

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](#)

[ISEの前提条件とその他のタスク](#)

[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](#)

[ソフトウェアバージョンと基本設定の確認](#)

[TACACS+サーバの設定](#)

[方法1: デバイスで生成されたキーペア](#)

[トラストポイントの設定](#)

[方法2: CAによって生成されたキーペア \(PFX方式 \)](#)

[トラストポイントの設定](#)

[TACACS+ TLSの設定](#)

[AAA 設定](#)

[証明書更新プロセス](#)

[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 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
- ・ Nexus 9000スイッチモデルC9364D-GX2A、Cisco NX-OSバージョン10.6(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たものです。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。

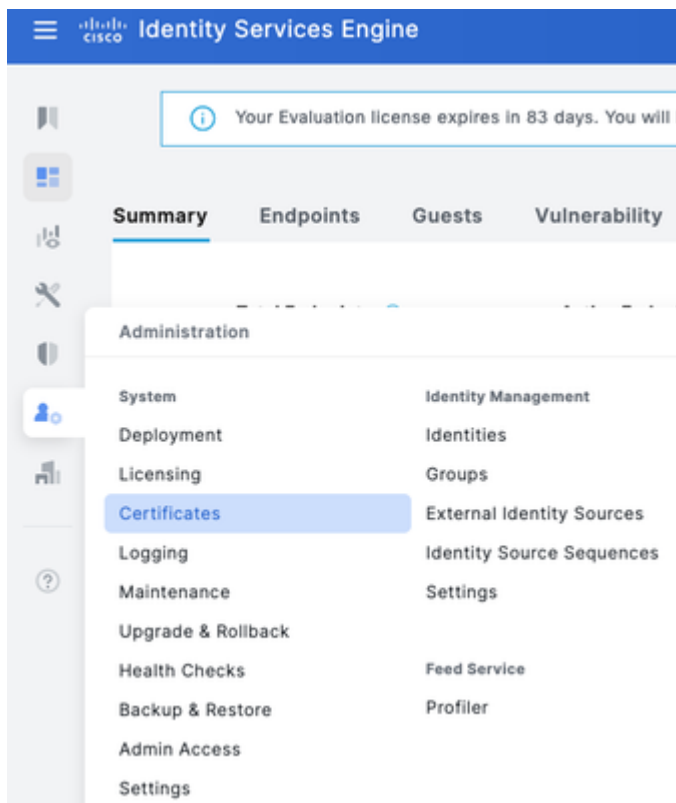
Device Admin用のISEの設定

TACACS+サーバ認証用の証明書署名要求の生成

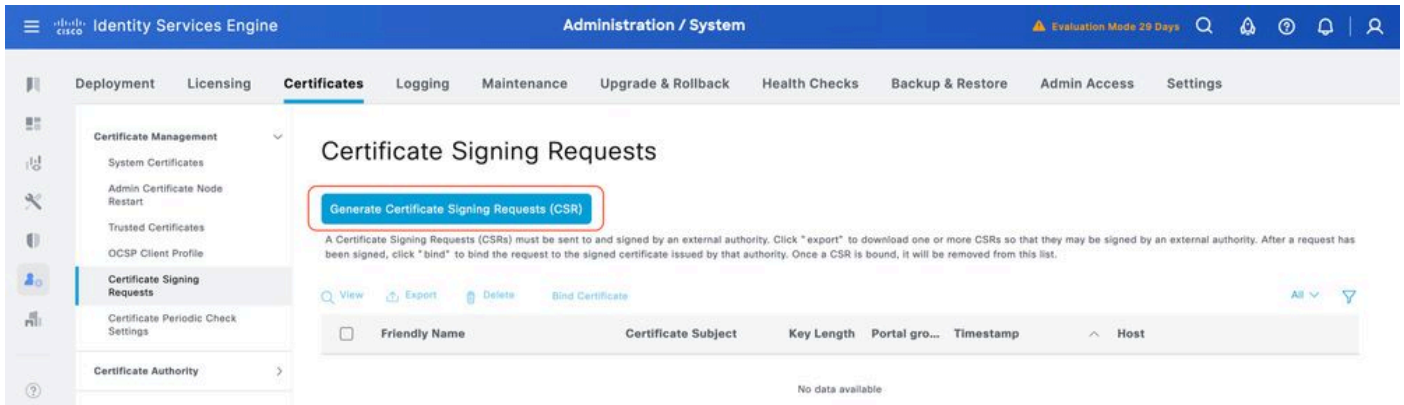
ステップ 1: サポートされているいずれかのブラウザを使用して、ISE管理Webポータルにログインします。

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。

Usage

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

Allow Wildcard Certificates ⓘ

ステップ 5 TACACS+ が有効になっている PSN を選択します。

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ISE1	ISE1#TACACS

ステップ 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 Subject Alternative Name (SAN)の下にDNS NameとIP Addressを追加します。

Subject Alternative Name (SAN)

DNS Name	ISE1.lab	-	+	
IP Address	10.225.253.209	-	+	?

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。

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 OSCP Client Profile Certificate Signing Requests Certificate Periodic Check Settings Certificate Authority

Trusted Certificates

For disaster recovery it is recommended to export and backup all your trusted certificates.

Import Export Delete View show internal CA certificates

<input type="checkbox"/>	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Ent
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
<input type="checkbox"/>	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。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。

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

[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 'Trusted Certificates' page in the Cisco Identity Services Engine. The page title is 'Trusted Certificates' with a warning icon and text: 'For disaster recovery it is recommended to export and backup all your trusted certificates.' Below the title are action buttons: Edit, Import, Export, Delete, View, and show internal CA certificates. A table lists the certificates with columns: Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Status. The first row is highlighted with a red box.

Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐ CN=SVS LabCA, OU=SVS, O=Cisco, L=...	Infrastructure Cisco Services Endpoints AdminAuth	20 CD 74 02 ...	SVS LabCA	SVS LabCA	Mon, 28 Apr 2025	Sat, 28 Apr 2...	Ens
☐ Default self-signed server certificate	Endpoints Infrastructure	02 36 30 F4 6...	ISE2.svs.lab	ISE2.svs.lab	Fri, 11 Jul 2025	Sun, 11 Jul 2...	Ens
☐ DigiCert Global Root CA	Cisco Services	08 3B E0 56 9...	DigiCert Global R...	DigiCert Global R...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Ens
☐ DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6 ...	DigiCert Global R...	DigiCert Global R...	Thu, 1 Aug 2013	Fri, 15 Jan 20...	Ens
☐ DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26 ...	DigiCert High Ass...	DigiCert High Ass...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Ens
☐ DigiCert SHA2 High Assurance Server ...	Endpoints Infrastructure	04 E1 E7 A4 ...	DigiCert SHA2 HI...	DigiCert High Ass...	Tue, 22 Oct 2013	Sun, 22 Oct 2...	Ens

署名付き証明書署名要求(CSR)のISEへのバインド

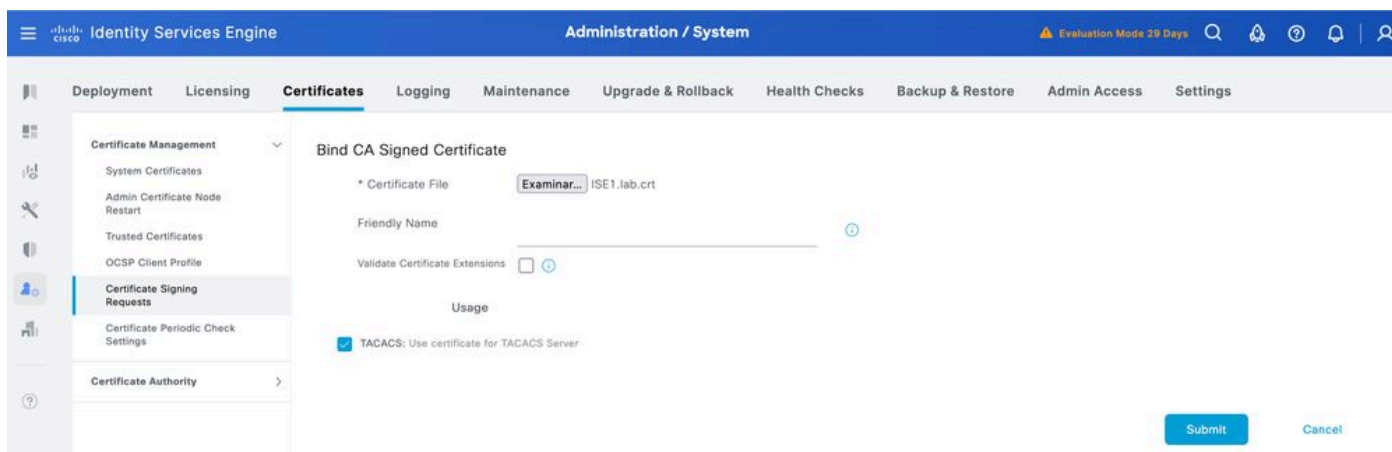
証明書署名要求(CSR)が署名されたら、署名付き証明書をISEにインストールできます。

