

ISEをRADIUSサーバとして使用するFMCおよびFTD外部認証の設定

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](#)

[FMCの外部認証](#)

[FTDの外部認証](#)

[Network Topology](#)

[設定](#)

[ISE 設定](#)

[FMCの設定](#)

[FTD の設定](#)

[確認](#)

はじめに

このドキュメントでは、Secure Firewall Management Center(FMC)とファイアウォール脅威対策の外部認証設定の例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 Secure Firewall Management Centerの初期設定 (GUIまたはシェル経由)
- ISE 上での認証ポリシーおよび認可ポリシーの設定.
- RADIUS の基礎知識.

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。

- vFMC 7.2.5
- vFTD 7.2.5
- ISE 3.2.

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

セキュアファイアウォールシステムの管理ユーザおよび管理ユーザに対して外部認証を有効にすると、デバイスは外部認証オブジェクトで指定されているLightweight Directory Access Protocol(LDAP)またはRADIUSサーバを使用してユーザクレデンシャルを確認します。

外部認証オブジェクトは、FMCおよびFTDデバイスで使用できます。異なるアプライアンス/デバイスタイプ間で同じオブジェクトを共有したり、別々のオブジェクトを作成したりできます。

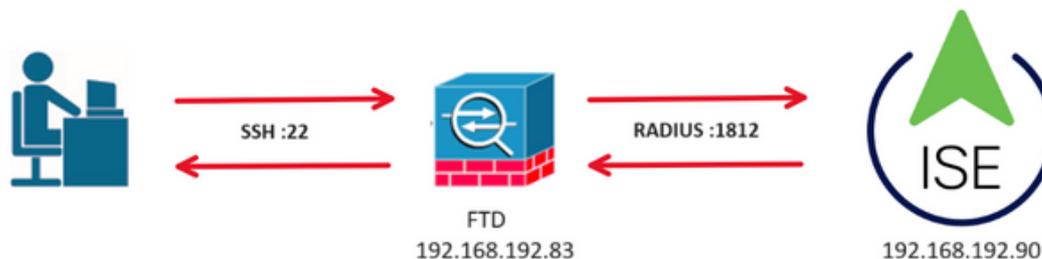
FMCの外部認証

Webインターフェイスアクセス用に複数の外部認証オブジェクトを設定できます。CLIまたはシェルアクセスに使用できる外部認証オブジェクトは1つだけです。

FTDの外部認証

FTDでは、1つの外部認証オブジェクトしかアクティブにできません。

Network Topology



設定

ISE 設定



注:FMCなどのネットワークアクセスデバイス(NAD)用にISE認証および認可ポリシーを設定する方法は複数あります。このドキュメントで説明する例は、参照点として2つのプロファイル(1つは管理者権限を持ち、もう1つは読み取り専用)を作成し、ネットワークにアクセスするためのベースラインを満たすように調整できます。RADIUS属性値をFMCに返すISEで1つ以上の認可ポリシーを定義し、次にその属性値をFMCシステムポリシー設定で定義されたローカルユーザグループにマッピングできます。

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 >管理>ネットワークリソース>ネットワークデバイス> +追加に移動します。



Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | More

Network Devices

Default Device
Device Security Settings

Network Devices

Selected 0 Total 2

Edit + Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

ステップ 2 : ネットワークデバイスオブジェクトに名前を割り当て、FMCのIPアドレスを挿入します。

RADIUSのチェックボックスをオンにして、共有秘密を定義します。

後で同じキーを使用してFMCを設定する必要があります。

完了したら、Saveをクリックします。

Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | More

Network Devices

Default Device
Device Security Settings

Network Devices List > FMC

Network Devices

Name **FMC**

Description

IP Address * IP: **192.168.192.60** / 32

Device Profile Cisco

Model Name vFMC

Software Version 7.2.5

Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret ********* Show

Use Second Shared Secret

Second Shared Secret Show

ステップ 2.1 : 同じ手順を繰り返してFTDを追加します。

ネットワークデバイスオブジェクトに名前を割り当て、FTDのIPアドレスを挿入します。

RADIUSのチェックボックスをオンにして、共有秘密を定義します。

完了したら、Saveをクリックします。

The screenshot shows the configuration page for a Network Device named 'FTD'. The IP Address is 192.168.192.83/32. The Device Profile is Cisco, Model Name is vFTD, and Software Version is 7.2.5. The RADIUS Authentication Settings checkbox is checked and highlighted with a red box. The Shared Secret field is filled with asterisks. The RADIUS UDP Settings section shows the Protocol is RADIUS and the Shared Secret is masked with asterisks. The Use Second Shared Secret checkbox is unchecked.

