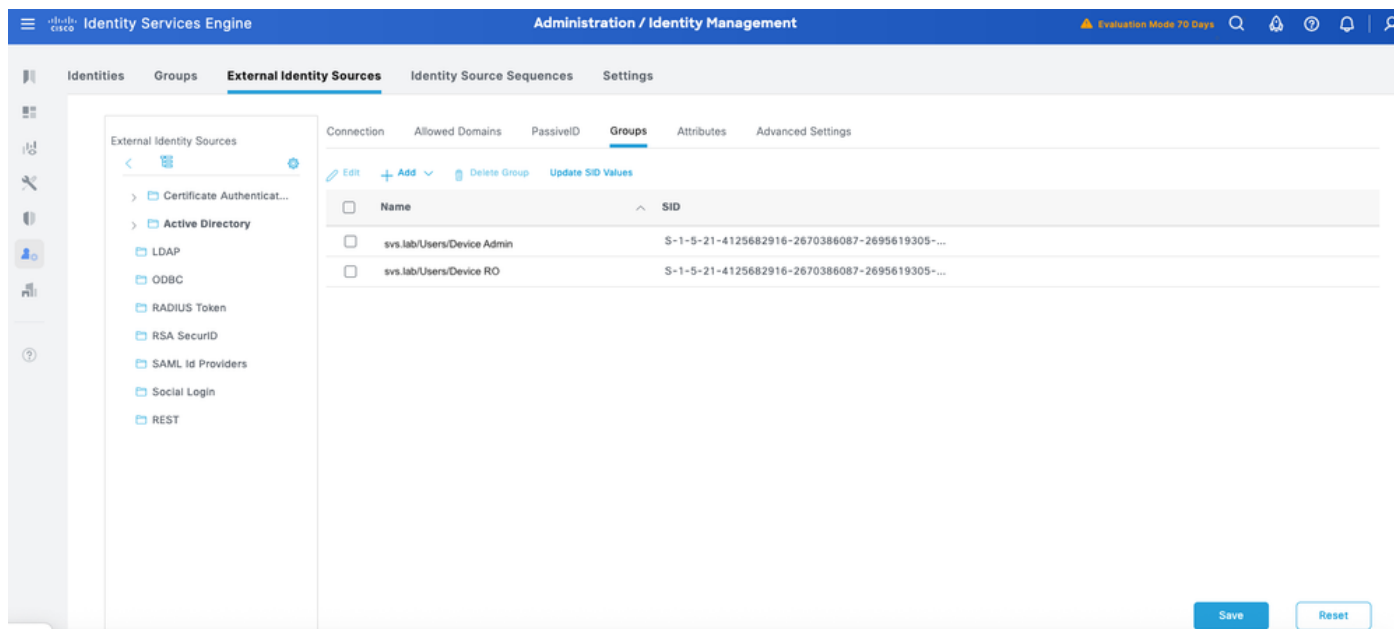
SID *
Filter

Type
Filter ALL

Retrieve Groups...

2 Groups Retrieved.

☐	Name	Group SID	Group Type
☐	svs.lab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
☐	svs.lab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



TACACS+プロファイルの設定

TACACS+プロファイルをCisco IOS XEデバイスの2つの主要なユーザロールにマッピングします。

- 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。

これらは、IOS XE_RWとIOSXR_ROの2つのTACACS+プロファイルとして定義されています。

IOS XE_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、IOS XE_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、保存します。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. The left sidebar contains navigation icons and a menu with 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements' (selected), 'Device Admin Policy Sets', and 'More'. The main content area is titled 'TACACS Profiles > IOSXE_RW TACACS Profile'. It includes a 'Name' field with 'IOSXE_RW', a 'Description' text area, and tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'Shell'. Below this, there are two rows of settings: 'Default Privilege' and 'Maximum Privilege', both set to '15' with a dropdown arrow and the text '(Select 0 to 15)'.

