

ISEを使用したCatalyst Center外部認証TACACSの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[Cisco Identity Services Engine \(ISE\)](#)

[TACACS+サービスのライセンスと有効化](#)

[管理者ユーザの作成とネットワークデバイスの追加](#)

[TACACS+プロファイルの設定](#)

[TACACS+ポリシーの設定](#)

[Cisco Catalystセンター](#)

[ISE/AAAサーバの設定](#)

[外部認証をイネーブルにして設定します。](#)

[確認](#)

[トラブルシューティング](#)

[1. 属性の設定ミス](#)

[2. 共有秘密の不一致](#)

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)をCatalyst Centerと統合してTACACS+認証を有効にするために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ISEとCisco Catalyst Centerの両方への管理者アクセス
- AAA (認証、認可、アカウントिंग) の概念の基本的な知識。
- TACACS+プロトコルに関する実務知識
- Catalyst CenterとISEサーバ間のネットワーク接続。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- Cisco Catalyst Centerバージョン2.3.7.x
- Cisco Identity Services Engine(ISE)バージョン3.x (以降)
- 外部ユーザ認証用のTACACS+プロトコル

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。

背景説明

この統合により、外部ユーザはCatalyst Centerにログインして、管理アクセスと管理を行うことができます。

設定

Cisco Identity Services Engine (ISE)

TACACS+サービスのライセンスと有効化

ISEでTACACS+の設定を開始する前に、正しいライセンスがインストールされ、機能が有効になっていることを確認する必要があります。

1. Cisco Smart Software Manageポータルまたは[Cisco License Central](#)ポータルで、PIDライセンスL-ISE-TACACS-ND=があることを確認します。

ISEライセンシングポータルでデバイス管理を有効にします。

- デバイスマネージャライセンス(PID:L-ISE-TACACS-ND=)により、ポリシーサービスノード(PSN)でTACACS+サービスが有効になります。
- 次のとおりに移動します。

Administration > System > Licensing

- TierオプションでDevice Adminのボックスをオンにします。

Tier Essential Advantage Premier Device Admin

Virtual Appliance ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

Reset

Update

デバイス管理者

<input type="checkbox"/>	Premier	Enabled	Released Entitlement	0	-	Dec 27, 2024 18:16:00 PM
<input type="checkbox"/>	Device Admin	Enabled	In Compliance	1	-	Sep 11, 2025 20:53:12 PM
Virtual Appliance						
	ISE VM License	Enabled	In Compliance	1	-	Sep 11, 2025 20:53:12 PM

ライセンスデバイス管理者

3. TACACS+サービスを実行するISEノードでDevice Admin Serviceを有効にします。

- 次のとおりに移動します。

Administration > System > Deployment > ノードの選択

- Enable Device Admin Serviceオプションにチェックマークを付けます。

Deployment Nodes List > ise-mxc1

Edit Node

General Settings Profiling Configuration

Hostname: ise-mxc1
FQDN: ise-mxc1.cisco.com
IP Address: 10.88.244.180
Node Type: Identity Services Engine (ISE)

Role: STANDALONE [Make Primary](#)

Administration

> Monitoring

Policy Service

- > Enable Session Services ⓘ
Include Node in Node Group: None ⓘ
- Enable Profiling Service ⓘ
- Enable Threat Centric NAC Service ⓘ
- > Enable SXP Service ⓘ
- Enable Device Admin Service ⓘ
- Enable Passive Identity Service ⓘ

> pxGrid ⓘ

[デバイス管理サービスを有効にする (Enable Device Admin Service)]

管理者ユーザの作成とネットワークデバイスの追加

1. 管理者ユーザを作成します。

- このユーザアカウントは、ISE認証でCatalyst Center UIにログインするために使用されます。
- 次のとおりに移動します。
Work Centers > Network Access > Identity > Network Access User
- 新しいユーザを追加します(catc-userなど)。
- ユーザがすでに存在する場合は、次の手順に進みます。