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。

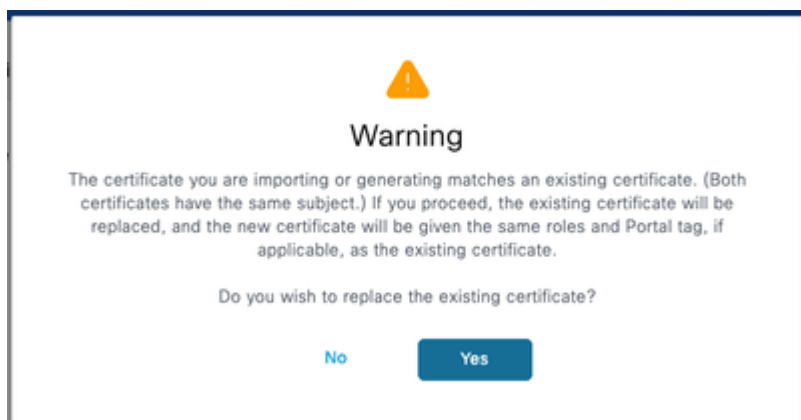
The screenshot shows the 'Certificate Signing Requests' page in the Cisco Identity Services Engine. The page title is 'Certificate Signing Requests'. Below the title is a button: 'Generate Certificate Signing Requests (CSR)'. A paragraph explains: 'A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.' Below this are action buttons: View, Export, Delete, and Bind Certificate. A table lists the requests with columns: Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, and Host.

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

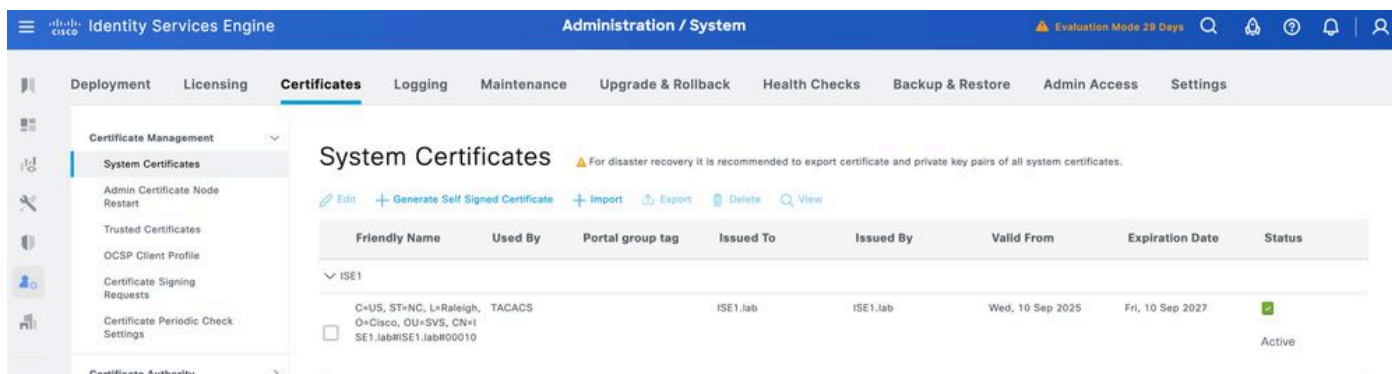
ステップ 2 署名付き証明書を選択し、Usage の下の TACACS チェックボックスが選択されたままになっていることを確認します。



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。



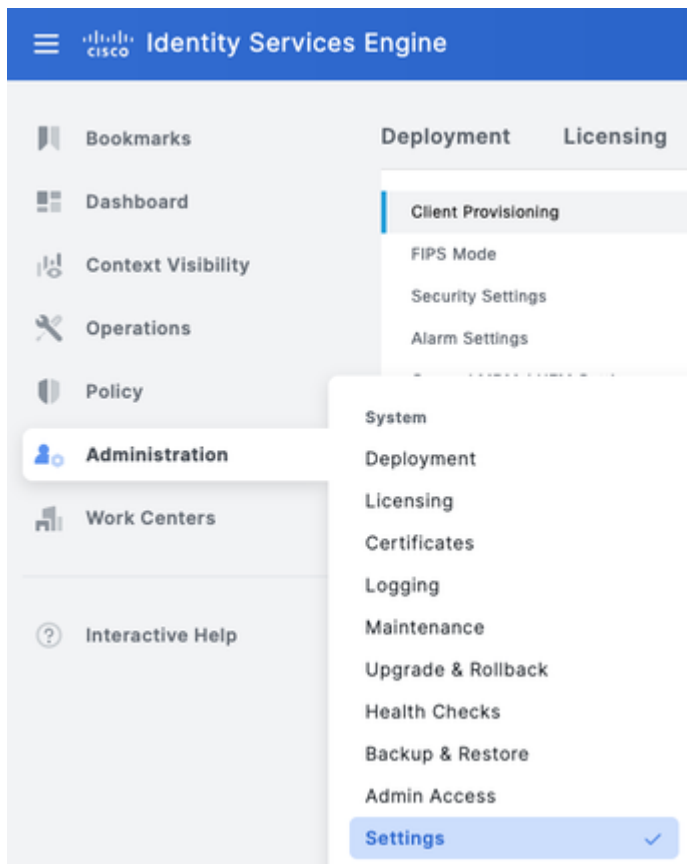
これで、証明書が正しくインストールされました。これは、「システム証明書」で確認できます。



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 TLS 1.3 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。