IOS XE_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、IOS XE_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。

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets More

Conditions > Network Conditions > Results > Allowed Protocols > TACACS Command Sets > **TACACS Profiles**

Name: IOSXE_RO

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege	1	(Select 0 to 15)
☒ Maximum Privilege	1	(Select 0 to 15)
☐ Access Control List		
☐ Auto Command		

ConfigureTACACS+コマンドセット

これらは、CISCO_IOS XE_RWとCISCO_IOS XE_ROという2つのTACACS+コマンドセットとして定義されています。

CISCO_IOS XE_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_IOS XE_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。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. The left sidebar contains icons for Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, and More. The main content area is titled 'Policy Elements' and shows the configuration for a TACACS Command Set named 'CISCO_IOSXE_RW'. The 'Name' field is filled with 'CISCO_IOSXE_RW'. The 'Description' field is empty. The 'Commands' section has a checkbox 'Permit any command that is not listed below' which is checked. Below this, there is a table with columns 'Grant', 'Command', and 'Arguments'. The 'Grant' column has a checkbox, and the 'Command' column is currently empty.

CISCO_IOS XE_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_IOS XE_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で、新しいコマンドを追加します。

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

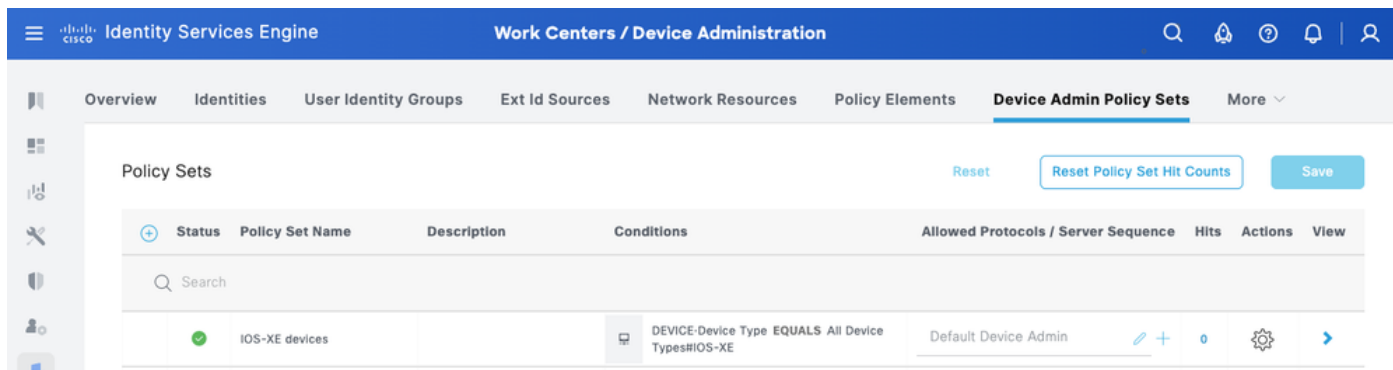
ステップ4：データを確認して、Saveをクリックします。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. The left sidebar contains icons for Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, and More. The main content area is titled 'Policy Elements' and shows the configuration for a TACACS Command Set named 'CISCO_IOSXE_RO'. The 'Name' field is filled with 'CISCO_IOSXE_RO'. The 'Description' field is empty. The 'Commands' section has a checkbox 'Permit any command that is not listed below' which is unchecked. Below this, there is a table with columns 'Grant', 'Command', and 'Arguments'. The 'Grant' column has a checkbox, and the 'Command' column is filled with 'show'. The 'Arguments' column is empty.

