

Secure Firewall Chassis Manager(FCM)用のISE Radius認証の設定

内容

はじめに

このドキュメントでは、ISEを使用したSecure Firewall Chassis Manager(SFM)のRADIUS許可/認証アクセスを設定する方法のプロセス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。

- Secure Firewall Chassis Manager(FCM)
- Cisco Identity Services Engine (ISE)
- RADIUS 認証

使用するコンポーネント

- Cisco Firepower 4110セキュリティアプライアンスFXOS v2.12
- Cisco Identity Services Engine(ISE)v3.2パッチ4

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。

設定

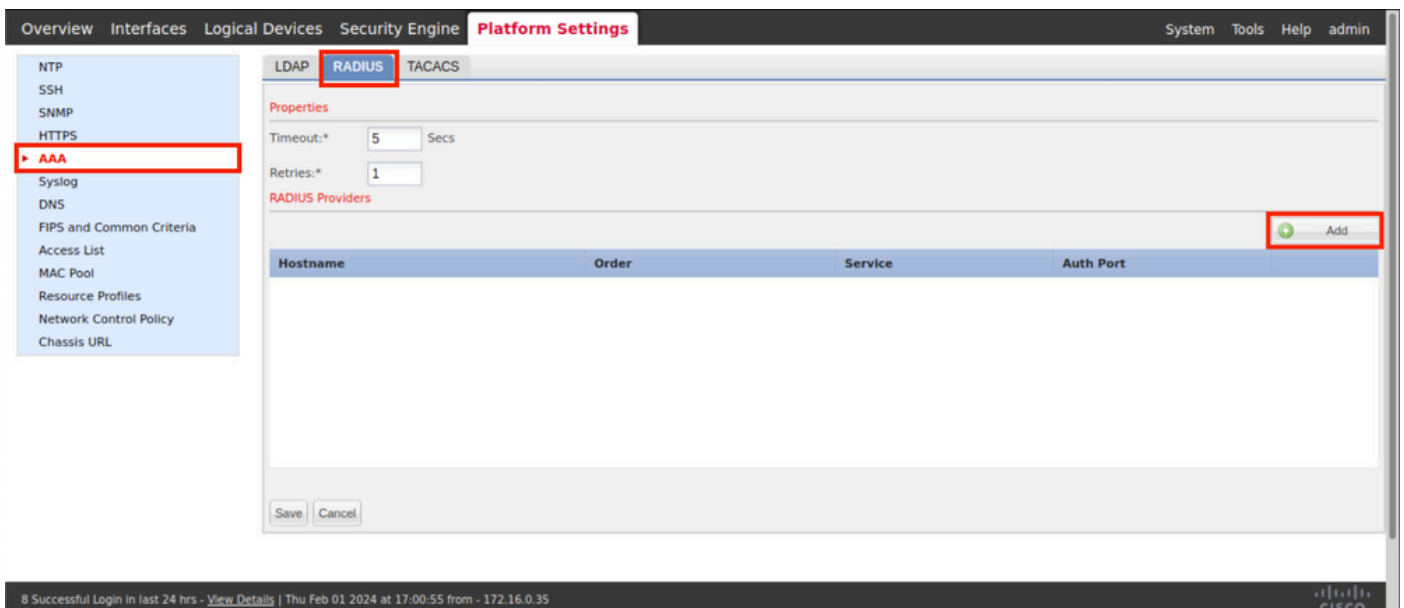
コンフィギュレーション

セキュアファイアウォールシャーシマネージャ

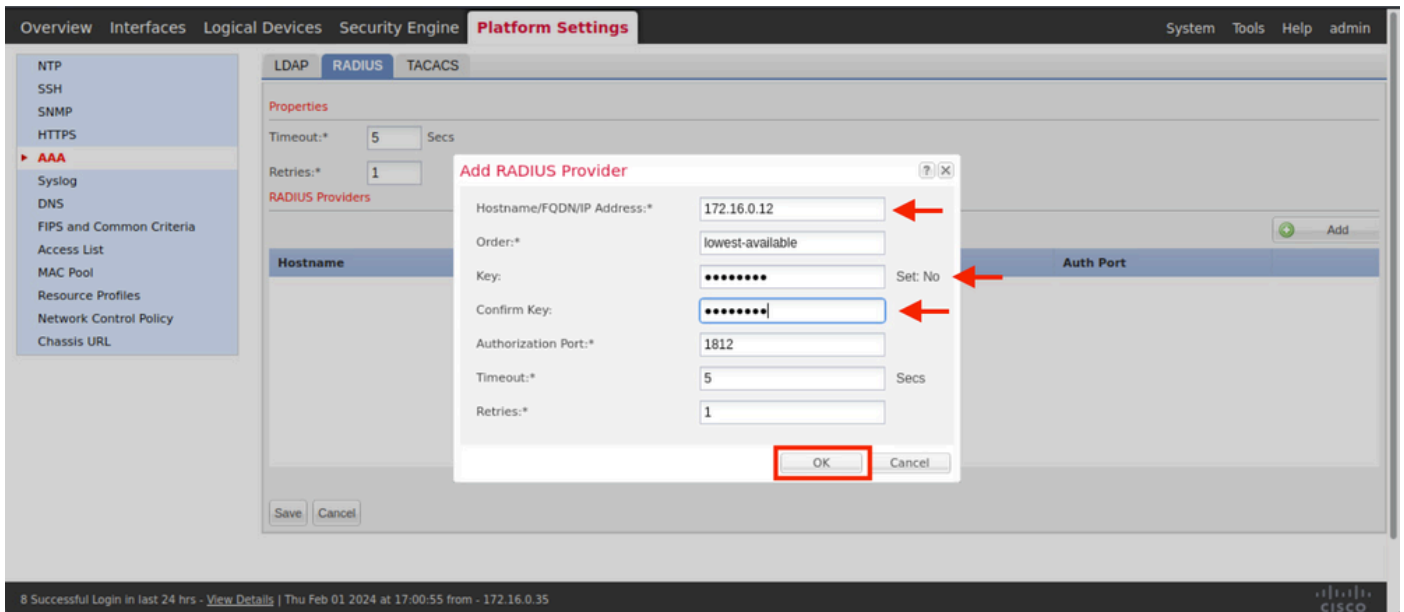
- ステップ 1 : Firepower Chassis Manager(FCM)のGUIにログインします。
- ステップ 2 : Platform Settingsに移動します。



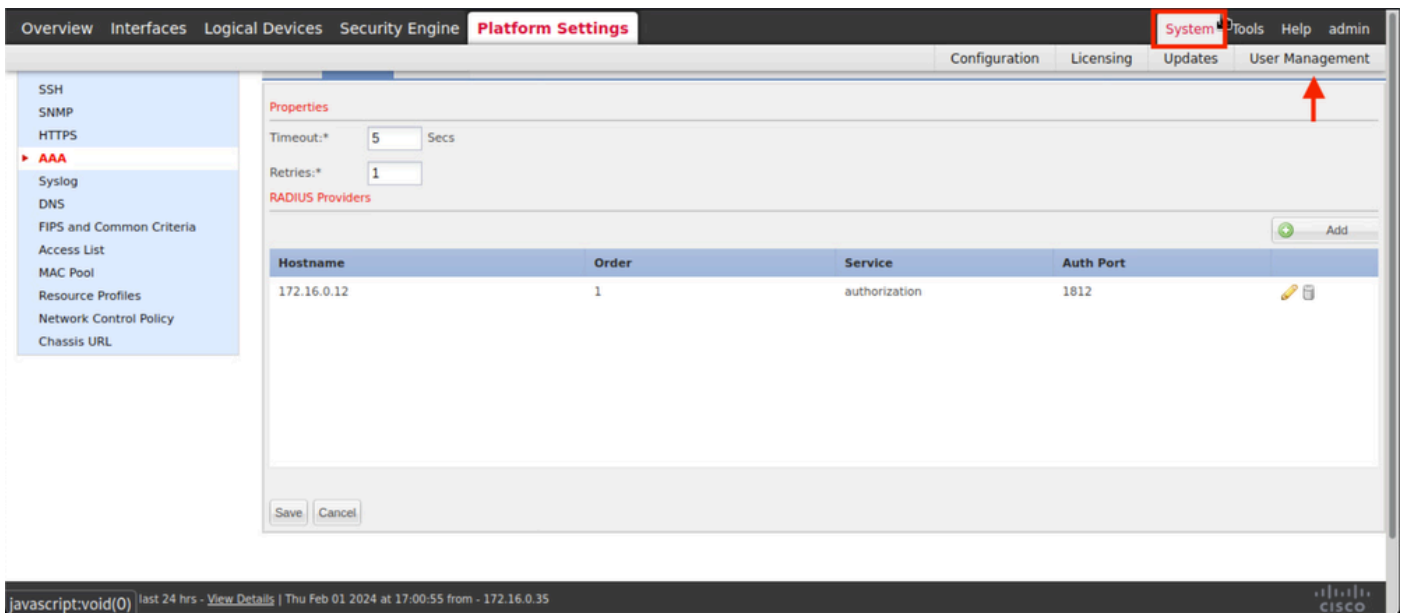
ステップ 3 : 左側のメニューからAAAをクリックします。 RadiusとAdd a new RADIUS providerを選択します。