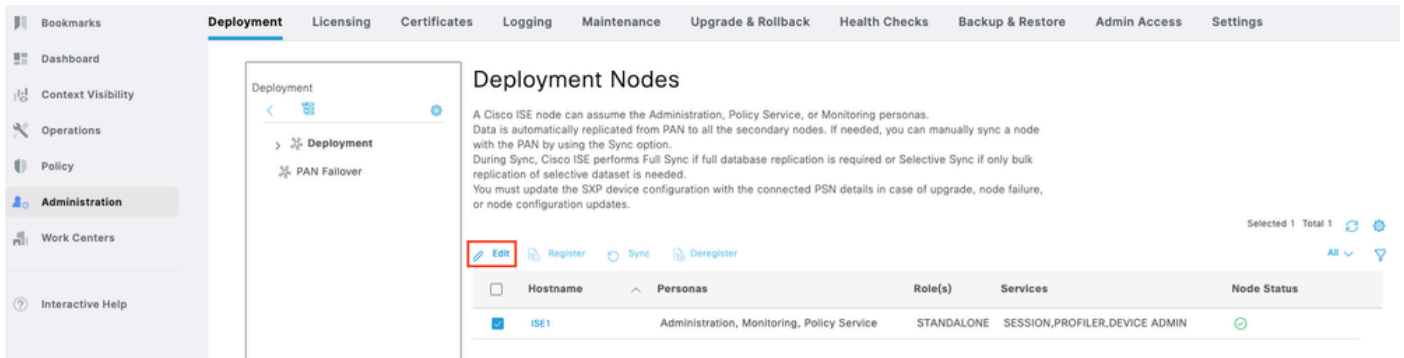


警告: TLS バージョンを変更すると、Cisco ISE アプリケーションサーバがすべての Cisco ISE 導入マシンで再起動します。

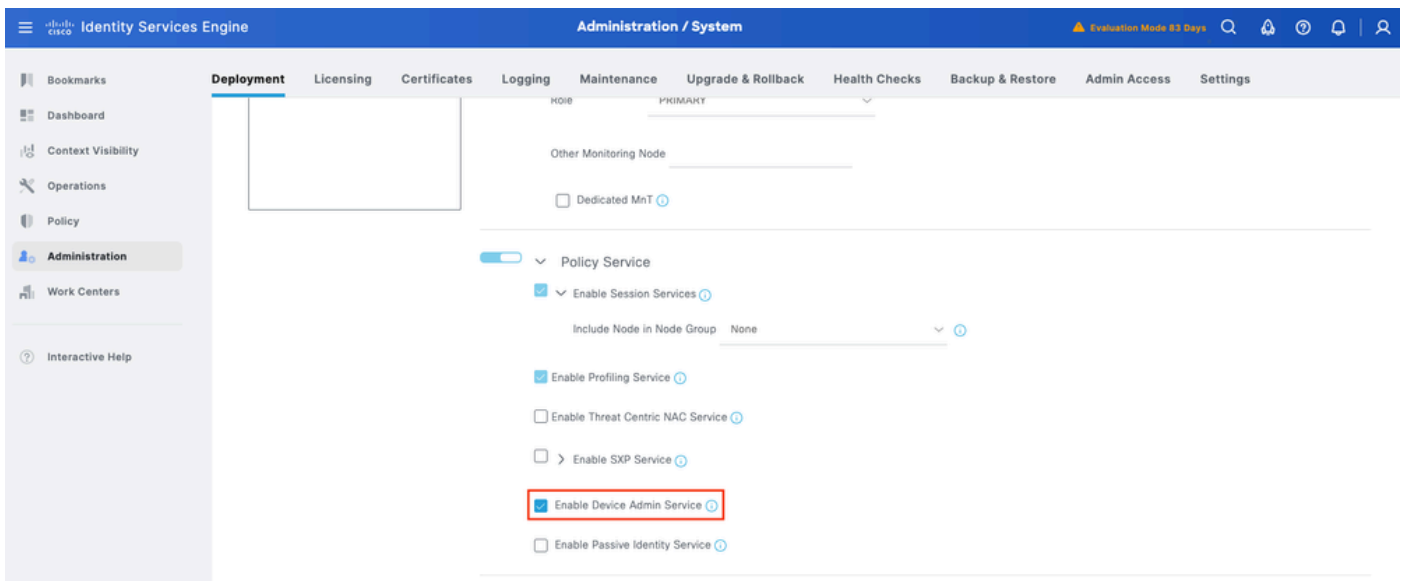
ISE でのデバイス管理の有効化

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。



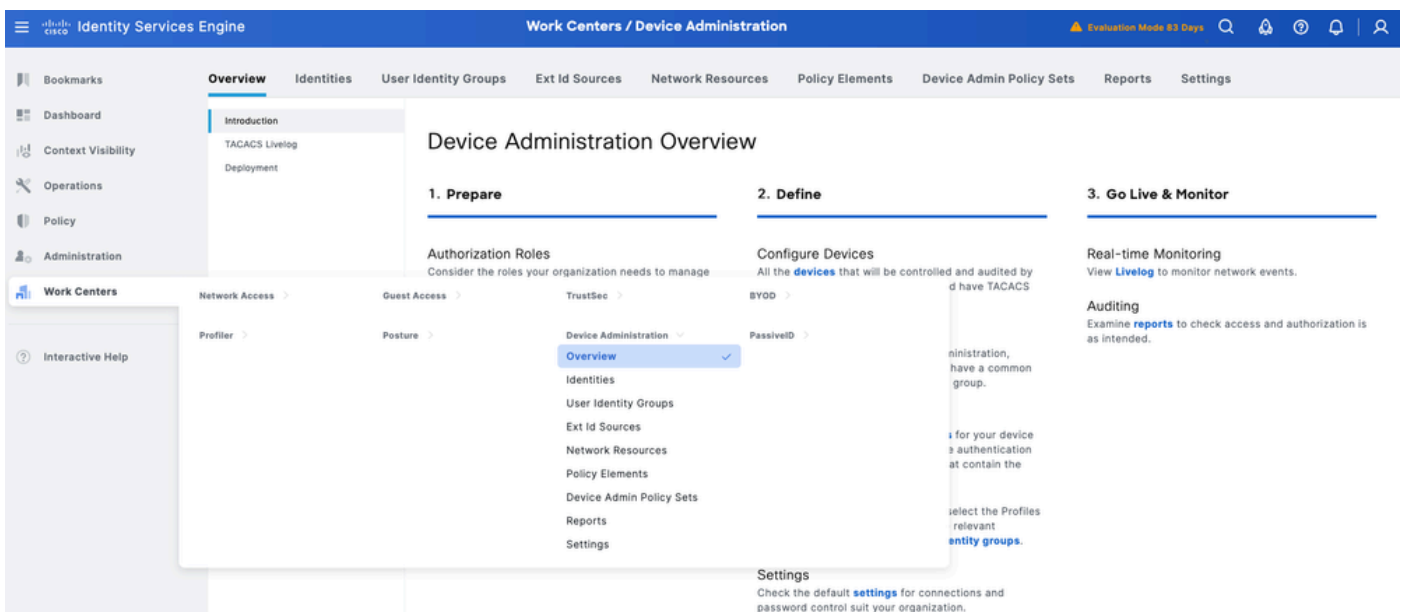
ステップ2 General Settingsで、下にスクロールしてEnable Device Admin Serviceの横にあるチェックボックスをオンにします。



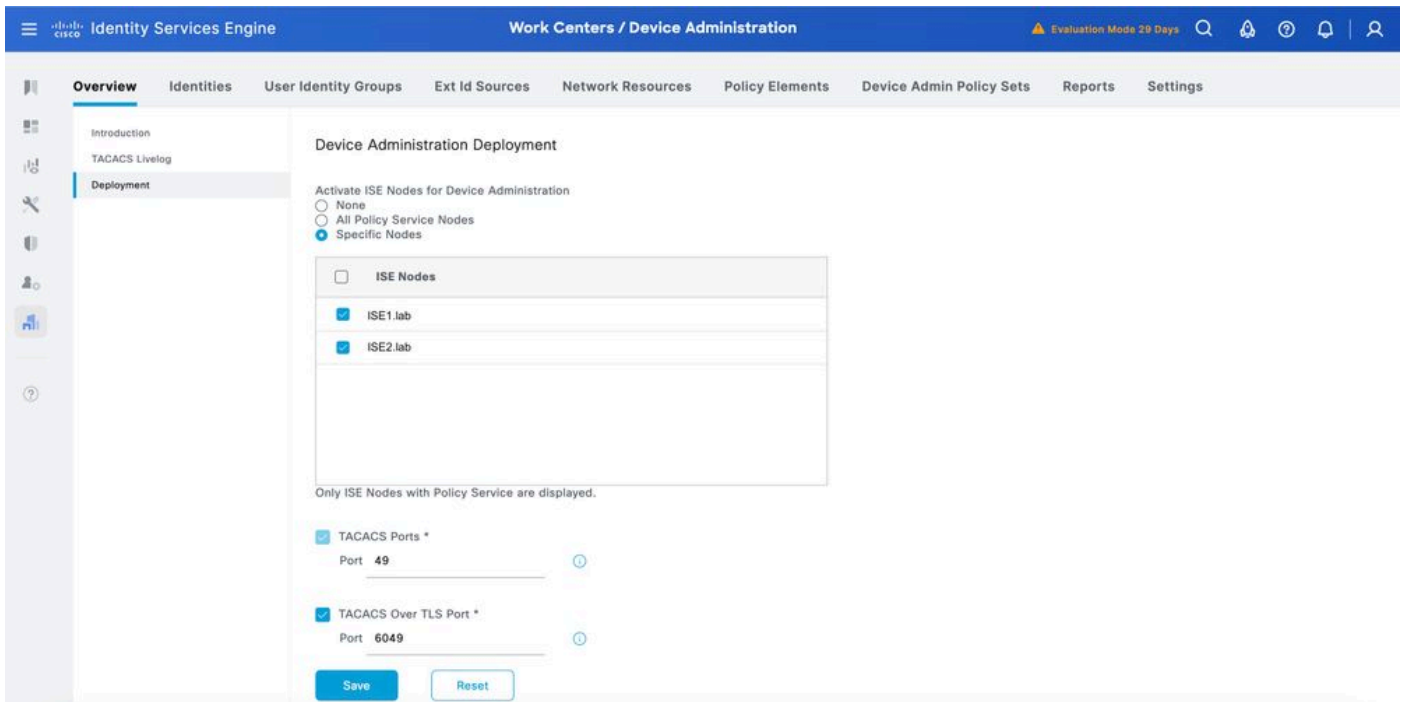
ステップ3 設定を保存します。Device Admin ServiceがISEで有効になりました。