デバイス管理ポリシーセットの設定

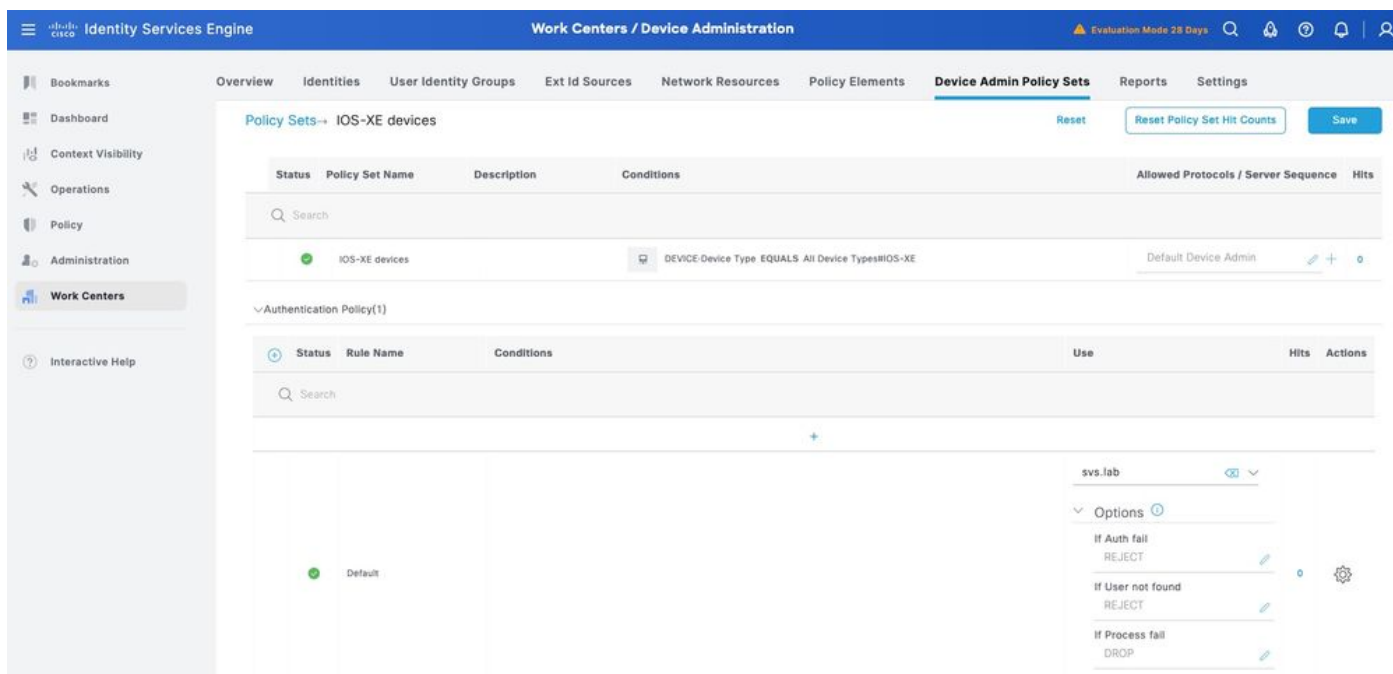
デバイス管理では、ポリシーセットはデフォルトで有効になっています。ポリシーセットは、デバイスタイプに基づいてポリシーを分割できるため、TACACSプロファイルの適用が容易になります。

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 XEデバイスを追加します。条件でDEVICE:Device Type EQUALS All Device Types#IOS XE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: 認証ポリシーの作成。認証用に、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許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。

Identity Services Engine Work Centers / Device Administration

Policy Sets → IOS-XE devices

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	IOS-XE devices		DEVICE-Device Type EQUALS All Device Types#IOS-XE	Default Device Admin	0

> Authentication Policy(1)