ステップ 4 : プロンプトメニューに、RADIUSプロバイダーに関する必要な情報を入力します。[OK] をクリックします。



ステップ 5 : System > User Managementの順に移動します。



手順 6 : Settingsタブをクリックして、ドロップダウンメニューからDefault AuthenticationをRadiusに設定し、スクロールダウンして設定を保存します。


Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication

Local *Local is fallback authentication method

Local
RADIUS 
LDAP
TACACS
None
No-Login

Console Authentication

Remote User Settings

Remote User Role Policy

Local User Settings

Password Strength Check Enable

History Count (0-disabled,1-15)

Change Interval (1-730 hours)

Change Count (1-10)

No Change Interval (1-730 hours)

Days until Password Expiration (0-never,1-9999 days)

Password Expiration Warning Period (0-9999 days)

Expiration Grace Period (0-9999 days)

Password Reuse Interval (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet) (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

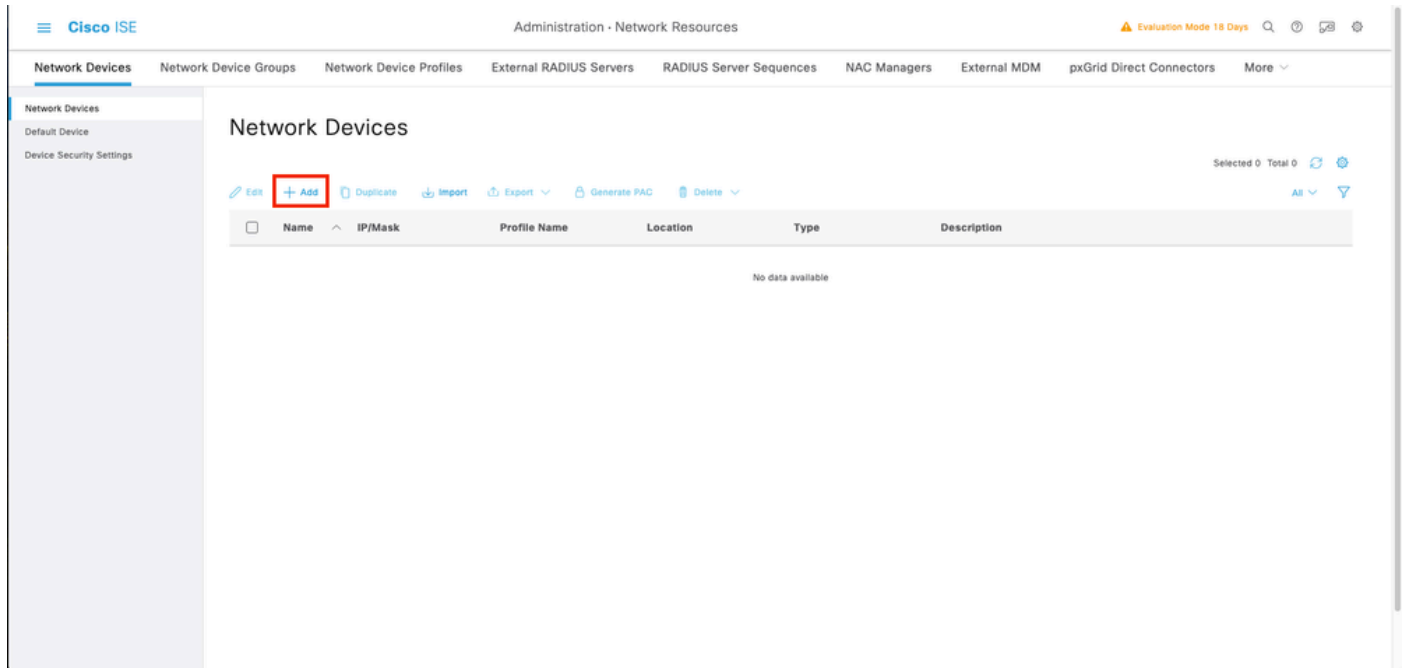
CISCO

注：FCMの設定はこの時点で完了しています。

アイデンティティサービスエンジン

ステップ 1：新しいネットワークデバイスを追加します。

左上隅にあるバーガーアイコン≡> Administration > Network Resources > Network Devices > +Addに移動します。