ステップ 2.3 : 両方のデバイスがネットワークデバイスの下に表示されていることを確認します

。

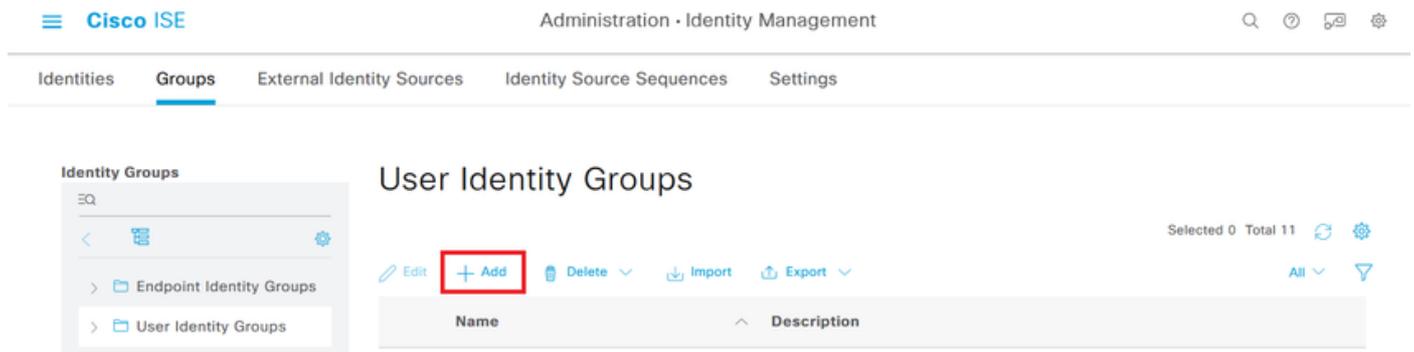
The screenshot shows the Network Devices list in Cisco ISE. The list contains two devices: FMC and FTD. Both devices have the same Profile Name (Cisco), Location (All Locations), and Type (All Device Types). The IP/Mask for FMC is 192.168.192.60/32 and for FTD is 192.168.192.83/32.

Name	IP/Mask	Profile Name	Location	Type	Description
FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

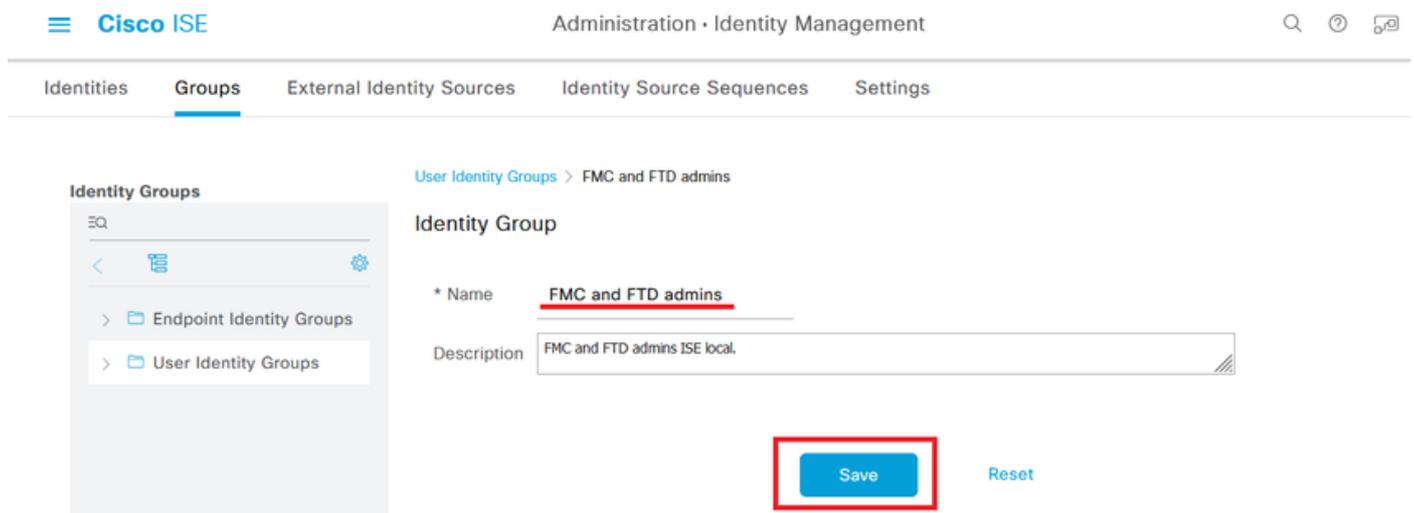
ステップ 3 : 必要なユーザIDグループを作成します。左上隅にあるバーガーアイコン