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。



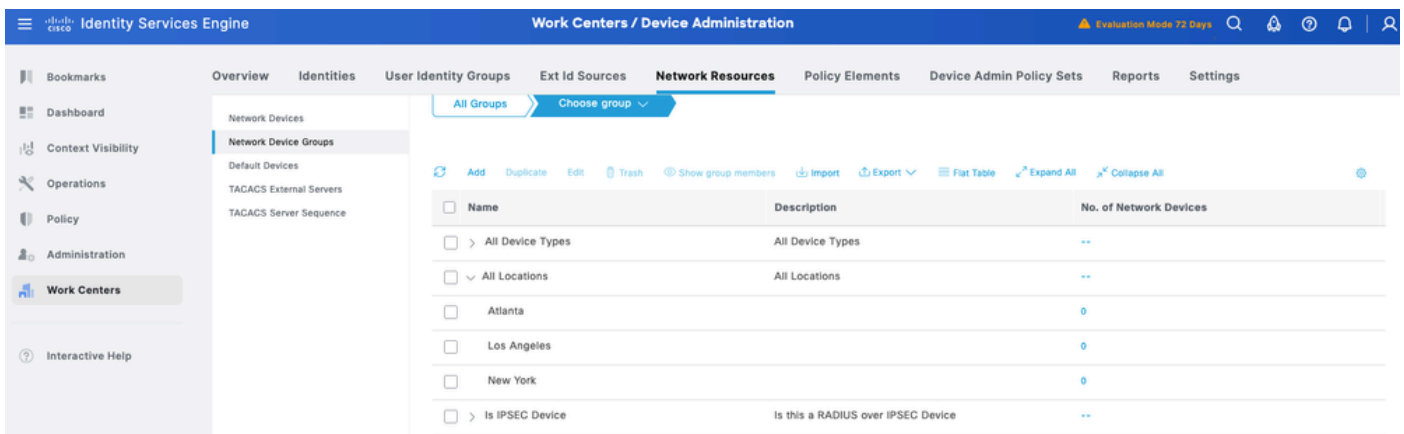
ステップ 3 デフォルトのポート 6049 をそのまま使用するか、TACACS over TLS に別の TCP ポートを指定して、Save をクリックします。

ISE の前提条件とその他のタスク

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

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。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main navigation menu on the left includes Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The top navigation bar shows 'Administration / Network Resources' and 'Evaluation Mode 83 Days'. The 'Network Devices' section is active, displaying a list with 'POD2IPN2'. The configuration details for this device are shown on the right:

- Name: POD2IPN2
- Description: (empty)
- IP Address: * IP: 10.225.253.177 / 32
- Device Profile: Cisco
- Model Name: C9364D-GX2A
- Software Version: 10.5(3t)
- Network Device Group: (empty)
- Location: Atlanta (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: NXOS (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。

The screenshot shows the 'TACACS over TLS Authentication Settings' configuration page for the device POD2IPN2. The settings are as follows:

- 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.



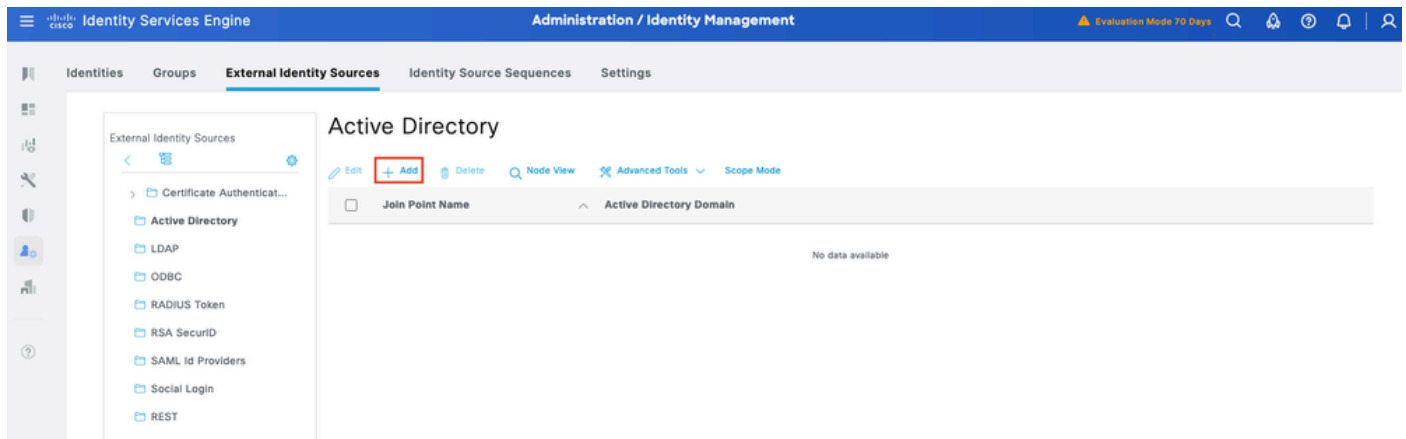
ヒント：デバイスにコマンドが送信されるたびにTCPセッションが再起動しないように、シングル接続モードを有効にすることを推奨します。

アイデンティティストアの設定

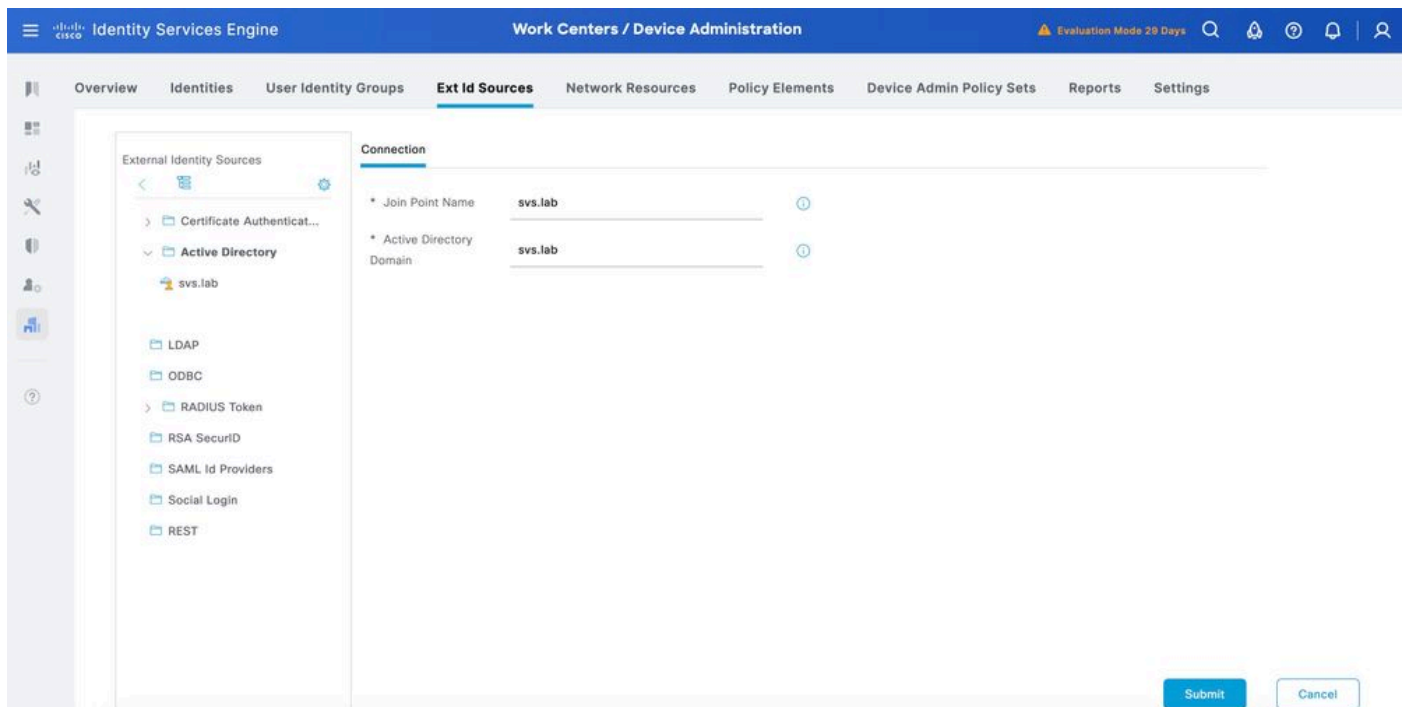
このセクションでは、デバイス管理者用のアイデンティティストアを定義します。これは、