2. ネットワークデバイスを作成します。

- 次のとおりに移動します。

ワークセンター>ネットワークアクセス>アイデンティティ>ネットワークリソース

- Catalyst CenterのIPアドレスを追加するか、Catalyst Center IPがあるサブネットを定義します。
- デバイスがすでに存在する場合は、次のパラメータが含まれていることを確認します。
 - TACACS Authentication Settingsが有効になっている。
 - 共有秘密が設定され、認識されている（後でCatalyst Centerで必要になるため、この値を保存します）。

Cisco ISE Work Centers - Network Access

Overview Identities Id Groups Ext Id Sources **Network Resources** Policy Elements Policy Sets Troubleshoot Reports Settings Dictionaries

Network Devices

Network Devices List > Catalyst-Center_6

Network Devices

Name Catalyst-Center_6

Description _____

IP Address * IP: 10.88.244.160 / 32

Device Profile Cisco

Model Name _____

Software Version _____

Network Device Group

Location All Locations [Set To Default](#)

IPSEC No [Set To Default](#)

Device Type All Device Types [Set To Default](#)

DNAC DNAC Devices [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret [Show](#) [Retire](#)

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

TACACS認証設定

TACACS+プロファイルの設定

1. 新しいTACACS+プロファイルを作成します。

- 次のとおりに移動します。

ワークセンター>デバイス管理>ポリシー要素>結果> TACACSプロファイル

- プロファイル名を追加します。
- 次の手順で、カスタム属性を追加します。
 - タイプ：必須

- 名前 : cisco-av-pair
- 値 : Role=SUPER-ADMIN-ROLE
- プロファイルを保存します。

Cisco ISE Work Centers - Device Administration

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

TACACS Profiles > CatC_TACACS_Profile
TACACS Profile

Name
CatC_TACACS_Profile

Description
Catalyst Center External Authentication

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege (Select 0 to 15)