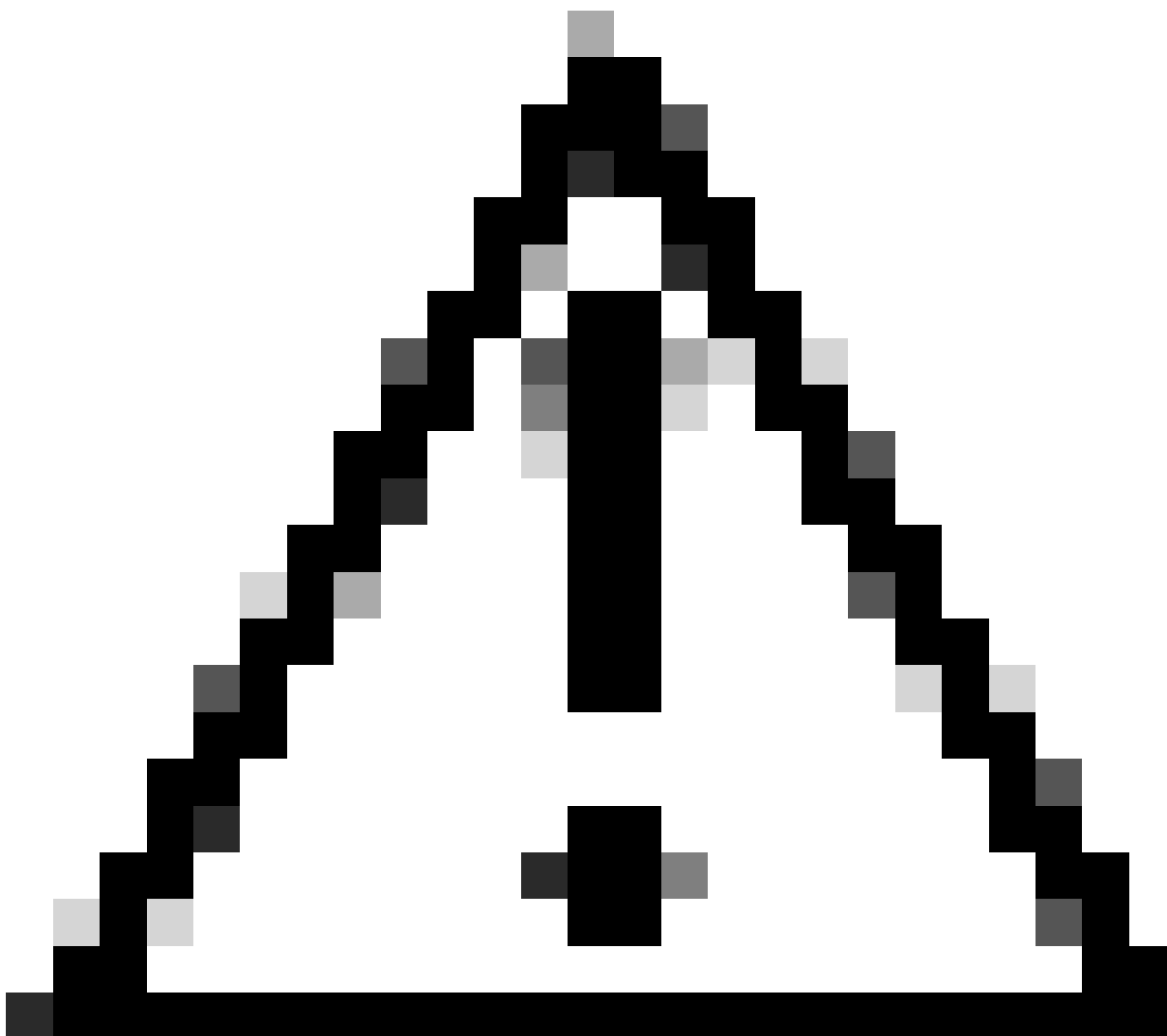
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