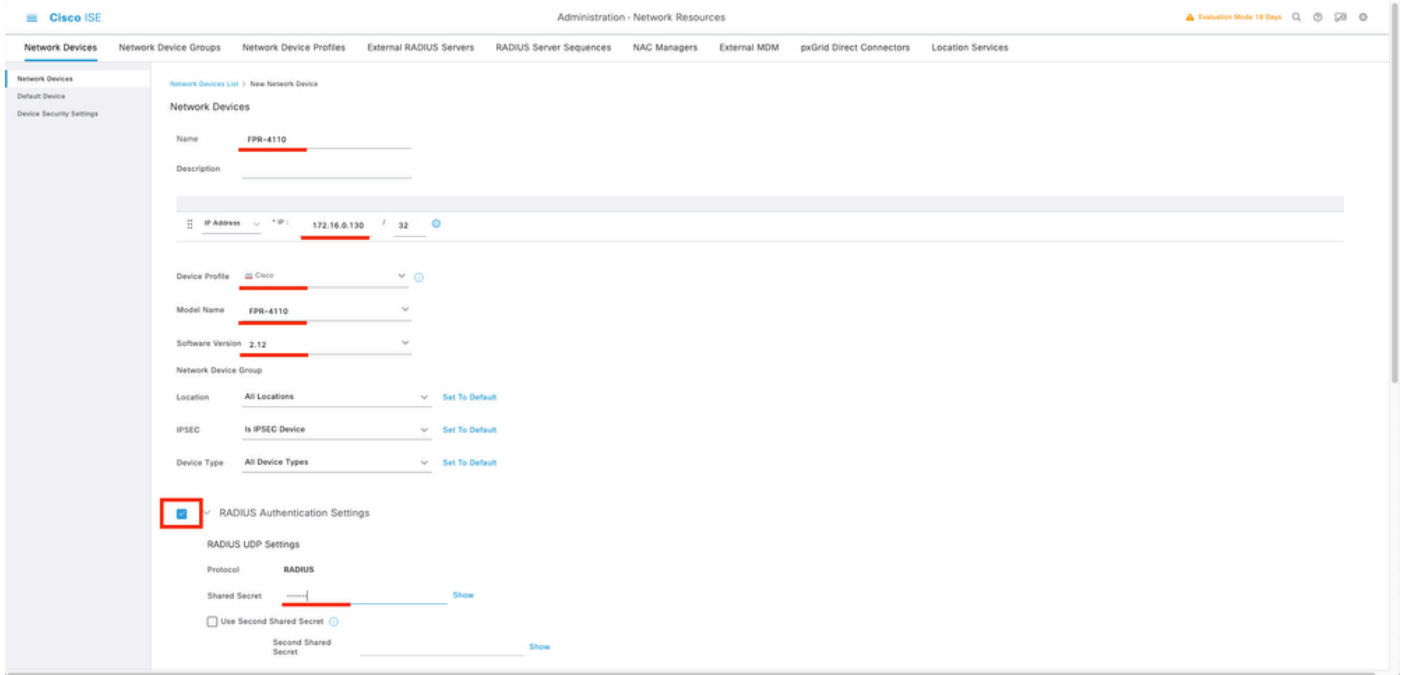


ステップ 2：新しいネットワークデバイス情報に関して要求されるパラメータを入力します。

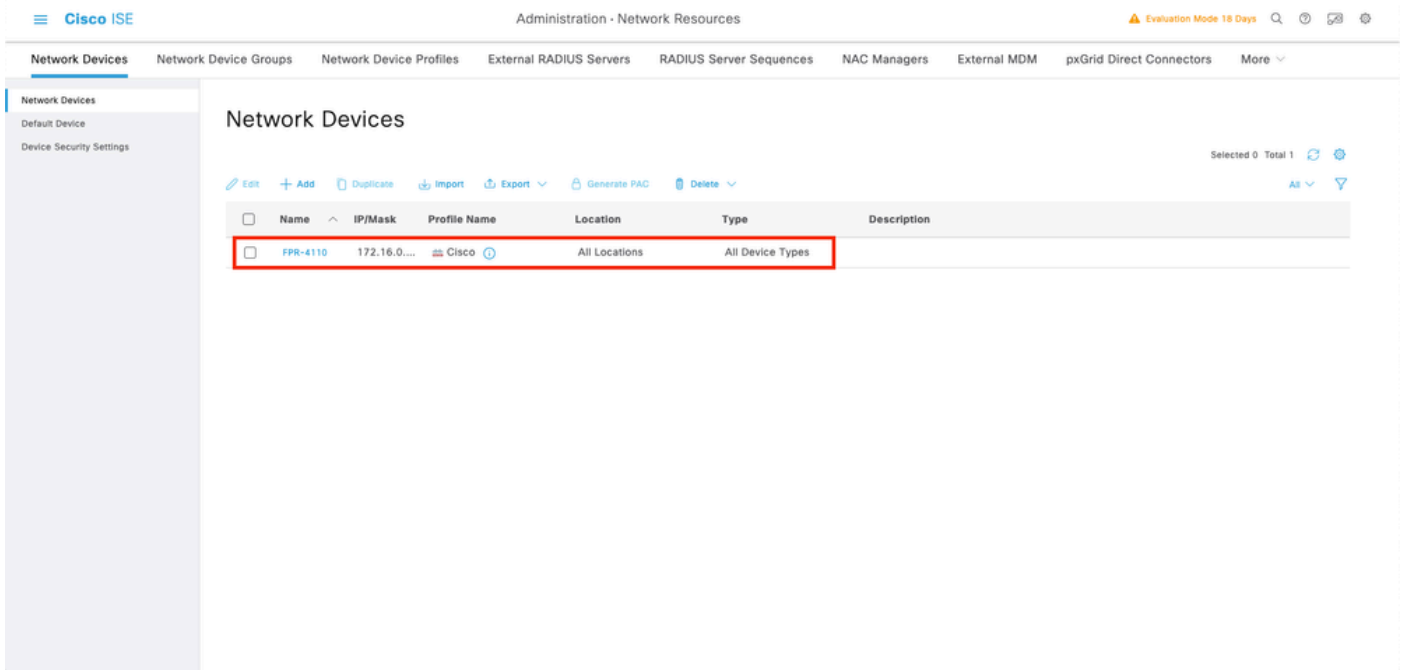
2.1 RADIUSチェックボックスのチェック

2.2 FCM RADIUS設定と同じ共有秘密キーを設定します。

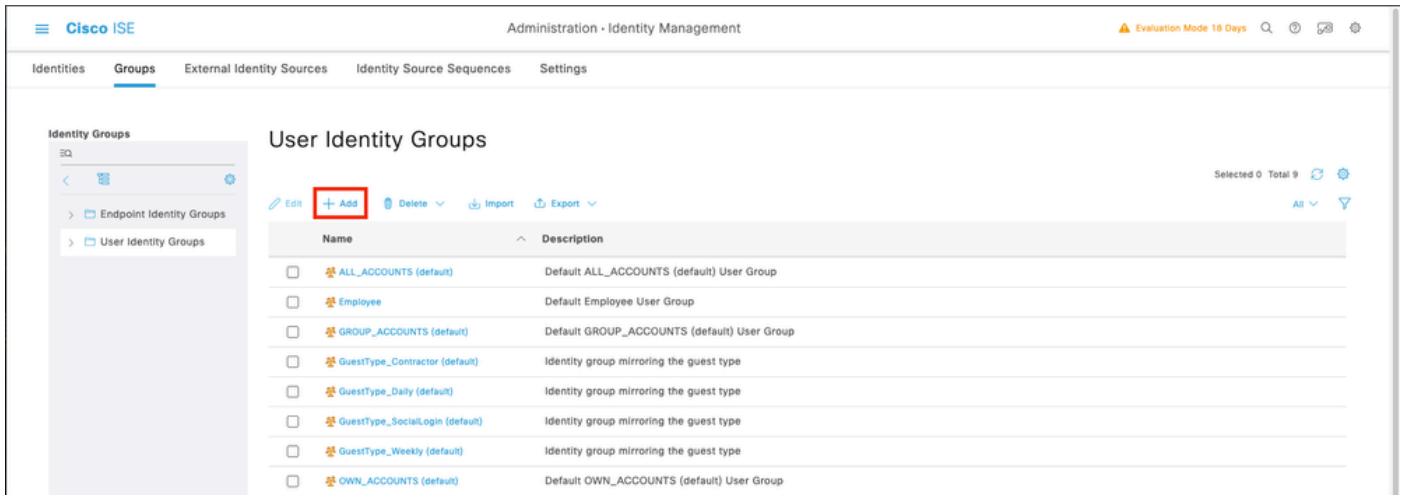
2.1下にスクロールして、Submitをクリックします。



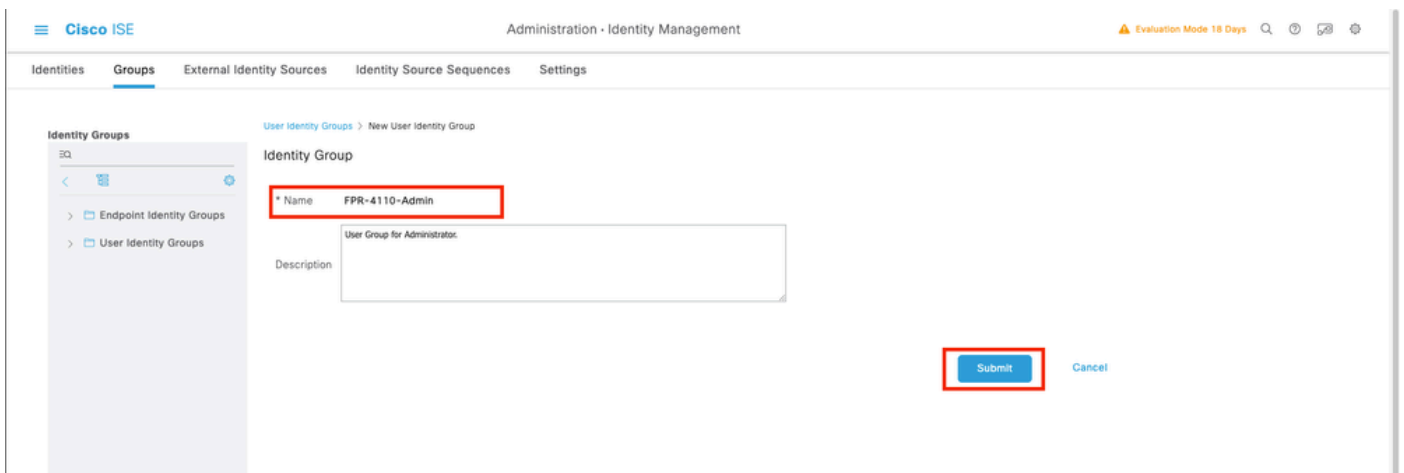
ステップ 3 : [ネットワークデバイス]に新しいデバイスが表示されていることを確認します。



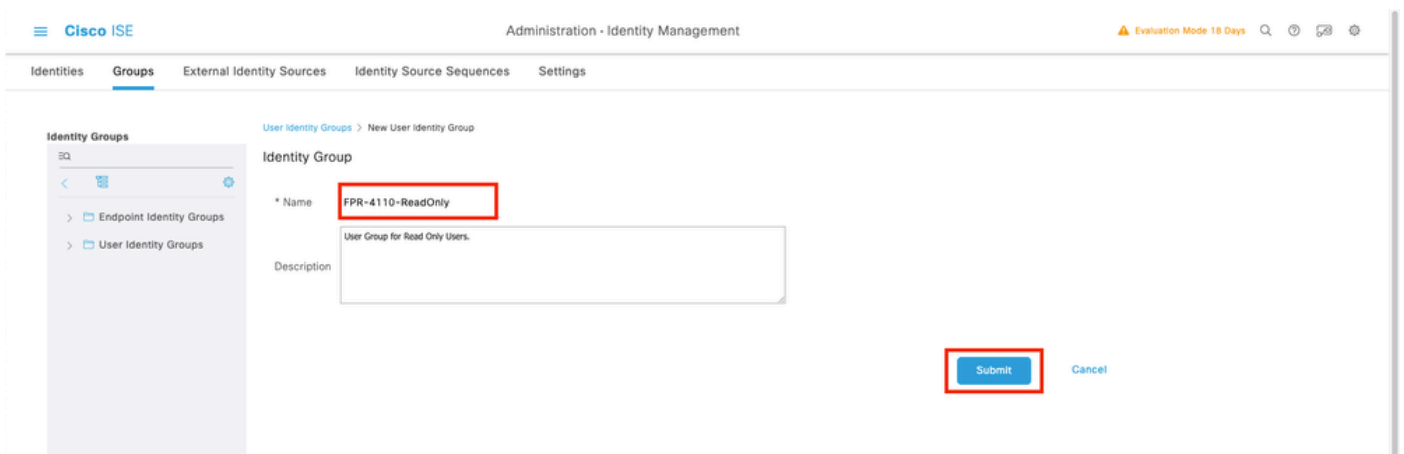
ステップ 4 : 必要なユーザIDグループを作成します。左上隅にあるバーガーアイコン≡> Administration > Identity Management > Groups > User Identity Groups > + Addに移動します