Maximum Privilege (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

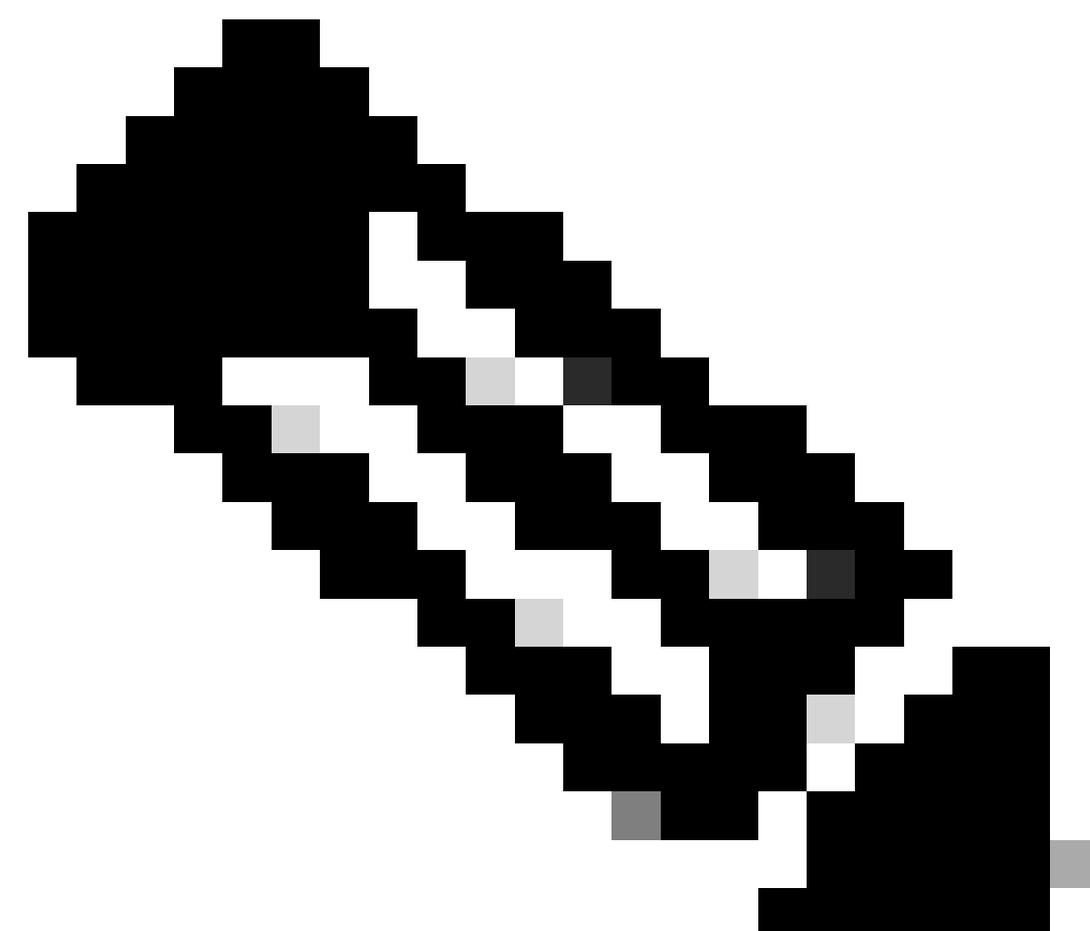
Custom Attributes

Add Trash Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	cisco-av-pair	Role=SUPER-ADMIN-ROLE

Cancel Save

TACACS+ プロファイル



注: Cisco Catalyst Centerは、アクセスコントロールのために外部の認証、許可、アカウントリング(AAA)サーバをサポートします。外部ユーザの認証と許可に外部サーバを使用している場合は、Cisco Catalyst Centerで外部認証を有効にできます。デフォルトのAAA属性設定は、デフォルトのユーザプロファイル属性と一致します。