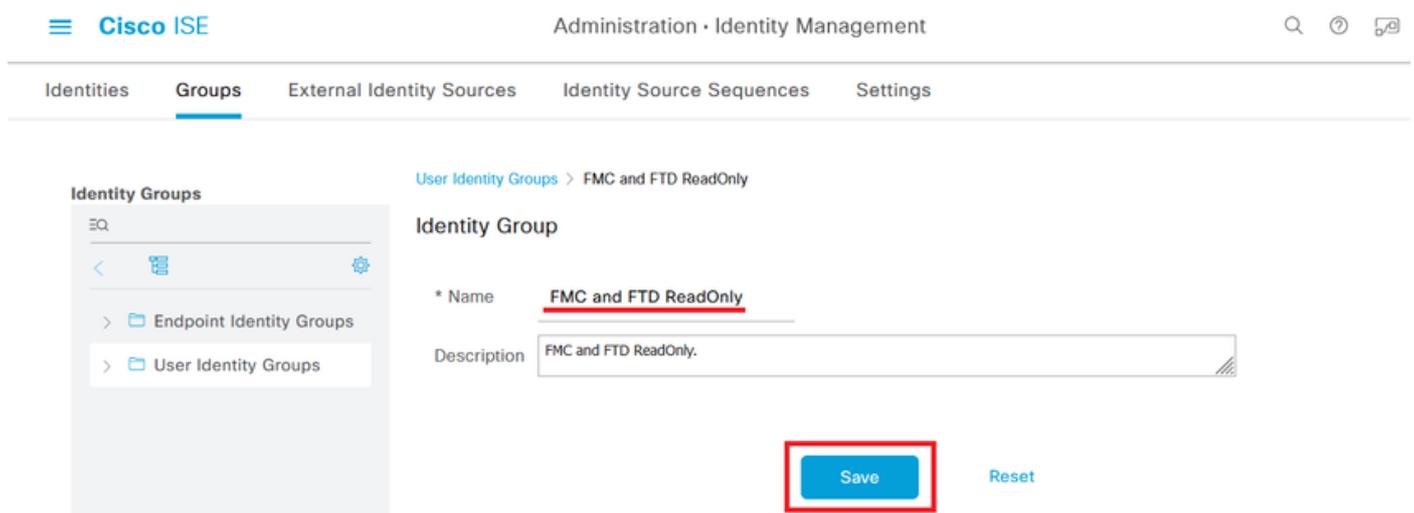
>管理>アイデンティティ管理>グループ>ユーザアイデンティティグループ> +追加に移動します



ステップ 4：各グループに名前を付けて、個別に保存します。この例では、管理者ユーザ用のグループと、読み取り専用ユーザ用のグループを作成します。まず、管理者権限を持つユーザのグループを作成します。



ステップ 4.1：ReadOnlyユーザの2番目のグループを作成します。



ステップ 4.2：両方のグループがUser Identity Groups Listの下に表示されていることを確認します。フィルタを使用すると、簡単に見つけることができます。

Identity Groups

Identity Groups sidebar navigation:

- Endpoint Identity Groups
- User Identity Groups

User Identity Groups

Selected 0 Total 2 🔄 ⚙️

✎ Edit + Add 🗑️ Delete 📄 Import 📤 Export

Quick Filter 📄 

Name	Description
fmc	
<input type="checkbox"/> FMC and FTD ReadOnly	FMC and FTD ReadOnly
<input type="checkbox"/> FMC and FTD admins	FMC and FTD admins ISE local.