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。

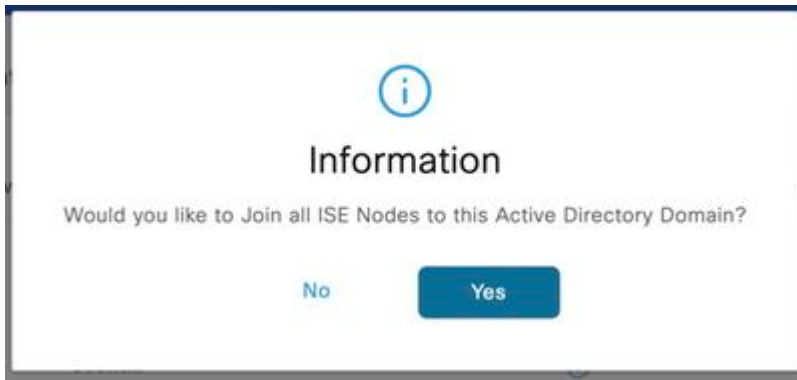
ステップ 1 Administration > Identity Management > External Identity Stores > Active Directoryの順に移動します。Addをクリックして、新しいADジョイントポイントを定義します。



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。



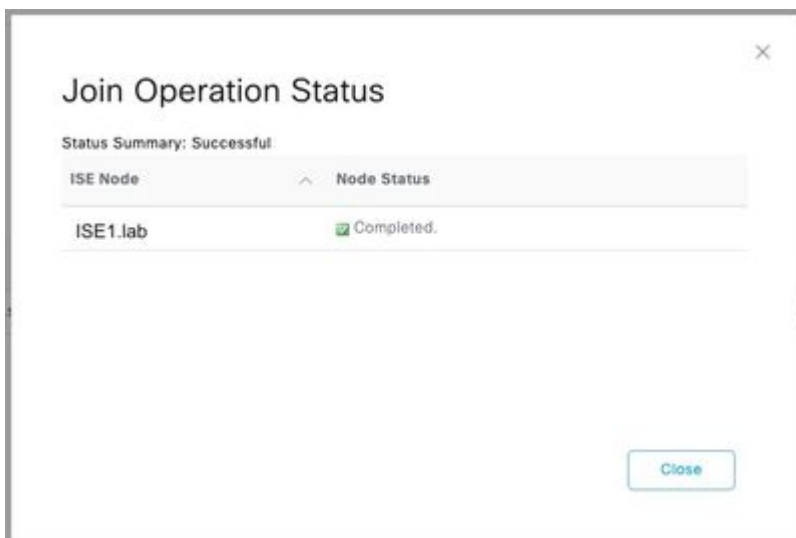
ステップ 3 「Would you like to Join all ISE Nodes to this Active Directory Domain?」というプロンプトが表示されたら、Yesをクリックします。



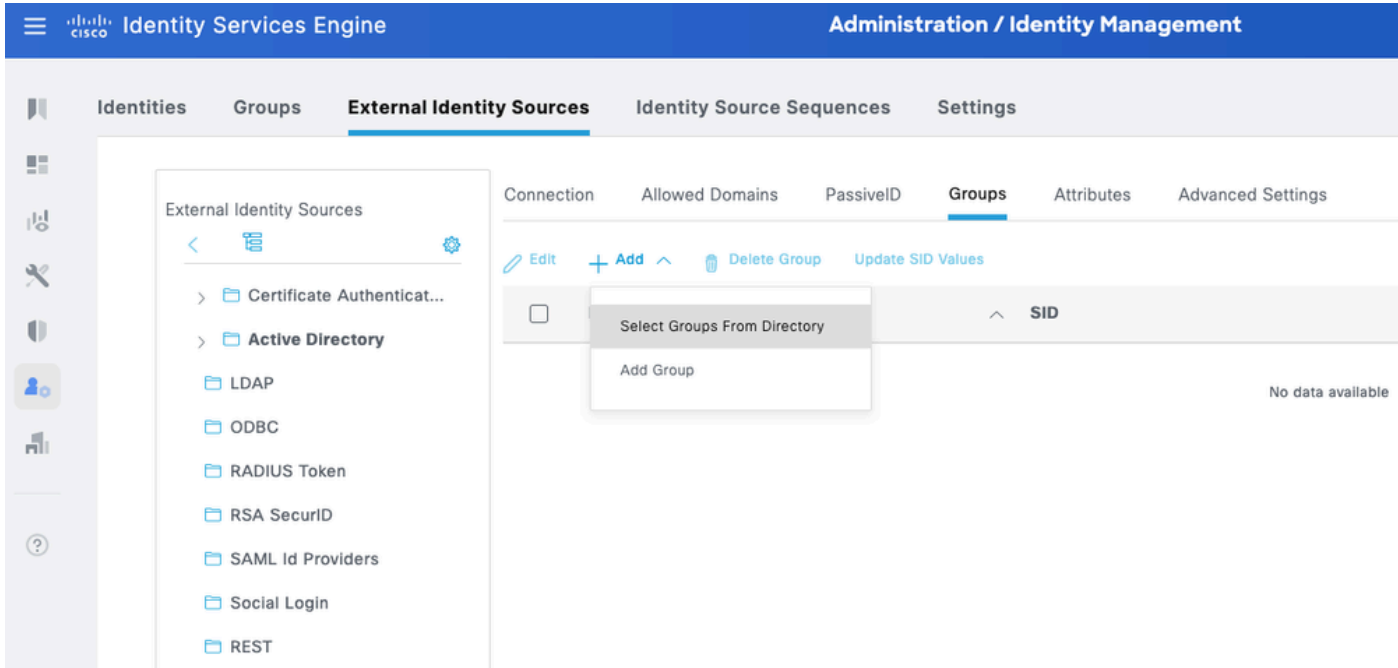
ステップ 4AD参加権限を持つクレデンシャルを入力し、ISEをADに参加させます。ステータスをチェックして、動作していることを確認します。

The dialog box is titled "Join Domain" and contains the following fields and options:

- AD User Name: administrator
- Password: masked with asterisks
- Specify Organizational Unit: unchecked checkbox
- Store Credentials: checked checkbox
- Buttons: Cancel and OK