TACACSプロトコルのデフォルトAAA属性値はcisco-av-pairです。

RADIUSプロトコルのデフォルトのAAA属性値はCisco-AVPairです。

変更が必要なのは、AAAサーバのユーザプロファイルにカスタム属性がある場合だけです。AAAサーバでは、AAA属性値の形式はRole=role1です。Cisco Identity Services Engine(Cisco ISE)サーバで、RADIUSまたはTACACSプロファイルを設定するときに、ユーザはAAA属性としてcisco av-pairを選択または入力できます。

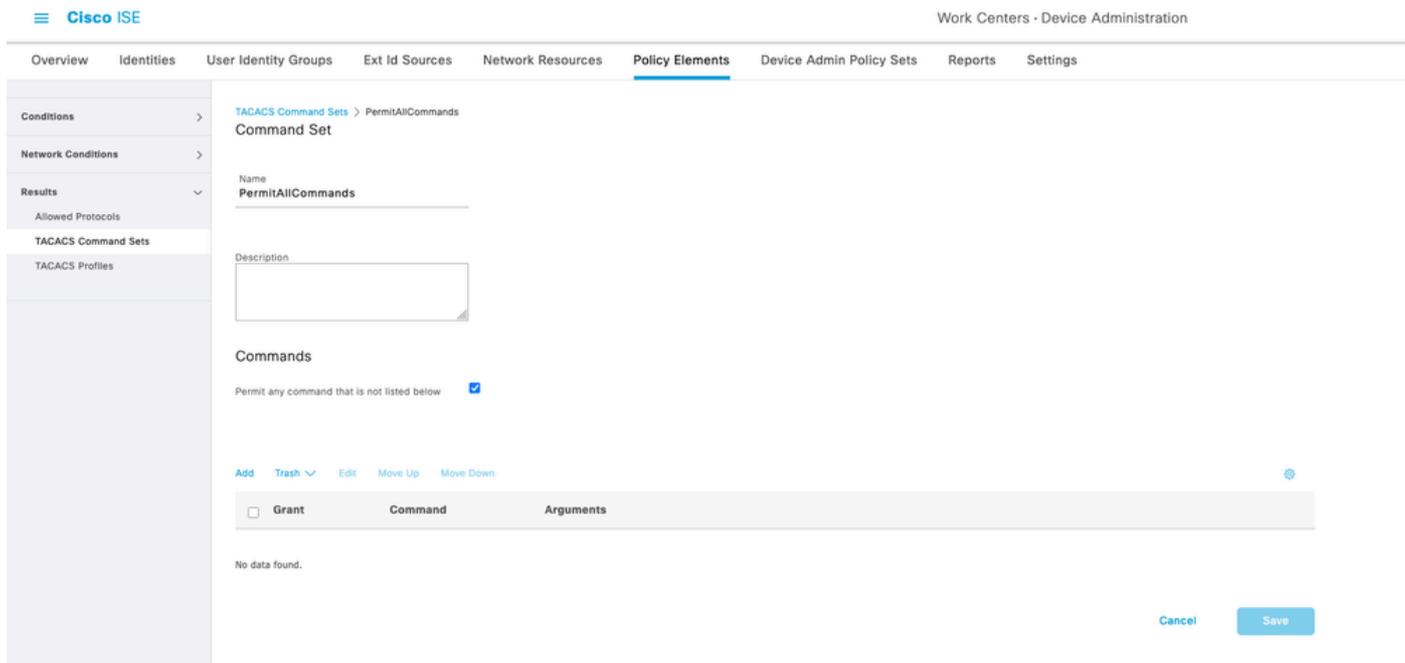
たとえば、AAA属性を手動で選択して、cisco-av-pair=Role=SUPER-ADMIN-ROLEまたはCisco-AVPair=Role=SUPER-ADMIN-ROLEとして設定できます。