ステップ 5：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。
> Administration > Identity Management > Identities > + Addの順に移動します。

Users

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 0 🔄 ⚙️

✎ Edit  Change Status 📄 Import 📤 Export 🗑️ DeleteAll 📄 

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Adm
--------	----------	-------------	------------	-----------	---------------	----------------------	-----

No data available

ステップ 5.1：まず、管理者権限を持つユーザを作成します。名前、パスワード、およびFMCとFTDの管理者グループを割り当てます。

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_admin

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

- With Expiration ⓘ
- Never Expires ⓘ

	Password	Re-Enter Password	
* Login Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

Users

Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD admins ▾ ⓘ +

ステップ 5.2 : 読み取り専用権限を持つユーザを追加します。名前、パスワード、およびFMCとFTDのReadOnlyグループを割り当てます。

Users
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_readuser

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

Password Re-Enter Password

* Login Password ⓘ

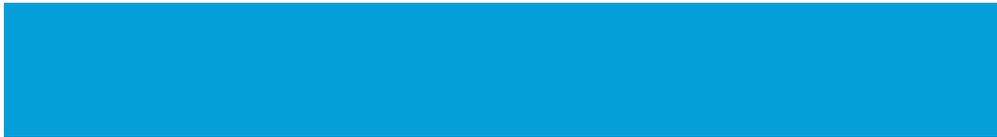
Enable Password ⓘ

Users
Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD ReadOnly ▾ ⓘ +

手順 6 : 管理者ユーザの認可プロファイルを作成します。



> 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、Access TypeをACCESS_ACCEPTのままにして、Advanced Attributes Settingsで値Administratorを指定してRadius > Class—[25]を追加し、Submitをクリックします。

The screenshot shows the Cisco ISE web interface for configuring an Authorization Profile. The breadcrumb path is "Policy > Policy Elements > Results > Authorization Profiles > FMC and FTD Admins". The left sidebar shows a navigation menu with "Authorization Profiles" selected. The main content area displays the configuration for the "FMC and FTD Admins" profile. The fields are as follows:

- Name:** FMC and FTD Admins
- Description:** (Empty text box)
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (Empty dropdown)

Dictionaryes Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

手順 7 : 前の手順を繰り返して、ReadOnly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、ReadUserの値でRadiusクラスを作成します。

Dictionaryes Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name FMC and FTD ReadUser

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Navigation: Dictionaries | Conditions | **Results**

Left sidebar menu:

- Authentication >
- Authorization ▾
 - Authorization Profiles
 - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Main content area:

Advanced Attributes Settings

⋮ Radius:Class ▾ = ReadUser ▾ - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

Buttons: **Submit** (highlighted with a red box) | Cancel

ステップ 8 : FMCの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。



左上隅にある
> Policy > Policy Sets >



アイコンに移動します。

Cisco ISE Policy · Policy Sets 🔍 ? 🗨️ ⚙️

Policy Sets Reset Reset Policyset Hitcounts Save

+ Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
🔍 Search							
🟢	Default	Default policy set		Default Network Access 📧 ⌵ +	45	⚙️	➡️