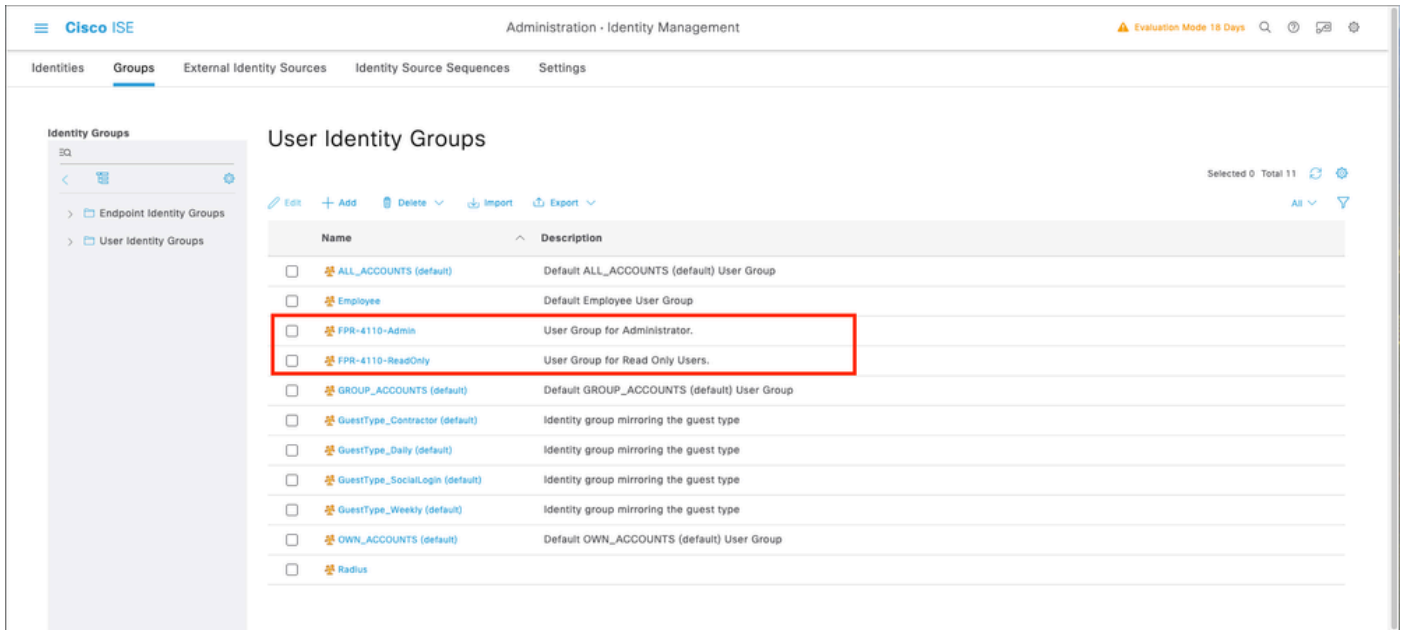
ステップ 5 : 管理者ユーザIDグループの名前を設定して、Submitをクリックし、設定を保存します。



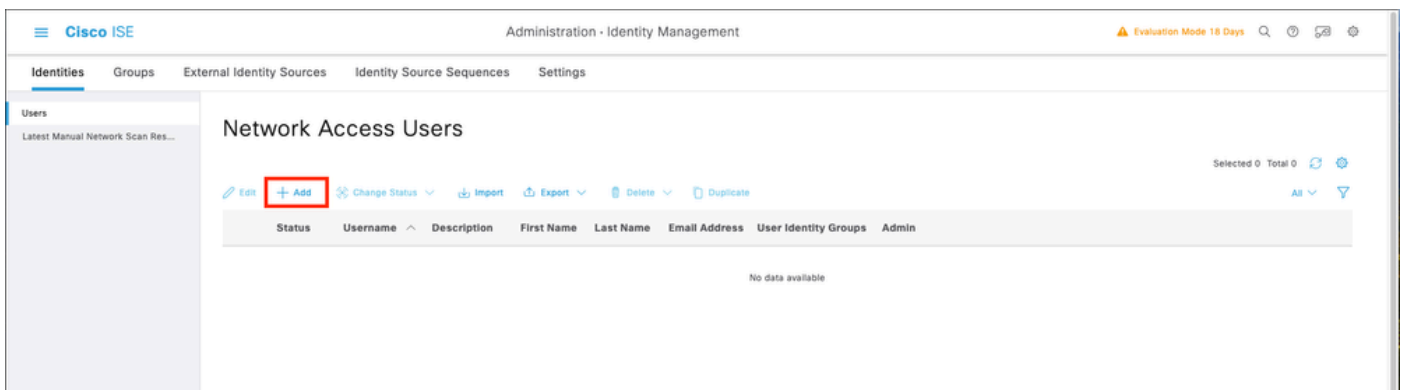
5.1読み取り専用ユーザに対して同じプロセスを繰り返します。



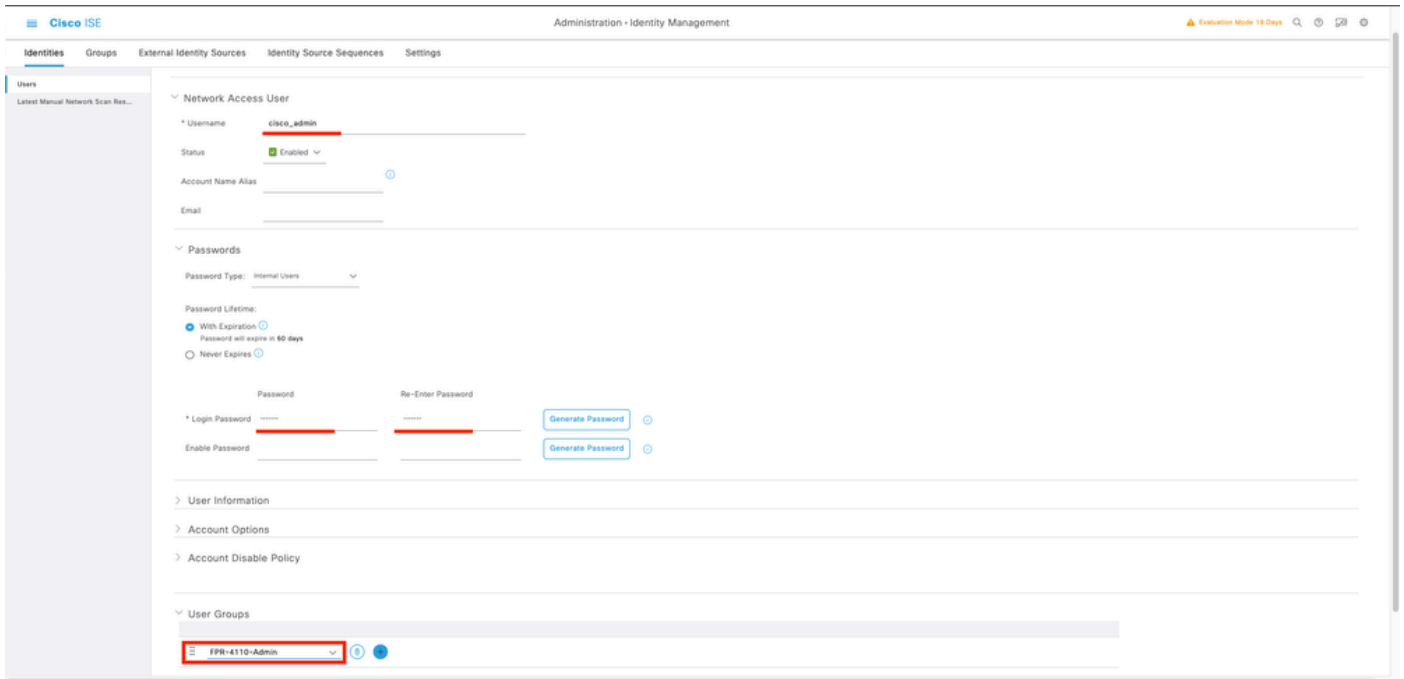
手順 6 : 新しいユーザグループがユーザIDグループの下に表示されていることを確認します。



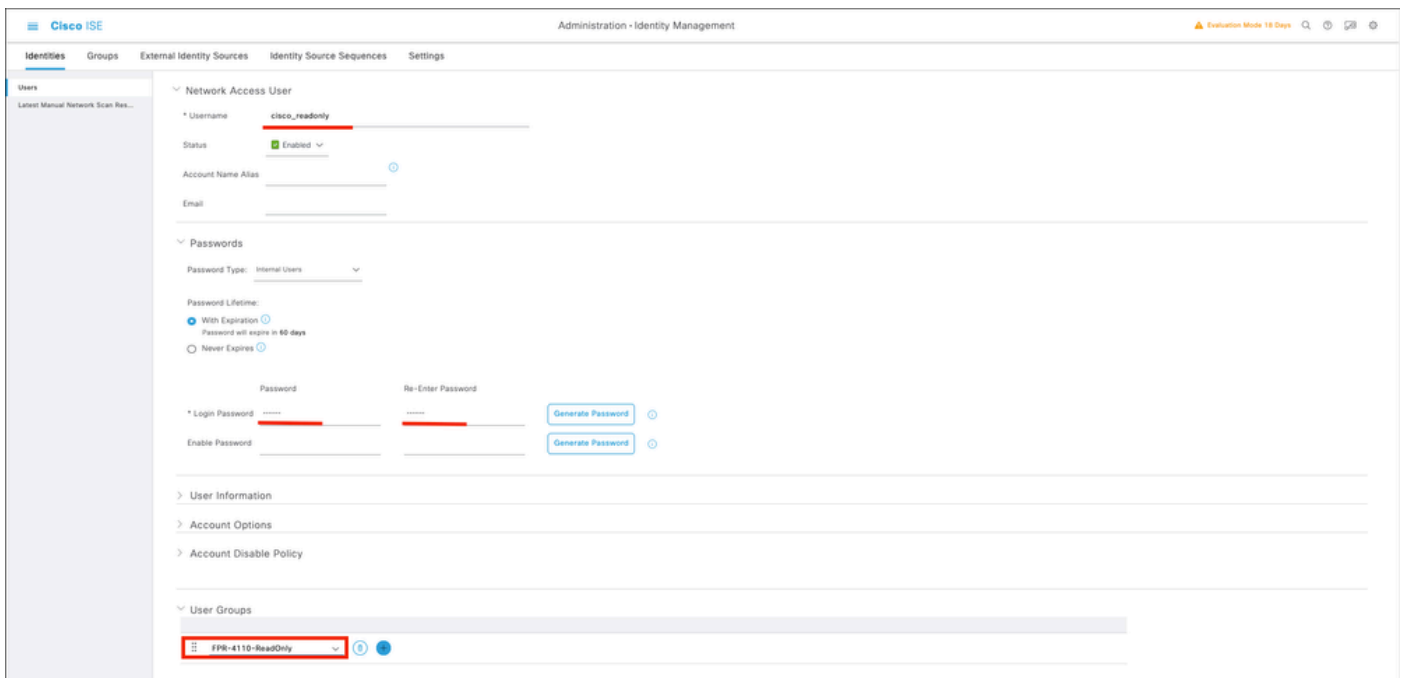
手順 7： ローカルユーザを作成し、対応するグループに追加します。バーガーアイコン☰> Administration > Identity Management > Identities > + Addに移動します。