2. TACACS+コマンドセットを作成します。

- 次のとおりに移動します。

ワークセンター>デバイス管理>ポリシー要素>結果> TACACSコマンドセット

- 名前を追加します。
- Permit any command that is not listed belowオプションにチェックマークを付けます。
- コマンドセットを保存します。



TACACSコマンドセット

TACACS+ポリシーの設定

1. 新しいTACACS+ポリシーセットを作成します。

- 次のとおりに移動します。

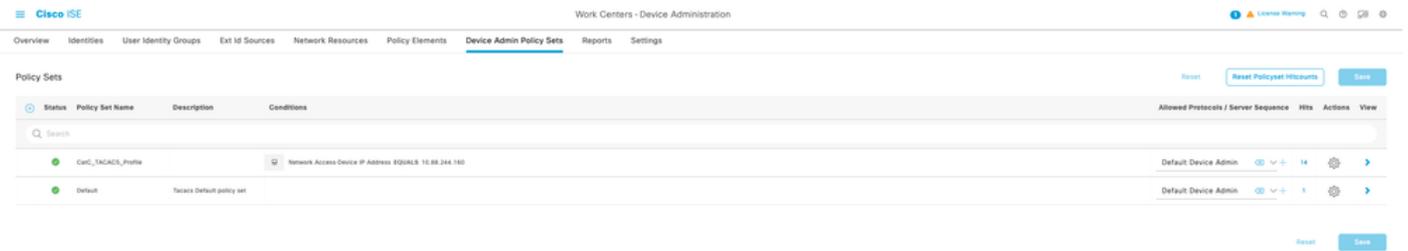
ワークセンター>デバイス管理>デバイス管理ポリシーセット

- ポリシーセットの名前を追加します。
- 条件を設定します。
 - この例では、条件はCatalyst CenterのIPアドレスと一致します。



Catalyst CenterのIPアドレス

1.3 Allowed Protocols / Server SequenceでDefault Device Adminを選択します。

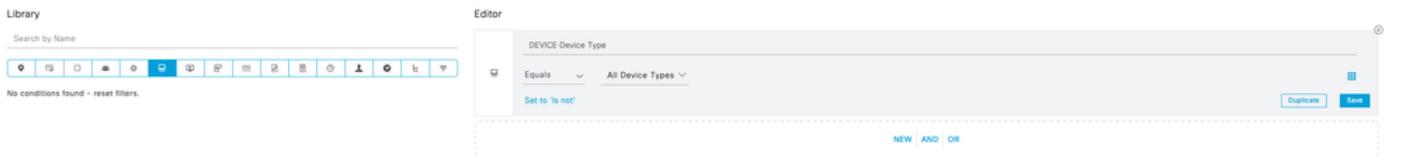


Default Device Adminの選択

2. ポリシーセットを設定します。

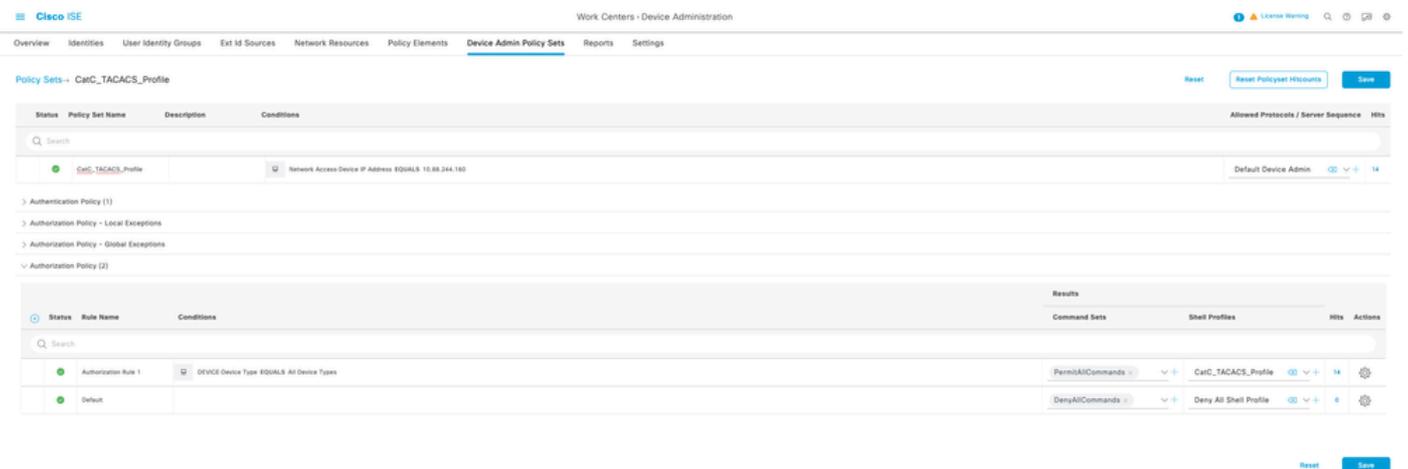
- 右側の矢印(>)をクリックして、ポリシーセットを展開および設定します。
- Authorization Policyの下に新しいRuleを追加します。
- 新しいルールを次のように設定します。
 - 名前：わかりやすいルール名を入力します。
 - 条件：この例では、条件はすべてのデバイスタイプに一致しました。

Conditions Studio



すべてのデバイスタイプ

- Command Set:以前に作成したTACACS+コマンドセットを選択します。
- Shell Profile:以前に作成したTACACS+プロファイルを選択します。