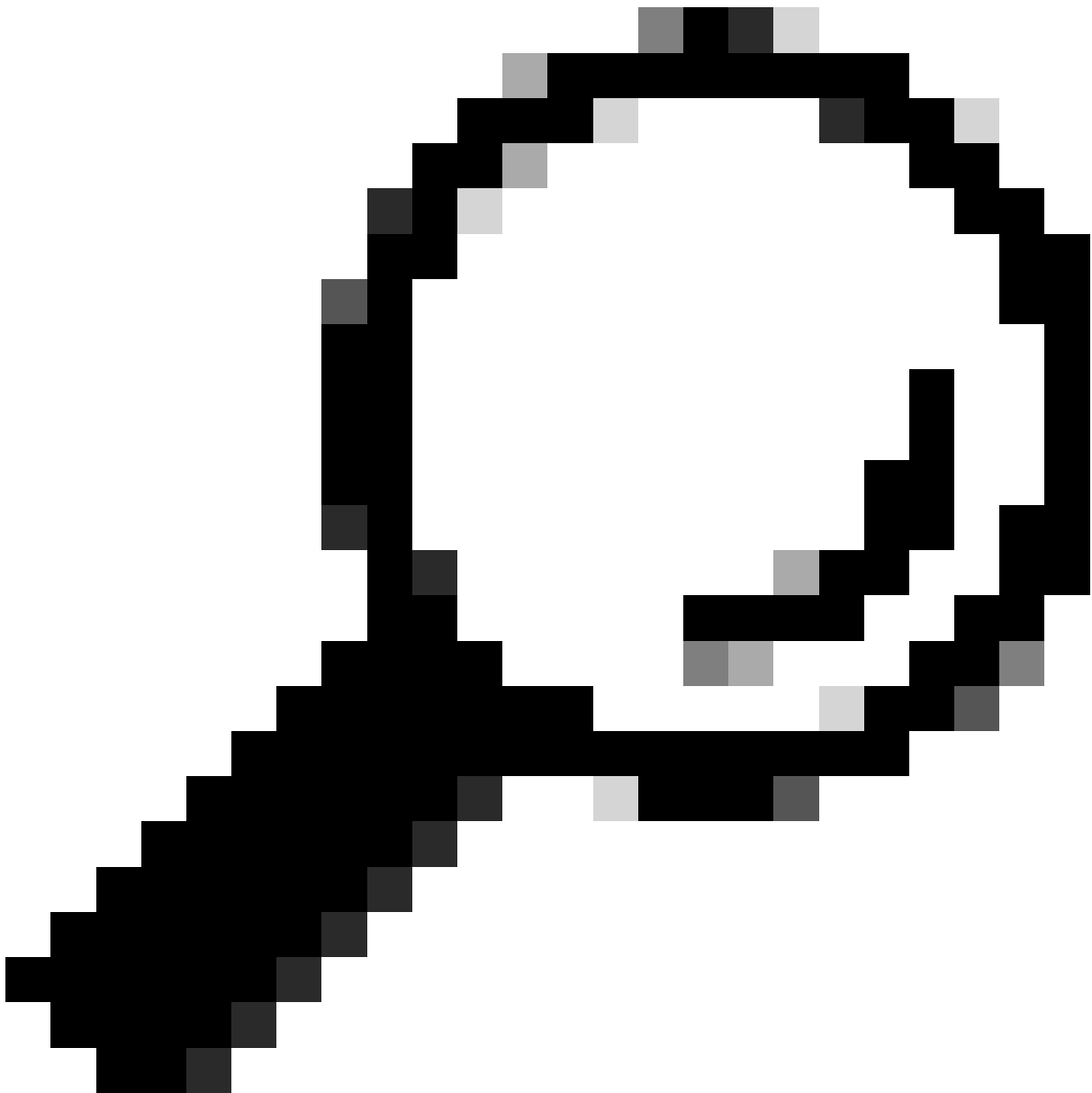
✓ Authorization Policy(3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	Authorization Rule RO	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device RO	CISCO_IOSXE_RO	IOSXE_RO	0		
✓	Authorization Rule RW	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device Admin	CISCO_IOSXE_RW	IOSXE_RW	0		
✓	Default		DenyAllCommands	Deny All Shell Profile	0		

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

設定方法1：デバイスが生成したキーペア

TACACS+サーバの設定

手順1 ドメイン名を設定し、ルータのトラストポイントに使用するキーペアを生成します。

```
ip domain name svs.lab
```

```
crypto key generate ec keysizes 256 label svs-256ec-key
```

トラストポイントの設定

手順1 ルータのトラストポイントを作成し、キーペアを関連付けます。

```
crypto pki trustpoint svcs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svcs-256ec-key
```

ステップ 2 : 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>

cat9k(config)#

```
crypto pki authenticate svcs_cat9k
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUUA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZDZAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLZWwNTV1MxEjAQBgNVBAMTCVNWUyBMWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTjy+kksifD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwV4MBBjHFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULO/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBCnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBNkX4pqY7CDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
```

```
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQMFgpTVlMgTGF iENBMAOGCSqGSib3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOmN7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTwL1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D

Fingerprint SHA1: 0EB181E9 5A3ED780 3BC5A805 9A854A95 C83AC737

% Do you accept this certificate? [yes/no]:

yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

cat9k(config)#

ステップ 3：証明書署名要求(CSR)を生成します。

<#root>

cat9k(config)#

crypto pki enroll svcs_cat9k

% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab

% The subject name in the certificate will include: cat9k.svs.lab

Display Certificate Request to terminal? [yes/no]:

yes

Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBfDCCASMAQAwgYQxGjAYBgNVBAMTEWdhD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAXCzAJBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCsqGSib3DQEJAHYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgqhkJOPQIBggqhkJOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqDww
OgYJKoZIhvcNAQKOMS0wKzAcBgNVHREFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTWm3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
```