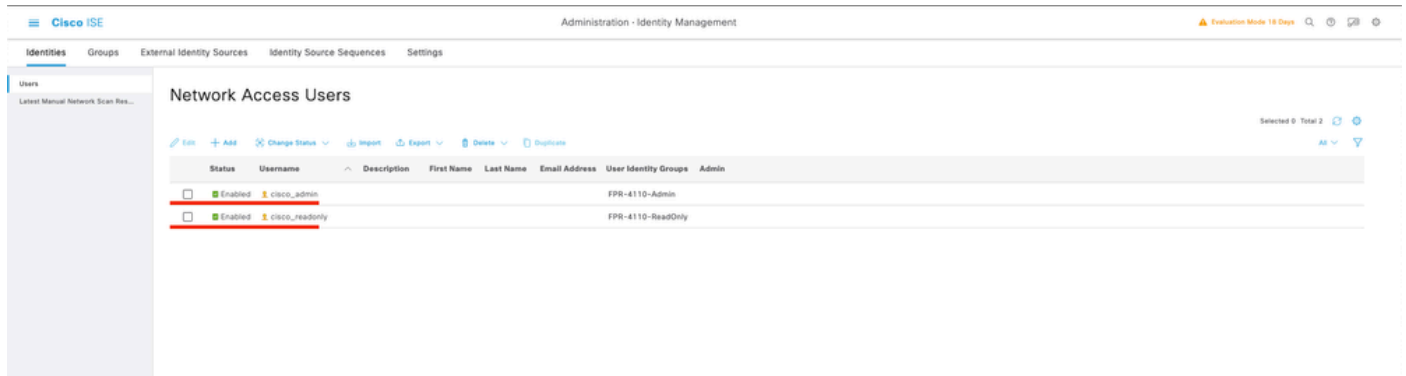
7.1管理者権限を持つユーザを追加する。名前とパスワードを設定し、それをFPR-4110-Adminに割り当て、スクロールダウンしてSubmitをクリックし、変更を保存します。



7.2読み取り専用権限を持つユーザを追加する。名前とパスワードを設定し、それをFPR-4110-ReadOnlyに割り当てます。スクロールダウンして、Submitをクリックし、変更を保存します。



7.3ユーザがNetwork Access Usersの下にあることを確認する。



ステップ8:Adminユーザの許可プロファイルを作成します。

FXOSシャーシには、次のユーザロールが含まれます。

- 管理者：システム全体への読み取り/書き込みアクセス権を付与します。デフォルトの管理者アカウントにはデフォルトでこのロールが割り当てられ、変更することはできません。
- 読み取り専用：システムの状態を変更する権限のない、システム設定への読み取り専用アクセス。
- 操作：NTP設定、Smart Licensing用のSmart Call Home設定、およびsyslogサーバと障害を含むシステムログへの読み取りおよび書き込みアクセス。システムの他の部分への読み取りアクセス。
- AAA：ユーザ、ロール、およびAAA設定への読み取り/書き込みアクセス。システムの他の部分への読み取りアクセス

各ロールの属性

```
cisco-av-pair=shell:roles="admin"
```

```
cisco-av-pair=shell:roles="aaa"
```

```
cisco-av-pair=shell:roles="操作"
```

```
cisco-av-pair=shell:roles="読み取り専用"
```



注：このドキュメントでは、admin属性とread-only属性のみを定義しています。

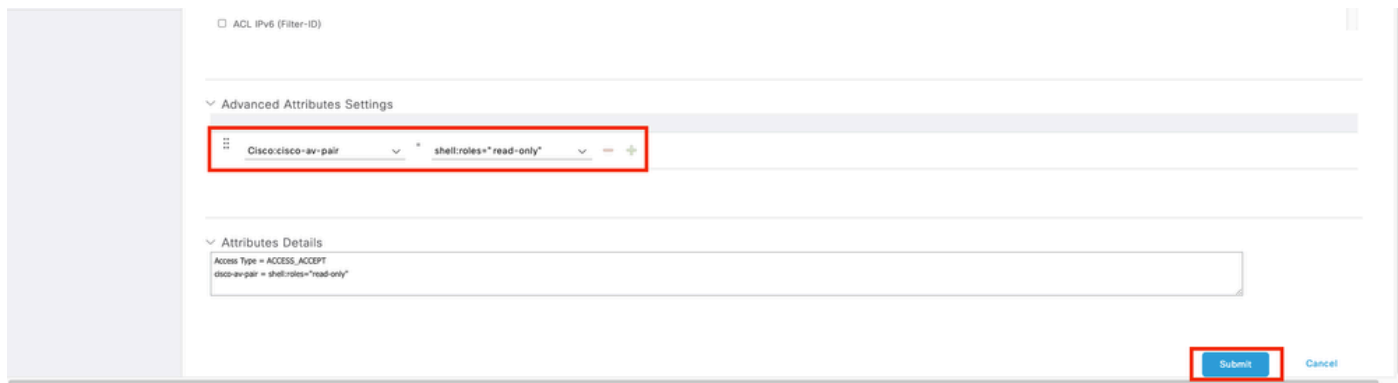
バーガーアイコン ≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Addの順に移動します。

許可プロファイルの名前を定義し、アクセスタイプをACCESS_ACCEPTのままにして、Advanced Attributes Settingsでcisco-av-pair=shell:roles="admin"を追加し、Submitをクリックします。

The screenshot shows the Cisco ISE Policy Elements configuration interface. The left sidebar contains navigation menus for Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profile' and shows the configuration for 'FPR-4110-Admins'. The 'Name' field is 'FPR-4110-Admins' and the 'Access Type' is 'ACCESS_ACCEPT'. Under 'Advanced Attributes Settings', a rule is defined as 'Cisco:cisco-av-pair = shell:roles=*admin*'. The 'Attributes Details' section shows the resulting attributes: 'Access Type = ACCESS_ACCEPT' and 'cisco-av-pair = shell:roles=*admin*'. A 'Submit' button is visible at the bottom right.

8.1前の手順を繰り返して、読み取り専用ユーザの許可プロファイルを作成します。今回は Administratorではなく、read-onlyの値でRadiusクラスを作成します。

The screenshot shows the Cisco ISE Policy Elements configuration interface for a new 'Authorization Profile'. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Authorization Profile' and shows the configuration for 'FPR-4110-ReadOnly'. The 'Name' field is 'FPR-4110-ReadOnly' and the 'Access Type' is 'ACCESS_ACCEPT'. The 'Advanced Attributes Settings' and 'Attributes Details' sections are currently empty.