ステップ 5Groups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。



Select Directory Groups

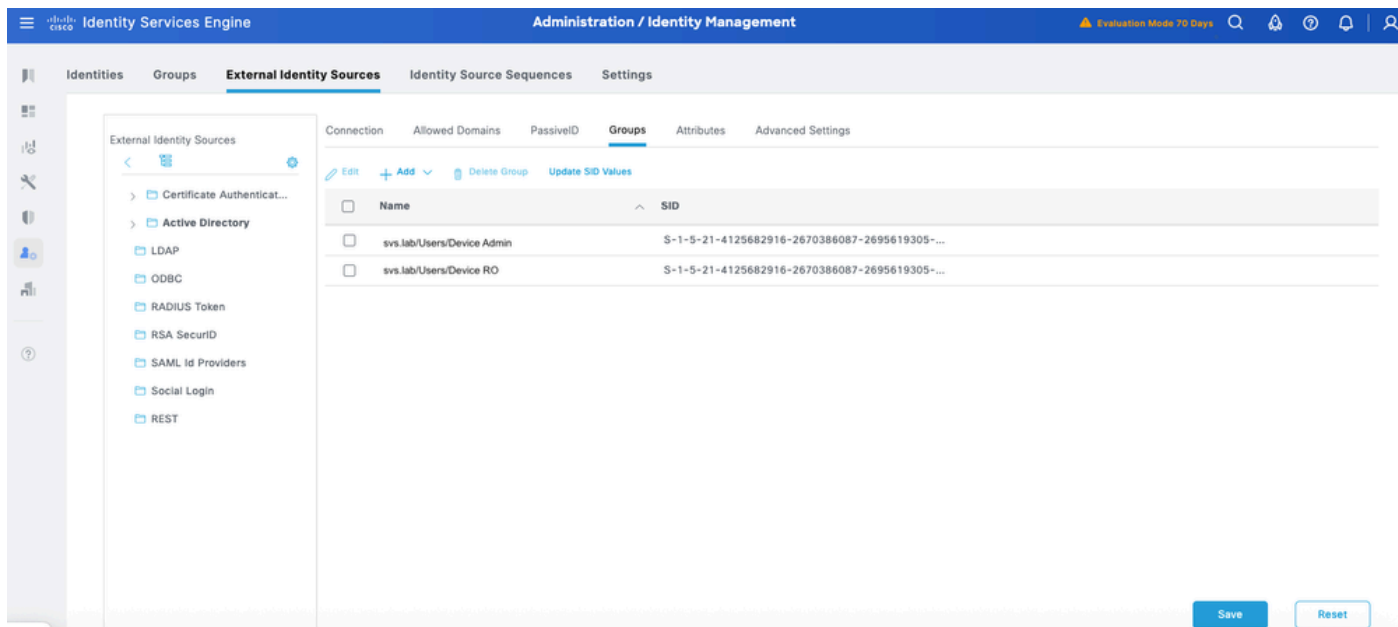
This dialog is used to select groups from the Directory.

Domain svcs.lab

Name SID
 Filter Filter Type
 Filter

[Retrieve Groups...](#) 2 Groups Retrieved.

<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	svcs.lab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
<input type="checkbox"/>	svcs.lab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



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。

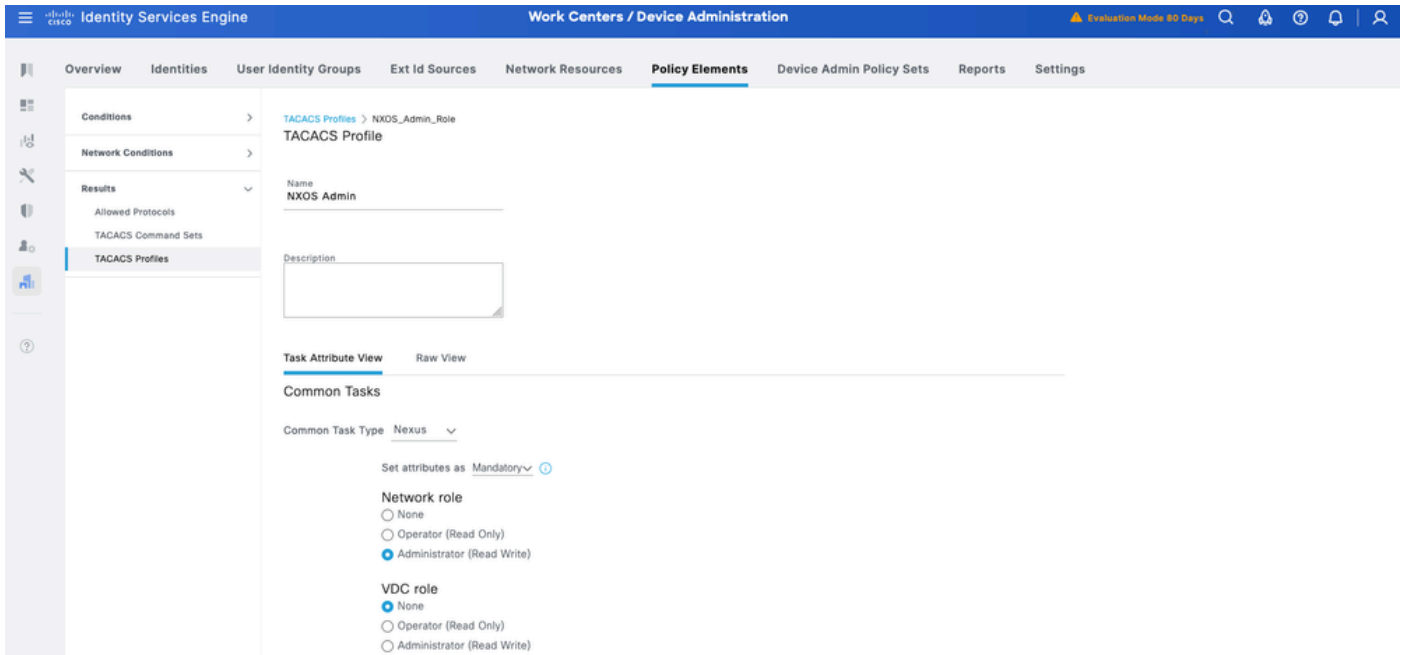
- network-admin : 事前定義されたネットワーク管理者ロールには、スイッチ上のすべてのコマンドに対する完全な読み取りおよび書き込みアクセス権があります。デバイス (Nexus 7000など) に複数のVDCがある場合にのみ、デフォルトの仮想デバイスコンテキスト (VDC)で使用可能です。NX-OS CLIコマンドshow cli syntax roles network-adminを使用して、このロールで使用可能な完全なコマンドリストを表示します。
- network-operator : 事前定義されたネットワーク管理者ロールには、スイッチ上のすべてのコマンドに対する完全な読み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