Reset Save

ステップ 8.1 : 新しい品目がポリシーセットの最上部に配置されます。

新しいポリシーに名前を付け、FMC IPアドレスに一致するRADIUS NAS-IP-Address属性の上位条件を追加します。

ORと一緒に使用して2番目の条件を追加し、FTDのIPアドレスを含めます。

Useをクリックして変更を保存し、エディタを終了します。

Conditions Studio

Library

Search by Name

5G

Catalyst_Switch_Local_Web_Authentication

Source FMC

Switch_Local_Web_Authentication

Switch_Web_Authentication

Wired_802.1X

Wired_MAB

Wireless_802.1X

Wireless_Access

Editor

Radius-NAS-IP-Address

Equals 192.168.192.60

OR

Radius-NAS-IP-Address

Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

ステップ 8.2 : 完了したら、Saveを押します。

Cisco ISE

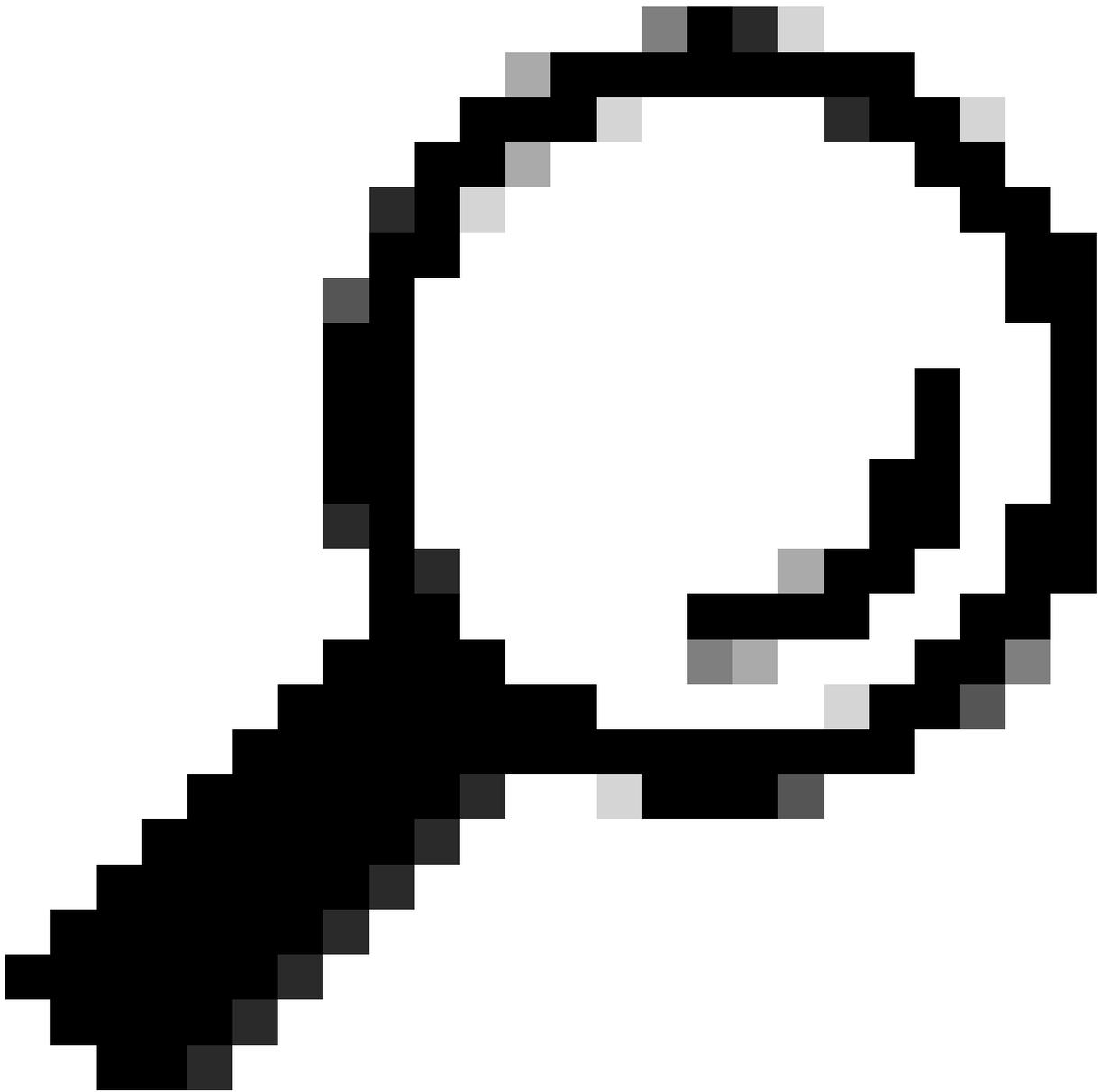
Policy > Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