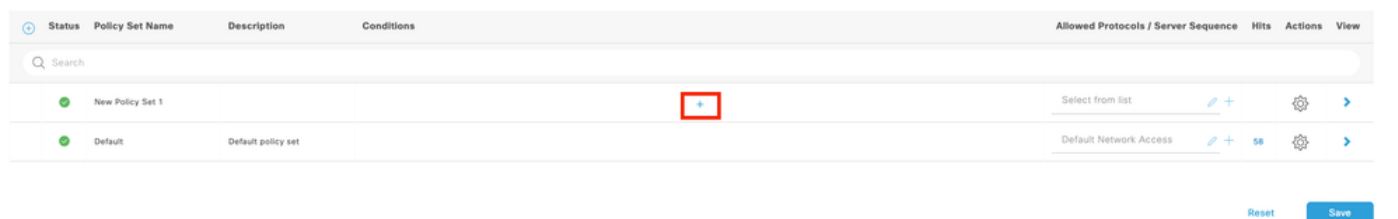


ステップ9:FMC IPアドレスに一致するポリシーセットを作成します。これは、他のデバイスがユーザにアクセス権を付与するのを防ぐためです。

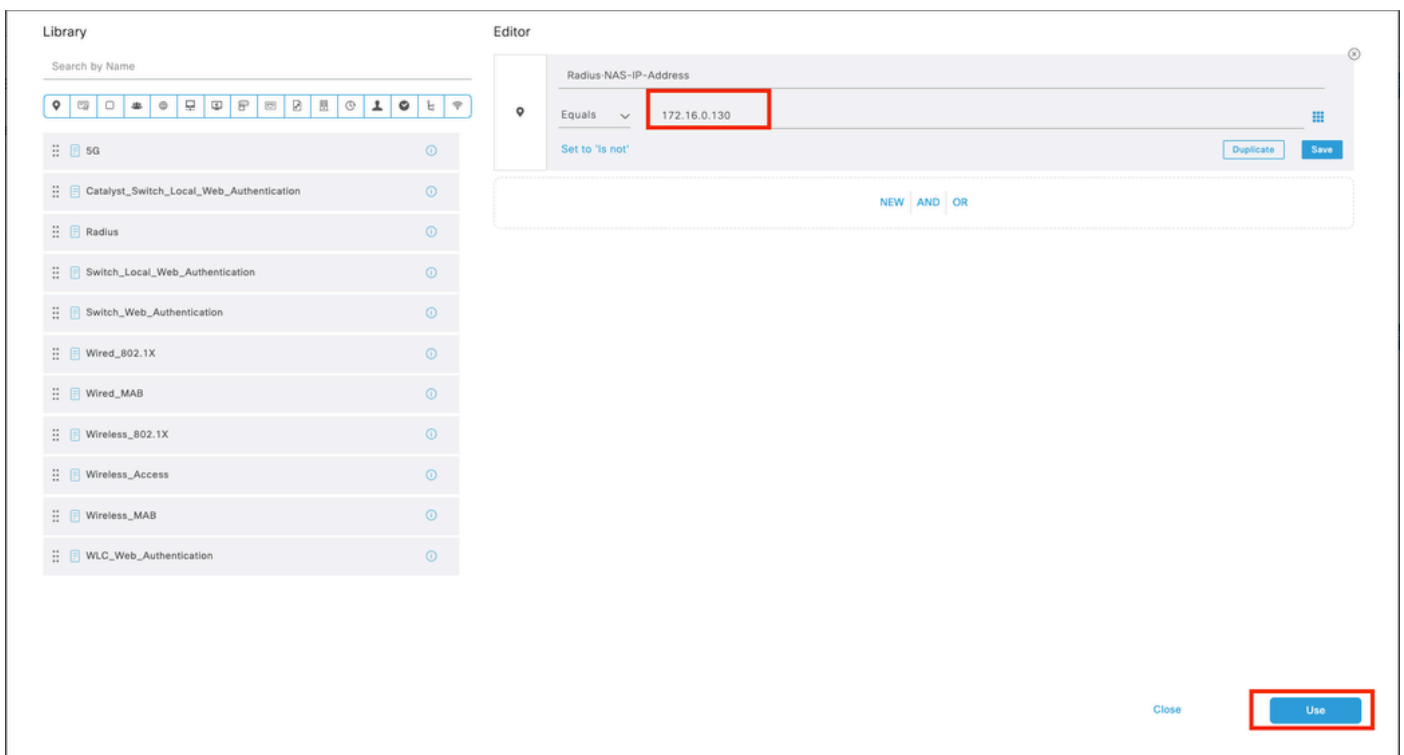
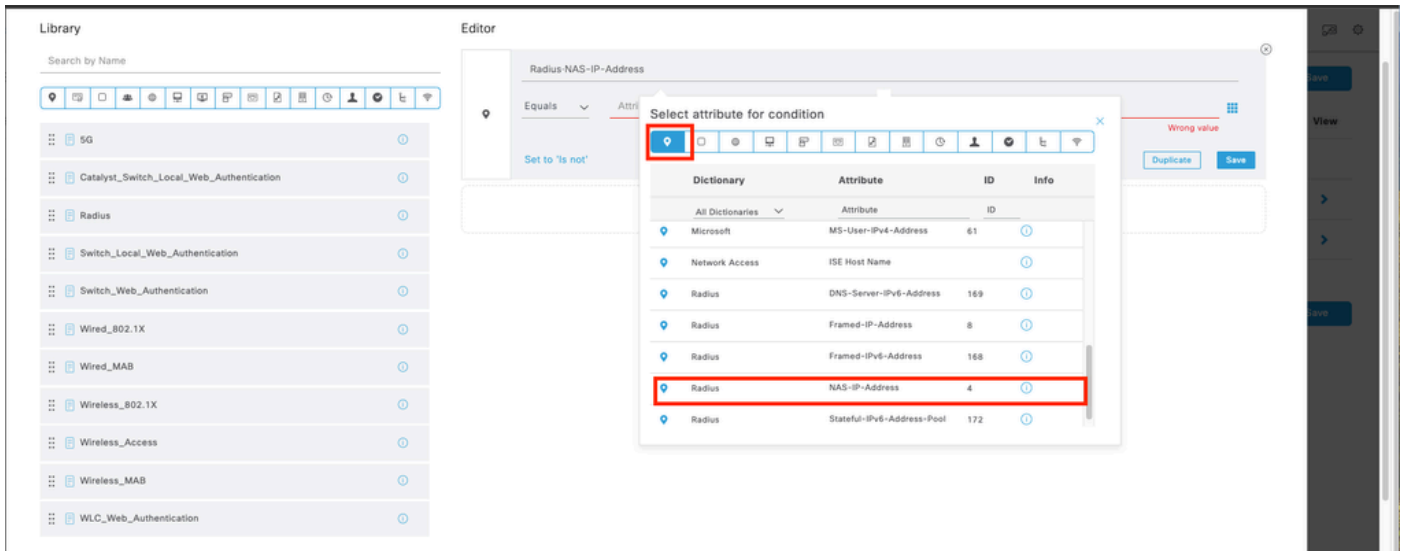
左上隅の⇒ Policy > Policy Sets >Add icon signに移動します。



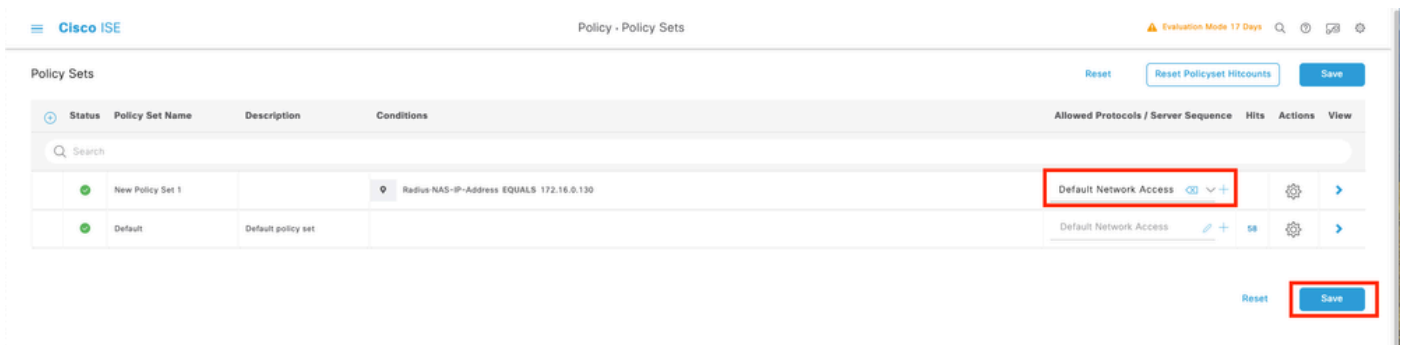
9.1新しい品目がポリシーセットの一番上に表示されます。Addアイコンをクリックして、新しい条件を設定します。