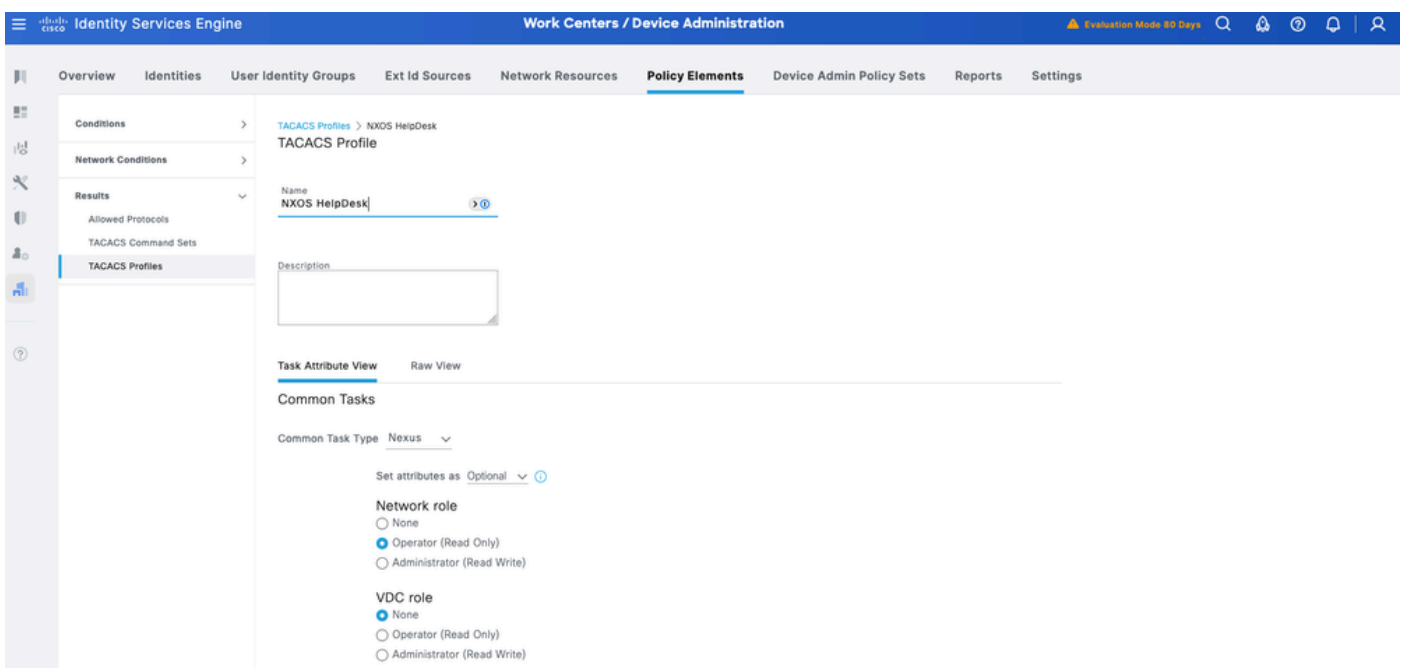
ステップ 3[Submit] をクリックしてプロファイルを保存します。

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 2Set 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。

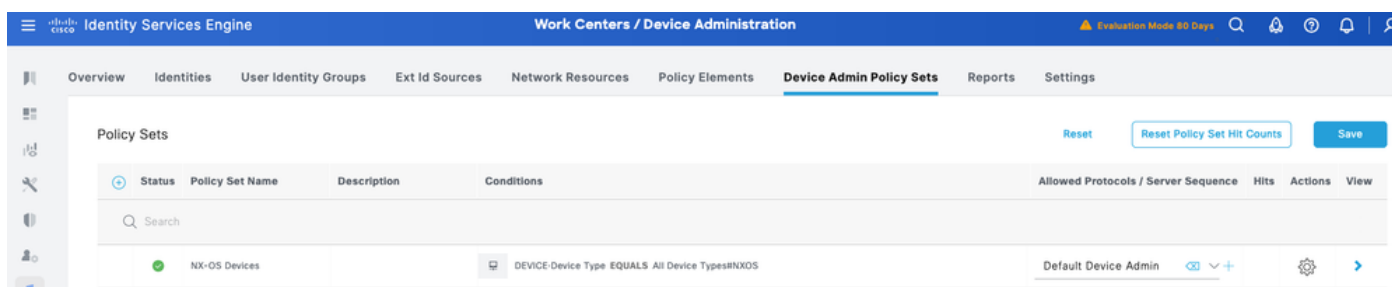


ステップ3:Saveをクリックして、プロファイルを保存します。

デバイス管理ポリシーセットの設定

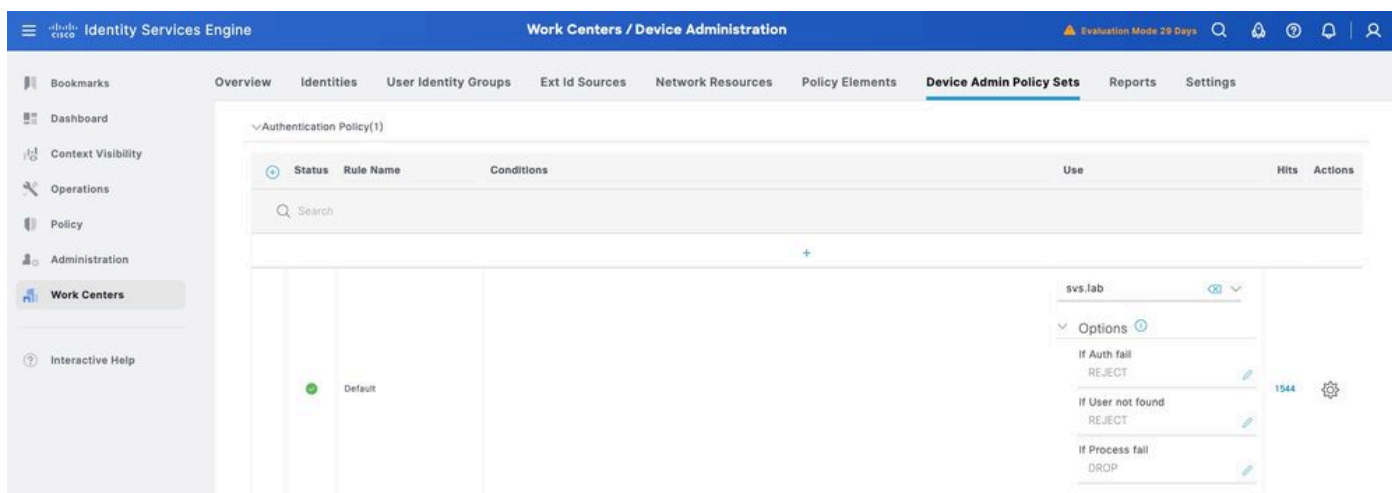
デバイス管理では、ポリシーセットはデフォルトで有効になっています。ポリシーセットは、デバイスタイプに基づいてポリシーを分割できるため、TACACSプロファイルの適用が容易になります。たとえば、Cisco IOSデバイスは特権レベルやコマンドセットを使用し、Cisco NX-OSデバイスはカスタム属性を使用します。

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。

Status	Rule Name	Conditions	Results			
			Command Sets	Shell Profiles	Hits	Actions
+	Authorization Rule RO	svs.lab-ExternalGroups EQUALS svS.lab/Users/Device RO	Select from list	NXOS HelpDe	0	
+	Authorization Rule RW	svs.lab-ExternalGroups EQUALS svS.lab/Users/Device Admin	Select from list	NXOS Admin	2	
+	Default		DenyAllCommands	Deny All Shell Profile	0	

TACACS+ over TLS用のCisco NX-OSの設定



注：詳細については、『NX-OSセキュリティ設定ガイド』(<https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/106x/configuration/security/cisco-nexus-9000-series-nx-os-security-configuration-guide-release-106x/m-configuring-tacacs.html>)を参照してください。

ソフトウェアバージョンと基本設定の確認

Nexus 9000スイッチでは、NX-OSリリース10.6(1)F以降でTACACS+ over TLS 1.3がサポートされています。現在のソフトウェアのバージョンがこれに一致していることを確認します。

```
<#root>
```

```
Software
```

```
BIOS: version 01.18
```

```
NXOS: version 10.6(1) [Feature Release]
```

```
Host NXOS: version 10.6(1)
```

```
BIOS compile time: 04/25/2025
```

```
NXOS image file is: bootflash:///nxos64-cs.10.6.1.F.bin
```

```
NXOS compile time: 7/31/2025 12:00:00 [08/12/2025 21:18:15]
```

```
NXOS boot mode: LXC
```



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
```

方法1：デバイスが生成したキーペア

この方法では、証明書管理にデバイス生成のキーペアを使用します。これには、デバイスでのキーの生成、CSR（証明書署名要求）の生成、およびCSRの署名後のデバイスへの署名付き証明書のインストール（信頼できるCA証明書のインストールなど）が含まれます。

CAで生成されたキーペア方式（PFXインストール方式）を使用する場合は、「方法2」を参照してください。

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 3CA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-----

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCMVVMxZAVBgnVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMdu1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDA0BgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTIxy9hpKZIKB86t2ZA3JX8CLsbCa13sA
z1XCoNX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QbnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFGpTV1MgTGFiiENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TFITVmAzcX8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOm7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgrU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDckzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

-----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(CSR)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:Cisco.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: FD026490P4T

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-----
```

```
MIIBtjCCARcCAQAwwTERMA8GA1UEAwIUE9EMk1QTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6Lzpk0hPAGE4jBveNHxYeIA7PfNwvJ7xTBWjDNX
/IYBm6E7Hd7q420mCe8Mef+bqJBDJ9wzpyEjhI21IIoXt4814nBxObkIWwYR5cZN
IiXtLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMk1QTjKHBArh/bEw
CgYIKoZIZj0EAWIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/441u1
+3H1y52vn4Rm4CGU3wkzXU3qG03YjhNjCXjhp3+uN2afff1Wf3ECQgC4bumHVs-fj
b5rwPIC5tvXS/A8upqIzqc0yt30hpaDD0TWzzvZY7qFf1C015p6pvUpHigqoZNg5
9xhNdM1CQSyk0g==
```