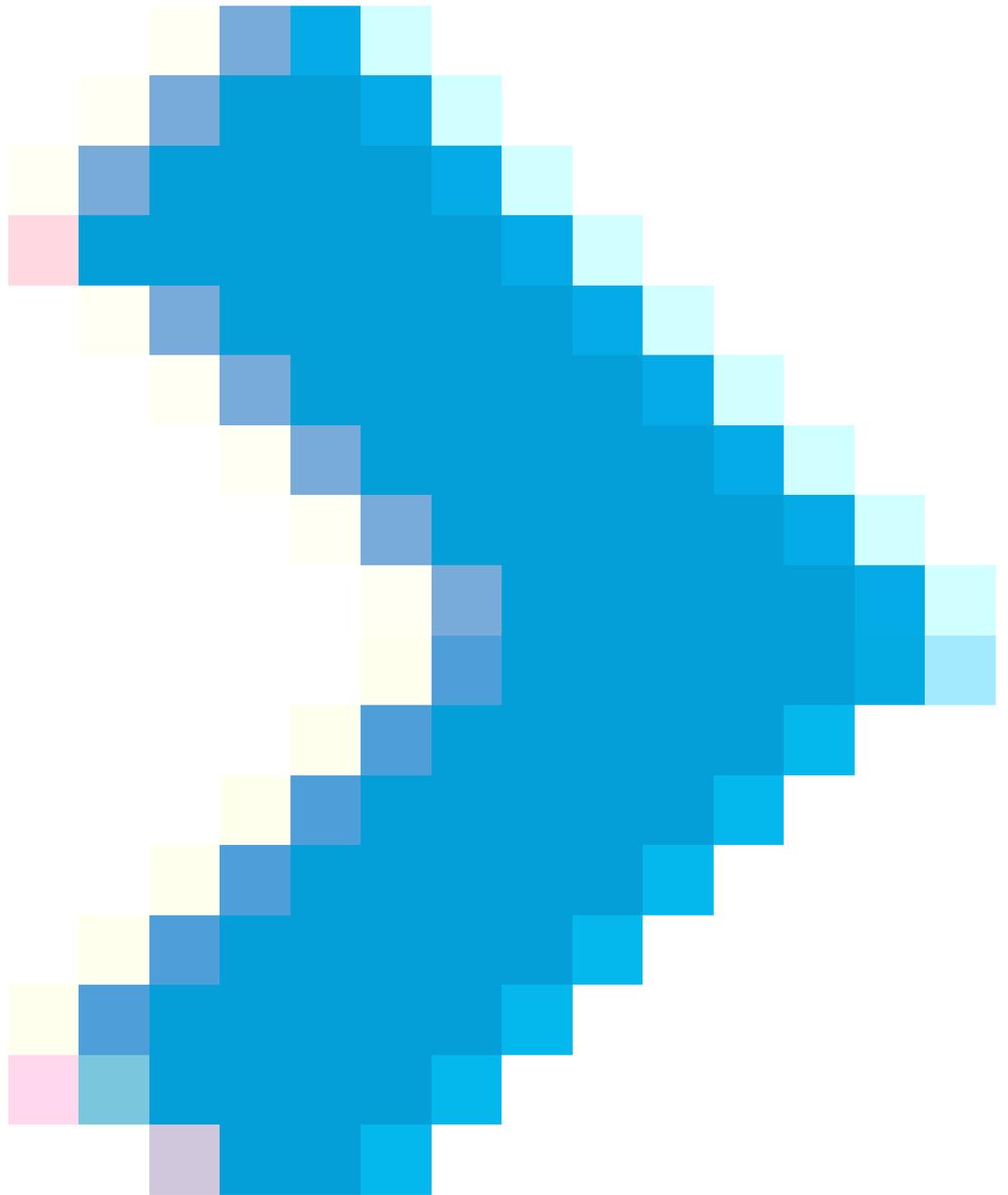
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0	⚙️	➔
✔	Default	Default policy set		Default Network Access	0	⚙️	➔