TACACS+コマンドセット

Cisco Catalystセンター

ISE/AAAサーバの設定

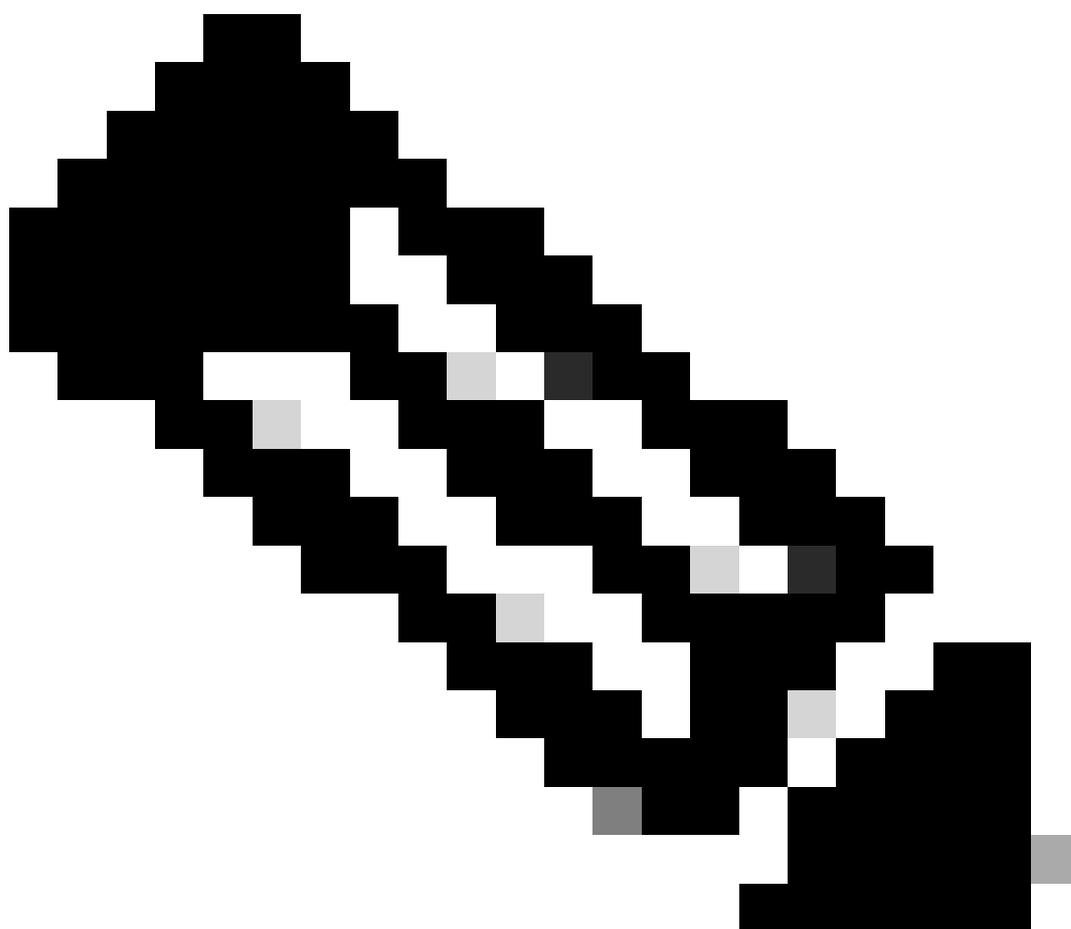
1. Catalyst Center Webインターフェイスにログインします。

- 次のとおりに移動します。

メインメニュー>システム>設定>外部サービス>認証およびポリシーサーバ

2. 新しいサーバを追加します。ISEまたはAAAのいずれかを選択できます。

- このデモでは、AAA serverオプションを使用します。
-



注:Catalyst Centerクラスタには、ISEクラスタを1つだけ設定できます。

3. 次のオプションを設定して保存します。

- aaaサーバのIPアドレスを入力します。

- 共有秘密 (Cisco ISEネットワークリソースで設定されているものと同じ秘密) を追加します。
- Advanced SettingsをOnに切り替えます。
- TACACSオプションをチェックします。

Add AAA server ×

Server IP Address*

10.88.244.180

Shared Secret*

.....

[SHOW](#)



Advanced Settings

Protocol

RADIUS TACACS

Enable KeyWrap

Authentication Port*

1812

Accounting Port*

1813

Port

49

Retries*

3

Timeout (seconds)*

4

認証サーバとポリシーサーバ

IP Address	Protocol	Type	Status	Actions
192.168.31.228	RADIUS	ISE	INACTIVE	—
10.88.244.180	RADIUS_TACACS	AAA	ACTIVE	—