-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:

no

cat9k(config)#

ステップ 4 : CA署名付き証明書をインポートします。

<#root>

cat9k(config)#

crypto pki import svcs_cat9k certificate

Enter the base 64 encoded certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIID8zCCAduGAWIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTE0MTUxMjAwWWhcNMjUwNTE0MTUxMjAwWjCBhDEaMBGGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAStA1NWUzE0MAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUEELMAkGA1UECBMCTkMxCzAJBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBGwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsgaZHGwy2H9Yd
m5vIau6PjczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyZCsTBb6RvL+HsXqBgXGc5
1xCSolTyOdUxFipJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvj4rSPUHQSY+4m
Qq2Sn3iqf4mGh/A08T4iXfWDwfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVRpitwN3Zb09poZyWiRLTnBsb42xNaWiL9bjQznA0iTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+41OTMawDgGiEv7iaiJ6xWc95EC+Adm0x3FvBXmtIM9qr7WwHW6
3C2hVYHJH254e1V5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAH0FcyXrvG6
3i/1b9erGQ==
```

-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#

TACACSおよびAAAとTLSの設定

ステップ 1 : TACACSサーバとAAAグループを作成し、クライアント（ルータ）トラストポイン

トを関連付けます。

```
tacacs server sv_s_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint client sv_s_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
server name sv_s_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

ステップ 2 : AAA方式を設定します。

```
aaa authentication login default group sv_s_tls local enable
aaa authentication login console local enable
aaa authentication enable default group sv_s_tls enable
aaa authorization config-commands
aaa authorization exec default group sv_s_tls local if-authenticated
aaa authorization commands 1 default group sv_s_tls local if-authenticated
aaa authorization commands 15 default group sv_s_tls
aaa accounting exec default start-stop group sv_s_tls
aaa accounting commands 1 default start-stop group sv_s_tls
aaa accounting commands 15 default start-stop group sv_s_tls
aaa session-id common
```