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

ステップ 5 CAでCSRに署名し、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
BhMCVVMxZmFzAVBgnVNBAGTdk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjM1ZTMRMiEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA3MTkxMDAwWhcNMjUwNTA3MTkxMDAwWjApMREwDwYDVQDDAhQ
T0QySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhpSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3D0n
ISOEjaUgihe3jzXicHE5uQhZbJH1xk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2FOZTAcBgNVHREBAf8EEjAQgghQ
T0QySVBOMocECuH9sTANBqkqkKiG9w0BAQsFAAOCAGANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msod0QK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShoHrZ01PUXNTyZidXpGd/yTrdQA15JzpW4pEudrbCJMZEETqoP
wD+40E8vKoYEgyW1DrpRZ0ZG1usZczuUHLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
1iToeYy2Q0cTesSZCKvRBv6Ewj5JuSLeMURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rou++ISACpH/PJ61Ln1VxhXombiS6
INoa0GvQONr1+1FT8ADIdZ/Ukd5Ubhc9bh/sYzf4MwtKk1wV016Hv7vGpSMYonD6
a271im+tJPyKneezQ60yKz1GqsL/Ta6J0dip/fEYp8UmRq9InDh23gDjqrojl7k
1R/bZpc+baMYXd/2pohMMSN0sKN3zNrJT1nuk5KCqFx//4P7mAoyZYiTiDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sg006Y6wIXyTP0UB3FWhD+GxtTkmEce
ZnAQbgxpgrg51hpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
1fKuuebdZkbwz72r70yyX/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 = F026490P4T
```

```
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)#
```

方法2:CAによって生成されたキーペア (PFX方式)

CSR方式ではなく、PKCS#12形式で直接、キー、デバイス、およびCA証明書をインポートする場合は、この方式を使用できます。

この方法は、証明書の管理における運用上のオーバーヘッドを削減できるため、証明書および鍵をPKI(Centralized Public Key Infrastructure)認証局から管理する場合に便利です。

トラストポイントの設定

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。

```
POD2IPN1(config)# crypto ca trustpoint svcs
```

ステップ 2 PKCS#12ファイル (PFXフォーマット) をブートフラッシュにコピーし、crypto ca importコマンドを使用してファイルをインポートします。



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



ヒント: bashシェルで次のコマンドを使用して、PKCS#12ファイルを確認します。

```
openssl pkcs12 -info -in <pxf file> -nodes  
file <pxf file> ---> should say data
```

```
<#root>
```

```
POD2IPN1(config)#
```

```
crypto ca import svcs pkcs12 bootflash:pod2ipn1-new.pfx
```

```
POD2IPN1#
```

```
POD2IPN1#
```

```
show crypto ca certificates svcs
```

```
Trustpoint: svcs  
certificate:
```

```
subject=C = US, ST = NC, L = RTP, O = Cisco, OU = SVS, CN = pod2ipn1, emailAddress = test@cisco.com
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=35BBC2517EEA3EF5
notBefore=May 20 20:16:00 2025 GMT
notAfter=May 20 20:16:00 2026 GMT
SHA1 Fingerprint=AA:4A:11:7A:97:B8:E4:B8:C6:F6:F0:94:29:F3:5F:AE:AB:95:6A:E3
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
```

ステップ 3方法1で説明されているように、TACACS、サーバグループ、およびAAAのTLS設定を行います。

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 2ISE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 4tacacs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
```

ステップ 6AAA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 3AAA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
```

証明書更新プロセス

このセクションでは、設定された証明書を置き換える必要がある場合、または証明書の有効期限が近づいている場合の、証明書の更新プロセスについて説明します。



注：更新時にトラストポイントをTACAC設定から削除する必要はありません。

ステップ 1：証明書の有効期間の確認

```
<#root>
```

```
POD2IPN2#
```

```
show crypto ca certificates
```

```
Trustpoint: KF_TP
```

```
certificate:
```

```
subject=CN = POD2IPN2.svs.lab
```

```
issuer=C = US, O = Keyfactor Command, OU = Certification Authorities, CN = Test  
Drive Sub CA G1
```

```
serial=09DD28B44BDA6FFA4D261926A4B54DD45C8B8F4E
```

```
notBefore=Jul 17 02:52:28 2025 GMT
```

```
notAfter=Jul 17 02:52:27 2026 GMT
```

```
SHA1 Fingerprint=AE:12:62:D4:73:BB:4B:77:B5:E2:B5:71:91:0B:38:AC:8F:42:F6:41
```

```
purposes: sslserver sslclient
```

```
<snip>
```

ステップ 2 信頼ポイントから証明書とキーペアを削除します。



注意：削除手順はこの順序で実行する必要があります。

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca trustpoint KF_TP
```

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

```
delete certificate force
```

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

```
no rsakeypair KF_TP
```

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

```
delete ca-certificate
```

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

```
POD2IPN2(config)#
```

```
no crypto key generate rsa label KF_TP exportable modulus 4096
```

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

```
show crypto ca certificate KF_TP
```

```
Trustpoint: KF_TP
```

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

ステップ 3 PFXファイルから新しい証明書をインポートします。

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca import
```

```
pkcs12 bootflash:
```

ステップ 4 新しい証明書の確認

<#root>

POD2IPN2(config)#

show crypto ca certificates

Trustpoint: KF_TP

certificate:

subject=C = us, ST = nc, L = rtp, O = cisco, OU = svcs, CN = pod2ipn2.svs.lab
issuer=C = US, O = Keyfactor Command, OU = Certification Authorities, CN = Test
Drive Sub CA G1
serial=6D6171F6DB2DD08C613937887E631D5CD35EDA18

notBefore=Aug 14 13:52:52 2025 GMT

notAfter=Aug 14 13:52:51 2026 GMT

SHA1 Fingerprint=4E:8A:CA:C7:E4:9D:05:83:6A:A7:27:FD:10:02:75:35:3F:05:37:96
purposes: sslserver sslclient

<snip>

ステップ 5 AAA認証のテスト

<#root>

POD2IPN2#

test aaa group

user has been authenticated

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

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...
```

トラブルシューティング

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_addr: 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

```



注意:Bashシェルを有効にする必要があります。また、ユーザはbash権限を持っている必要があります。

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。

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Di...
May 15, 2025 07:39:57.081 PM	✓	🔒	Admin-ro	Authorization	Test NXOS >> Default	Test NXOS >> Authorization Rule RO	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:57.061 PM	✓	🔒	Admin-ro	Authentication	Test NXOS >> Default	Test NXOS >> Authorization Rule RW	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.462 PM	✓	🔒	pamemart	Authorization	Test NXOS >> Default	Test NXOS >> Authorization Rule RW	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.443 PM	✓	🔒	pamemart	Authentication	Test NXOS >> Default	Test NXOS >> Authorization Rule RW	ISE1	POD2IPN1	10.225.253.1

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、アカウントिंग(AAA)レポートを取得します。

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	Failure
Today			Identity	Authentication Policy	ISE Node	Network Device Name	Network Device IP	Failure
2025-05-15 19:39:57.061	Success		Admin-ro	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:39:54.443	Success		pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:39:43.001	Success		pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 19:35:39.809	Success		pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 18:49:11.209	Success		pamemart	Test NXOS >> Default	ISE1	POD2IPN1	10.225.253.176	
2025-05-15 18:49:10.303	Success		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。