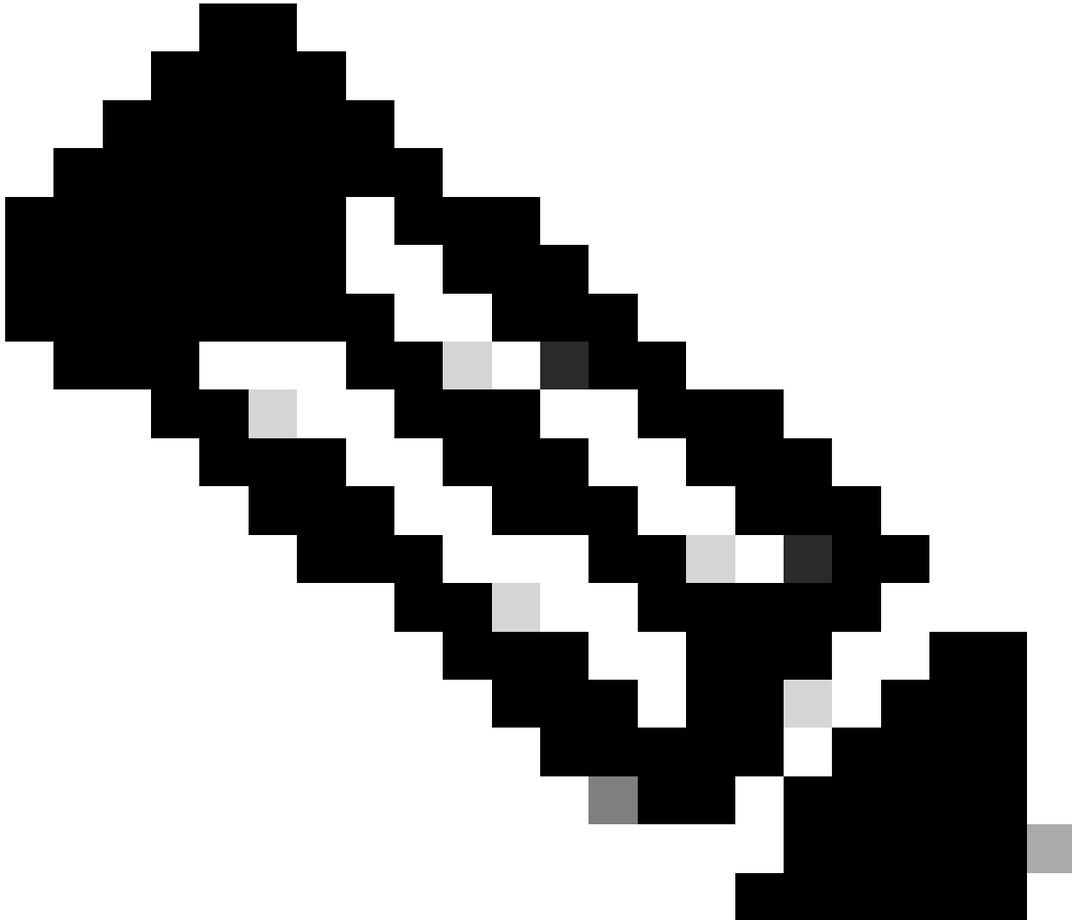
高度な設定

外部認証をイネーブルにして設定します。

1. 外部認証ページに移動します。

メインメニュー>システム>ユーザとロール>外部認証

2. AAA属性cisco-av-pairを追加し、Updateをクリックして変更を保存します。



注:TACACS+のデフォルト属性はすでにcisco-av-pairであるため、この手順は必須ではありませんが、明示的に設定することがベストプラクティスであると考えられます。

3. Primary AAA Serverの下で、以前に設定したAAA serverを選択します。

- View Advanced Settingsをクリックして、追加のオプションを表示します。
- TACACS+オプションを選択します。
- Cisco ISEのネットワークリソースに設定されている共有秘密を入力します。

- Updateをクリックして変更を保存します。

4. 「外部ユーザー」チェックボックスを有効にします。

- この操作により、設定が自動的に保存されます。

The screenshot shows the 'External Authentication' configuration page in Cisco Catalyst Center. The page is titled 'External Authentication' and includes a navigation sidebar on the left with options like 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area contains instructions and configuration fields. The 'AAA Attribute' field is set to 'Cisco-AI-PAI'. The 'AAA Server(s)' section shows two servers, both with the address '10.88.244.180'. The 'Protocol' is set to 'TACACS'. A 'Success' message is visible in the bottom right corner, indicating that the external authentication settings were saved successfully.