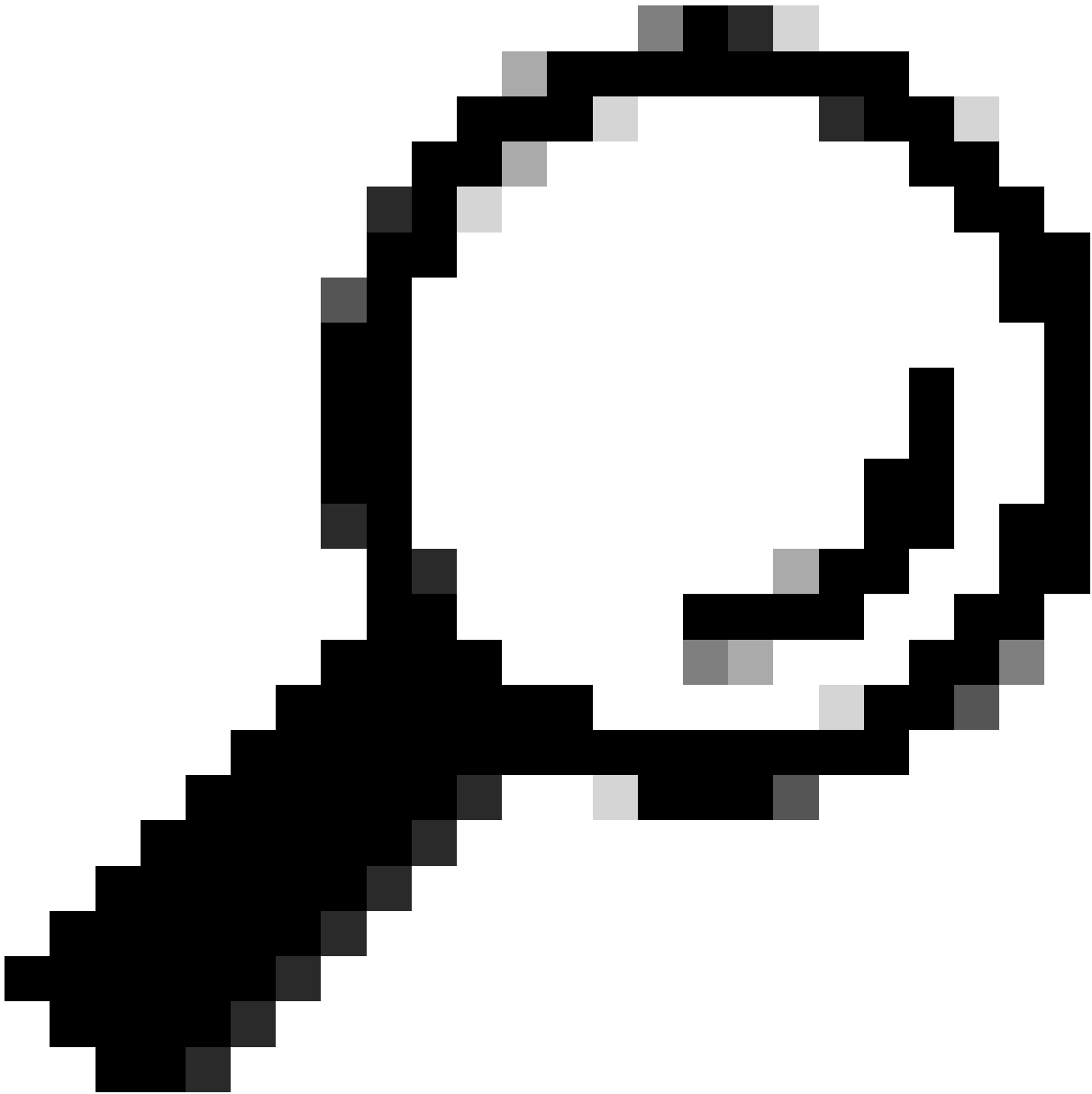


9.2 FCM IPアドレスに一致するRADIUS NAS-IP-Addressattributeのトップ条件を追加し、Useをクリックします。



9.3完了したら、Saveをクリックします。



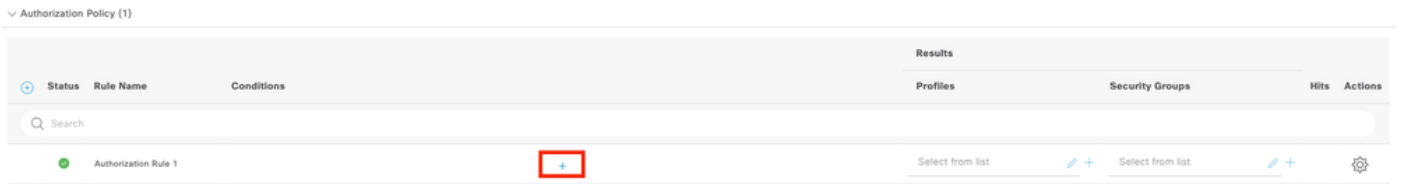


ヒント：この演習では、デフォルトのNetwork Access Protocolsリストを許可しています。新しいリストを作成し、必要に応じてリストを絞り込むことができます。

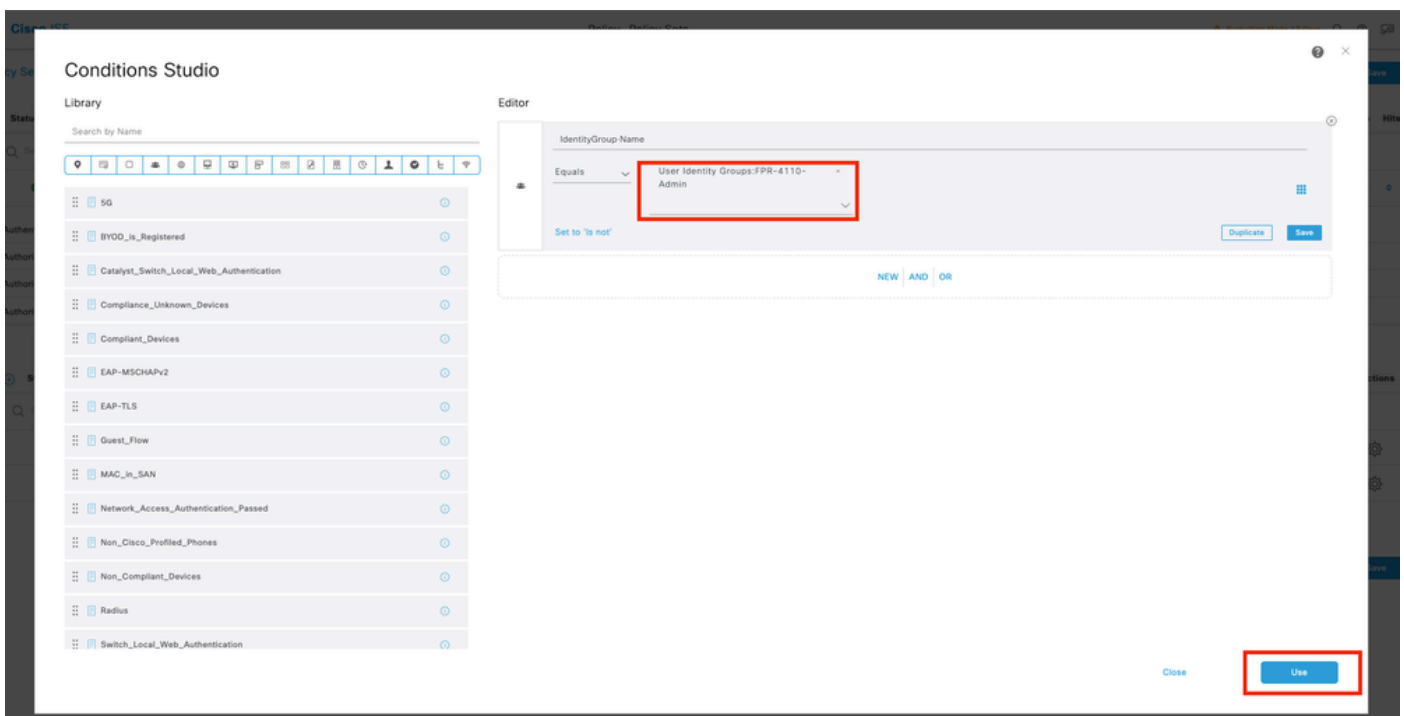
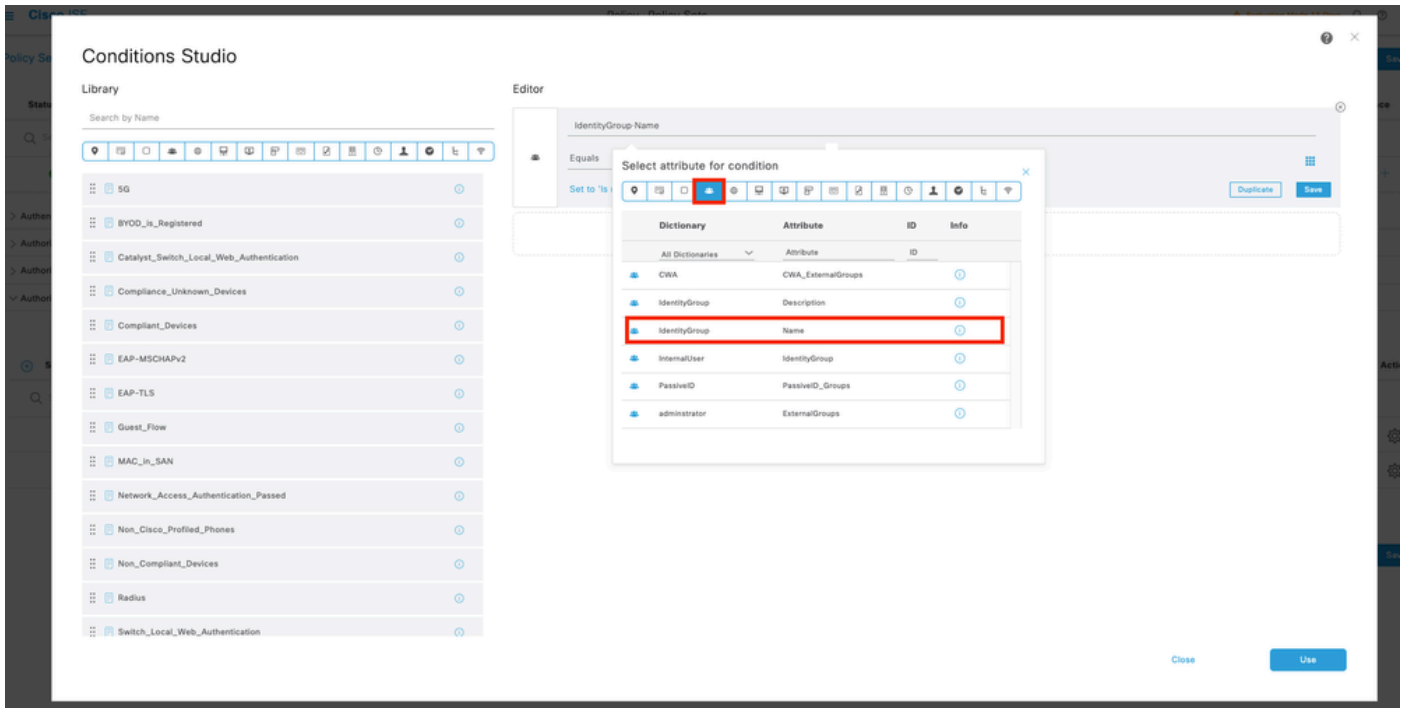
ステップ 10： 行の最後にある >アイコンをクリックして、新しいポリシーセットを表示します。