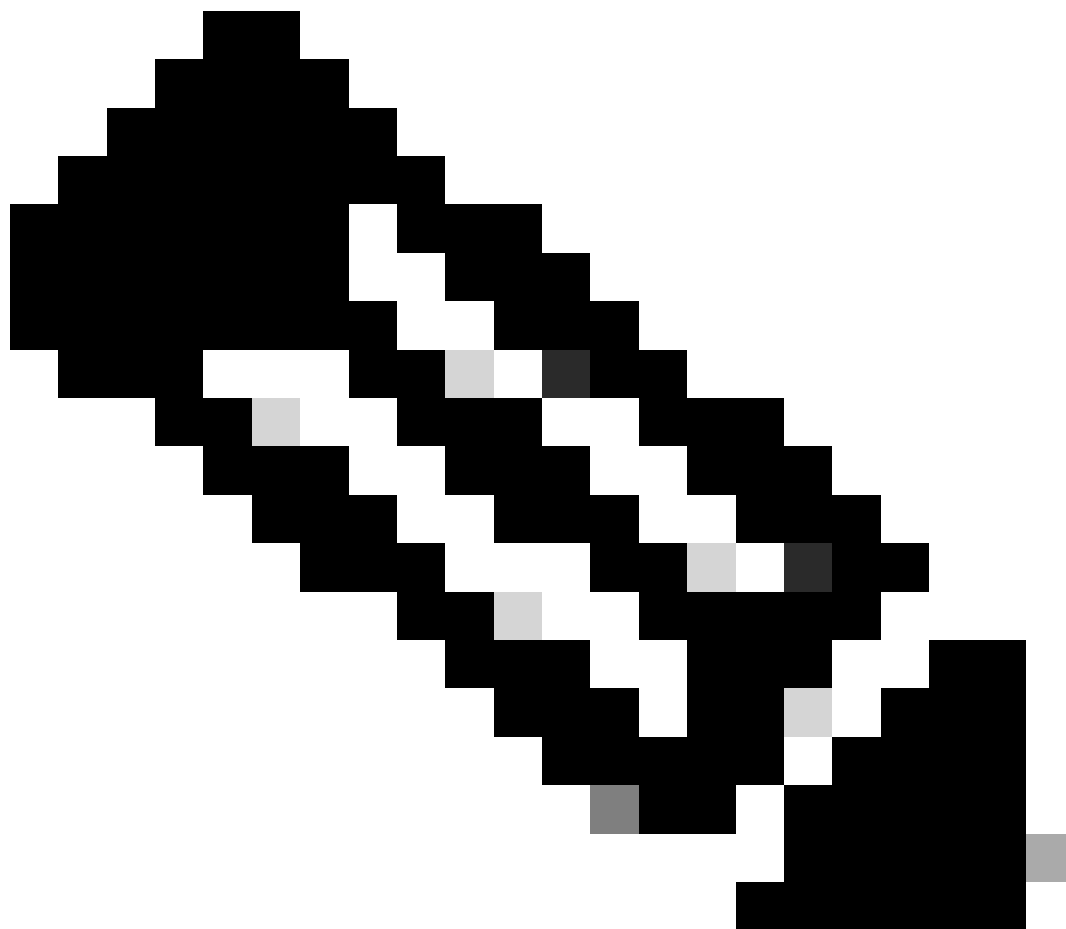
設定方法2:CAが生成したキーペア

CSR方式の代わりにPKCS#12形式でキーおよびデバイス証明書とCA証明書を直接インポートする場合は、この方式を使用できます。

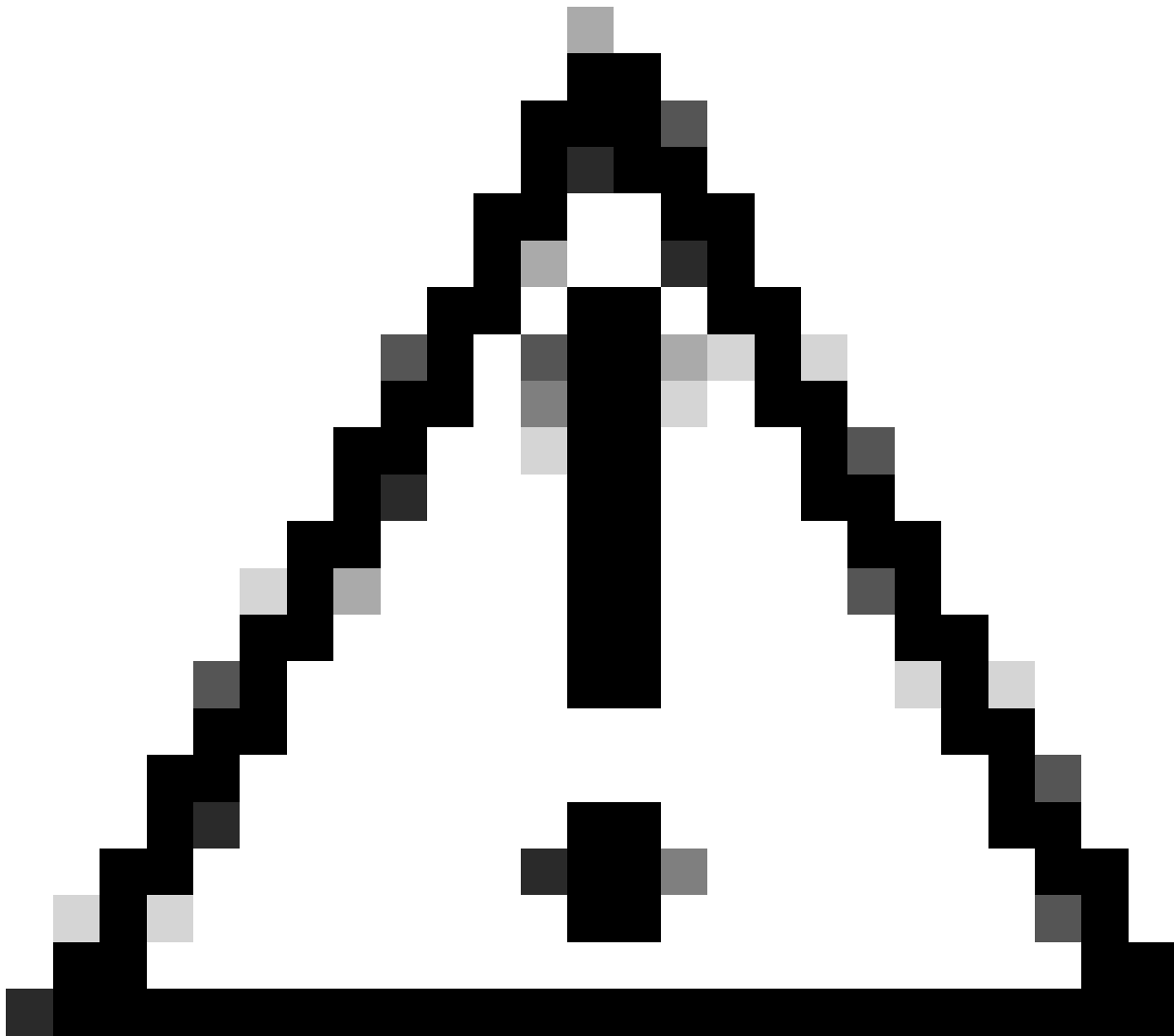
ステップ 1 : クライアントトラストポイントを作成します。

```
cat9k(config)#crypto pki trustpoint sv_s_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

ステップ 2 : PKCS#12ファイルをブートフラッシュにコピーします。



注:PKCS#12ファイルに完全な証明書チェーンと秘密キーが暗号化ファイルとして含まれていることを確認してください。



注意：インポートされるPKCS#12のキーは、ECCではなく、RSA (例：RSA 2048) タイプである必要があります。

<#root>

cat9k#

copy sftp bootflash: vrf Mgmt-vrf

Address or name of remote host [10.225.253.247]?

Source username [svs-user]?

Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx

Destination filename [cat9k-25jun17.pfx]?

Password:

!

2960 bytes copied in 3.022 secs (979 bytes/sec)

ステップ 3：importコマンドを使用してPKCS#12ファイルをインポートします。

<#root>

cat9k#

crypto pki import svc_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

password C1sco.123

% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx

CRYPTO_PKI: Imported PKCS12 file successfully.

cat9k#

cat9k#

show crypto pki certificates svc_cat9k_25jun17

Certificate

Status: Available

Certificate Serial Number (hex): 5860BF33A2033365

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

Name: cat9k.svs.lab

e=pkalkur@cisco.com

cn=cat9k.svs.lab

ou=svs

o=cisco

l=rtp

st=nc

c=us

Validity Date:

start date: 17:56:00 UTC Jun 17 2025

end date: 17:56:00 UTC Jun 17 2026

Associated Trustpoints: svc_cat9k_25jun17

CA Certificate

Status: Available

Certificate Serial Number (hex): 20CD7402C4DA37F5

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Validity Date:

start date: 17:05:00 UTC Apr 28 2025

end date: 17:05:00 UTC Apr 28 2035

Associated Trustpoints: svc_cat9k_25jun17 svc_cat9k

Storage: nvram:SVSLabCA#37F5CA.cer

TACACSおよびAAAとTLSの設定

ステップ 1 : TACACSサーバとAAAグループを作成し、クライアント (ルータ) トラストポイントに関連付けます。

```
tacacs server svb_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint client svb_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svb_tls
server name svb_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

ステップ 2 : AAA方式を設定します。

```
aaa authentication login default group svb_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svb_tls enable
aaa authorization config-commands
aaa authorization exec default group svb_tls local if-authenticated
aaa authorization commands 1 default group svb_tls local if-authenticated
aaa authorization commands 15 default group svb_tls
aaa accounting exec default start-stop group svb_tls
aaa accounting commands 1 default start-stop group svb_tls
aaa accounting commands 15 default start-stop group svb_tls
aaa session-id common
```

検証

設定を確認します。

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

AAAおよびTACACS+のデバッグ。

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure
```

! Below debugs will be needed only if there is any issue with SSL Handshake

```
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

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。