外部認証

確認

1. 新しいブラウザセッションを開くか、Incognitoモードを使用して、Cisco ISEで設定したユーザーアカウントでCatalyst Center Webページにログインします。
2. Catalyst Centerから、ログインが成功したことを確認します。



ログインISEを使用したCatalyst Center外部認証TACACSの設定

3. Cisco ISEで、ログを検証します。

Operations > TACACS > Live Logs

- 認証ステータス：成功
- 認証ステータス：成功

Live Logs

Refresh Never Show Latest 20 records Within Last 3 hours Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.851...			isa01-user	Authentication	CatC_TACACS_Profile >> Authn...	CatC_TACACS_Profile >> Authori...	isa-mac1	Catalyst-Centr...	10.88.244.160	Device Type680 D...	LocationM&M Locat...	console		10.189.17.203	Matched Command	CatC_TACACS_M...
Sep 12, 2025 12:12:20.798...			isa01-user	Authentication	CatC_TACACS_Profile >> Default		isa-mac1	Catalyst-Centr...	10.88.244.160	Device Type680 D...	LocationM&M Locat...	console		10.189.17.203		

Last Updated: Thu Sep 11 2025 18:14:58 GMT-0800 (Central Standard Time) Records Shown: 2

ライブログ

4. Authorization Detailsで、次の出力と比較します。

- メッセージテキスト：デバイス管理：セッションの承認に成功しました
- すべての応答属性：cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No, DNAC#DNAC Devices, Location#All Locations, Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes	
All Response Attributes	cisco-av-pair=Role=SUPER-ADMIN-ROLE

cisco-av-pair=Role=SUPER-ADMIN-ROLE

トラブルシューティング

統合中に発生する可能性のある一般的な問題と、その特定方法を次に示します。

1. 属性の設定ミス

Catalyst Centerでの症状：無効なログインクレデンシャル



Cisco Catalyst Center

The bridge to possible

 Invalid Login Credentials

Username

catc-user

Password

.....

[SHOW](#)

Log In

属性の設定ミス

- Cisco ISEでの症状 (TACACSログ) :

- 。 認証：合格
- 。 許可：合格

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:25.861...	■		cat0-user	Authorization	CatC_TACACS_Profile --> Authoriz...	CatC_TACACS_Profile --> Authoriz...	isa-mst1	Catalyst-Center_8	10.88.244.180	Device TypeMst1 G...	LocationMst1 Locat...	console		10.188.17.203		CatC_TACACS_Pt...
Sep 12, 2025 12:12:26.788...	■		cat0-user	Authentication	CatC_TACACS_Profile --> Default		isa-mst1	Catalyst-Center_8	10.88.244.180	Device TypeMst1 G...	LocationMst1 Locat...	console		10.188.17.203		

属性の設定ミス

- 考えられる原因:
 - 。 属性値にスペースが存在します。

例：

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

属性の設定ミス

- 属性が誤って設定されており、Role=キーワードが欠落している。

例：

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No, DNAC#DNAC Devices, Location#All Locations, Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

属性の設定ミス

2. 共有秘密の不一致

- 症状:Catalyst CenterとCisco ISEの間の認証パッケージが失敗します。

- 原因：ISEのネットワークリソースに設定されている共有秘密が、Catalyst Center > External Authenticationページで設定されている共有秘密と一致しない。

検証方法:

- ISEのネットワークリソース設定を確認します。
- 共有秘密を、Catalyst Center > External Authenticationの設定と比較します。

例：

Authentication Details	
Generated Time	2025-09-11 18:22:24.078000 +00:00
Logged Time	2025-09-11 18:22:24.078
Epoch Time (sec)	1757614944
ISE Node	ise-mxc1
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Resolution	
Root Cause	
Username	
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No, DNAC#DNAC Devices, Location#All Locations, Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	
Remote Address	

共有秘密の不一致

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。