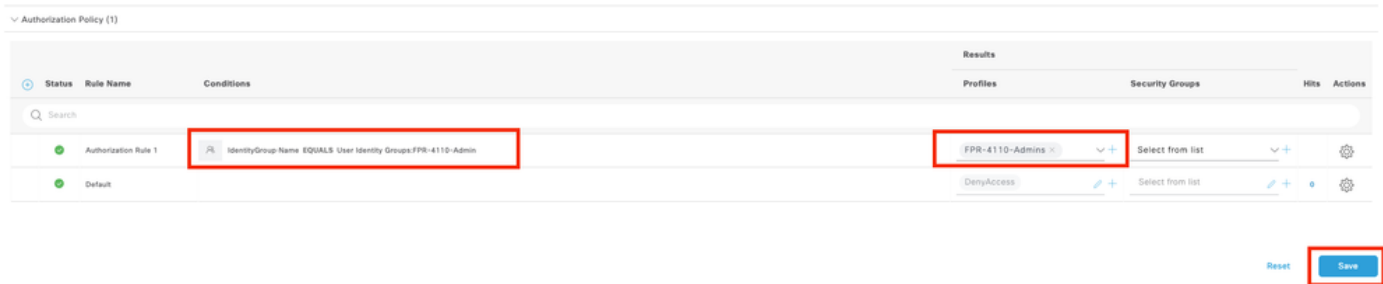
10.1 Authorization Policy メニューを展開し、(+)をクリックして新しい条件を追加します。



10.2 DictionaryIdentity Groupwith AttributeName Equals User Identity Groups: FPR-4110-Admins (ステップ7で作成したグループ名) に一致する条件を設定し、Useをクリックします。



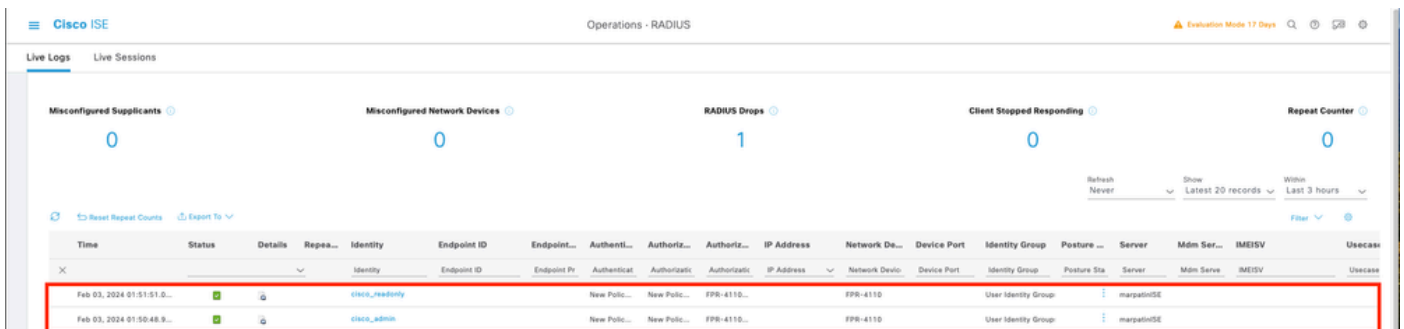
手順10.3:許可ポリシーで新しい条件が設定されていることを確認し、Profilesの下にユーザプロファイルを追加します。



ステップ 11ステップ9で同じプロセスを読み取り専用ユーザに繰り返し、保存をクリックします。

確認

1. 新しいRADIUSクレデンシャルを使用して、FCM GUIへのログインを試行します。
2. バーガーアイコンに移動します⇒ Operations > Radius > Live logs。
3. 表示される情報は、ユーザーが正常にログインしたかどうかを示します。



4. Secure Firewall Chassis CLIからLogged usersロールを検証します。

```
FPR4K-1-029A78B# scope se
security server service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
  Description:
  User Roles:
    Name: admin
    Name: read-only
FPR4K-1-029A78B /security #
```

トラブルシュート

1. ISE GUIで、バーガーアイコン≡ > Operations > Radius > Live logsの順に移動します。

1.1 ログセッション要求がISEノードに到達しているかどうかを検証します。

1.2 失敗ステータスについては、セッションの詳細を確認します。

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Pr	Authent...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture Sta	Server	Mdm Sen
Feb 02, 2024 07:32:18.8...	✖	✖		cisco_admin			Default >>...	Default			FPR-4110		User Identity Group:		marpat@ISE	
Feb 02, 2024 07:23:20.1...	✔	✔		cisco_readonly			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group:		marpat@ISE	
Feb 02, 2024 07:15:32.2...	✔	✔		cisco_admin			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group:		marpat@ISE	

2. RADIUSライブログに表示されない要求 (UDP要求がISEノードに到達しているかどうかをパケットキャプチャを介して確認する) の場合。

burgerアイコン≡ > Operations > Troubleshoot > Diagnostic Tools > TCP dumpの順に移動します。UDPパケットがISEノードに到着しているかどうかを確認するために、新しいキャプチャを追加し、ファイルをローカルマシンにダウンロードします。

2.1 必要な情報を入力し、下にスクロールしてSaveをクリックします。

Diagnostic Tools | Download Logs | Debug Wizard

General Tools

TCP Dump > New

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

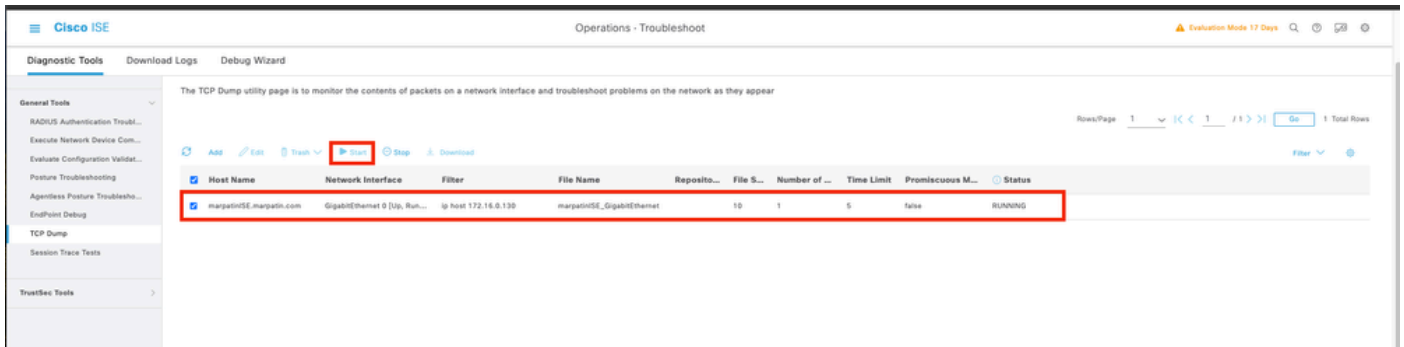
Host Name*
marpat@ISE

Network Interface*
GigabitEthernet 0 [Up, Running]

Filter
ip host 172.16.0.130

E.g. ip host 10.97.122.123 and not 10.172.122.119

2.2 キャプチャを選択して開始します。



2.3 ISEキャプチャの実行中にセキュアファイアウォールシャーシへのログインを試みる

2.4 ISEでTCPダンプを停止し、ファイルをローカルマシンにダウンロードします。

2.5 トラフィック出力のレビュー

予想される出力：

パケット番号1。セキュアファイアウォールからISEサーバへのポート1812(RADIUS)経由の要求
パケット番号2 ISEサーバが最初の要求を受け入れて応答します。

marpatinISE_GigabitEthernet 2.pcap

Apply a display filter ... <ctrl>

No.	Time	Source	Destination	Length	Protocol	Message Transaction ID	Info
1	2024-02-02 20:21:52.999276	172.16.0.130	172.16.0.12	128	RADIUS		Access-Request id=22
2	2024-02-02 20:21:53.090894	172.16.0.12	172.16.0.130	186	RADIUS		Access-Accept id=22

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。