Reset Save



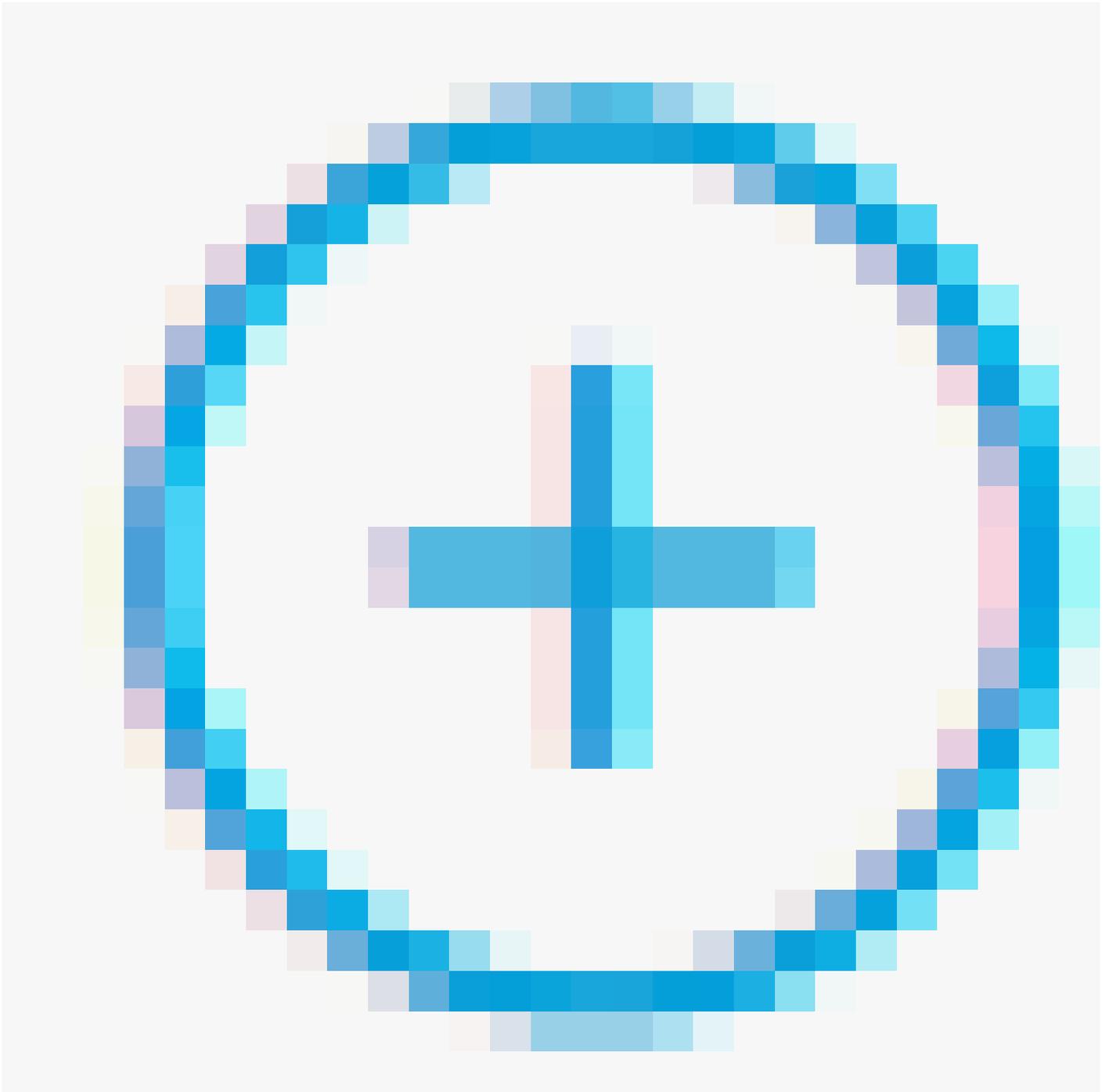
ヒント：この演習では、デフォルトのNetwork Access Protocolsリストを許可しています。新しいリストを作成し、必要に応じてリストを絞り込むことができます。

ステップ 9：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。

Authorization Policyメニューを展開し、



のアイコンを押して、管理者権限を持つユーザにアクセスを許可する新しいルールを追加します。

名前を指定します。

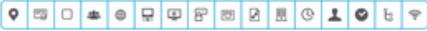
条件を設定して、Identity GroupとName Equals User Identity Groups: FMC and FTD admins (ステップ4で作成したグループ名) という属性を持つディクショナリを照合し、Useをクリックします。

Conditions Studio



Library

Search by Name



- 5G
- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- FMC and FTD Admin

Editor

IdentityGroup Name

Equals User Identity Groups:FMC and FTD admins

Set to 'is not'

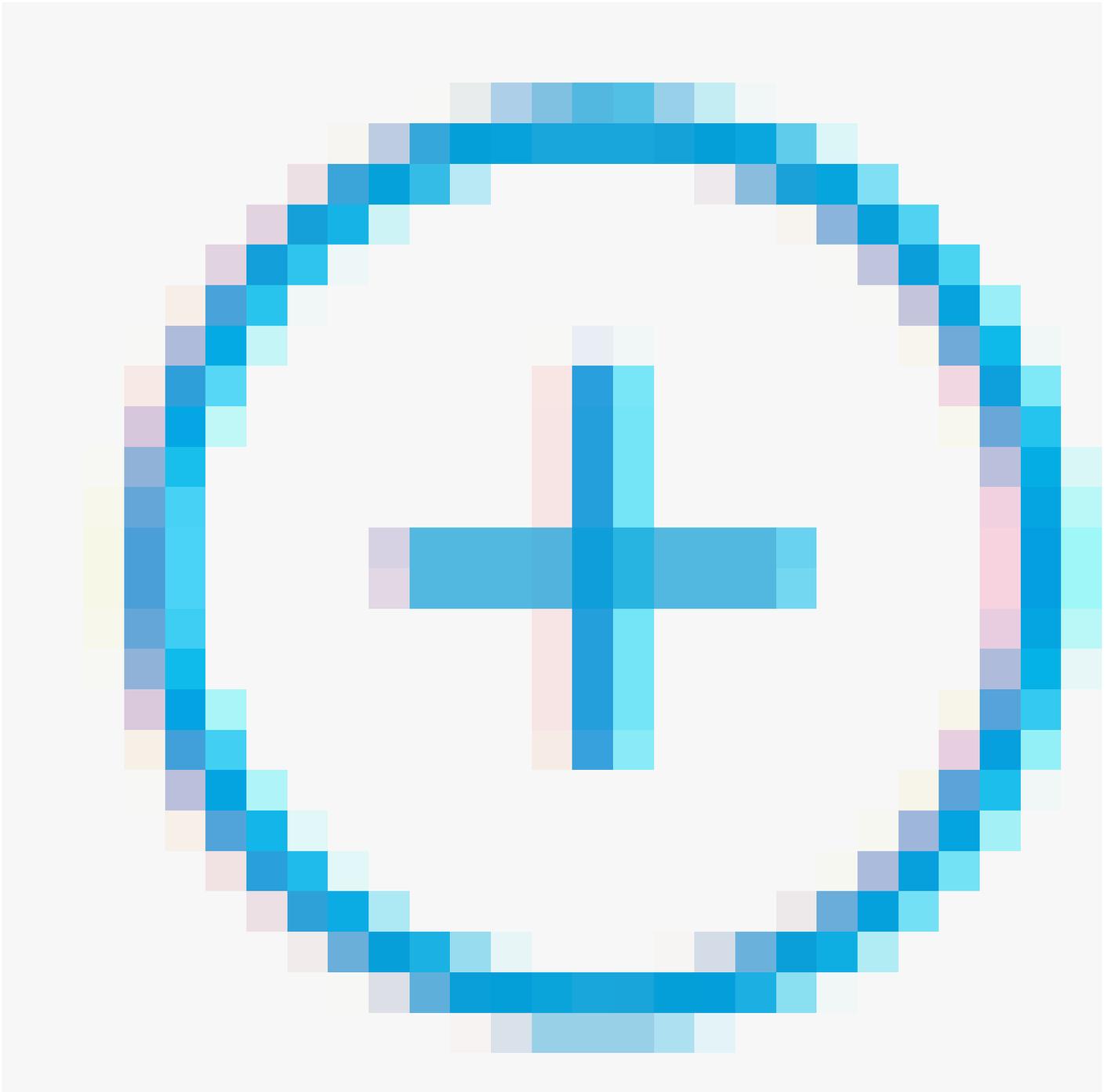
Duplicate Save

NEW AND OR

Close



ステップ 10 : 読み取り専用権限を持つユーザにアクセスを許可する2番目のルールを追加するには、



アイコンをクリックします。

名前を指定します。

条件を設定して、Identity GroupというディクショナリとName Equals User Identity Groups: FMCおよびFTD ReadOnly (手順4で作成したグループ名) を照合し、Useをクリックします。

Conditions Studio

Library

Search by Name



- 5G
- BYOD_Is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices

Editor

IdentityGroup-Name

Equals User Identity Groups:FMC and FTD - ReadOnly

Set to 'Is not'

Duplicate Save

NEW AND OR

Close



ステップ 11各ルールの認可プロファイルをそれぞれ設定し、Saveをクリックします。

Cisco ISE

Policy - Policy Sets

Policy Sets -> FMC and FTD Access

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
✓	FMC and FTD read user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly	FMC and FTD ReadUser	Select from list	0	⚙️	
✓	FMC and FTD admin user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins	FMC and FTD Admins	Select from list	0	⚙️	
✓	Default		DenyAccess	Select from list	0	⚙️	

Reset



FMCの設定

ステップ 1 : System > Users > External Authentication > + Add External Authentication Objectの順に選択し、外部認証オブジェクトを作成します。

Firewall Management Center
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ 👤 admin 🔒 cisco SECURE

Users User Roles External Authentication Single Sign-On (SSO)

Save Cancel Save and Apply

Default User Role: None Shell Authentication: Disabled

+ Add External Authentication Object

Name	Method	Enabled
No data to Represent		

ステップ 2 : 認証方式としてRADIUSを選択します。

External Authentication Objectで、新しいオブジェクトにNameを指定します。

次に、プライマリサーバ設定で、ISE IPアドレスと、ISE設定のステップ2で使用したのと同じRADIUS秘密鍵を挿入します。

Firewall Management Center
System / Users / Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ 👤 admin 🔒 cisco SECURE

Users User Roles External Authentication Single Sign-On (SSO)

External Authentication Object

Authentication Method: RADIUS

Name: ISE_Radius

Description:

Primary Server

Host Name/IP Address: 192.168.192.90 (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address: (ex. IP or hostname)

Port: 1812

RADIUS Secret Key:

RADIUS-Specific Parameters

Timeout (Seconds): 30

ステップ 3 : ISE設定のステップ6と7で設定したRADIUS Class属性の値 (firewall_adminには Administrator、 firewall_readuserにはReadUser) を挿入します。

RADIUS-Specific Parameters

Timeout (Seconds)

Retries

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

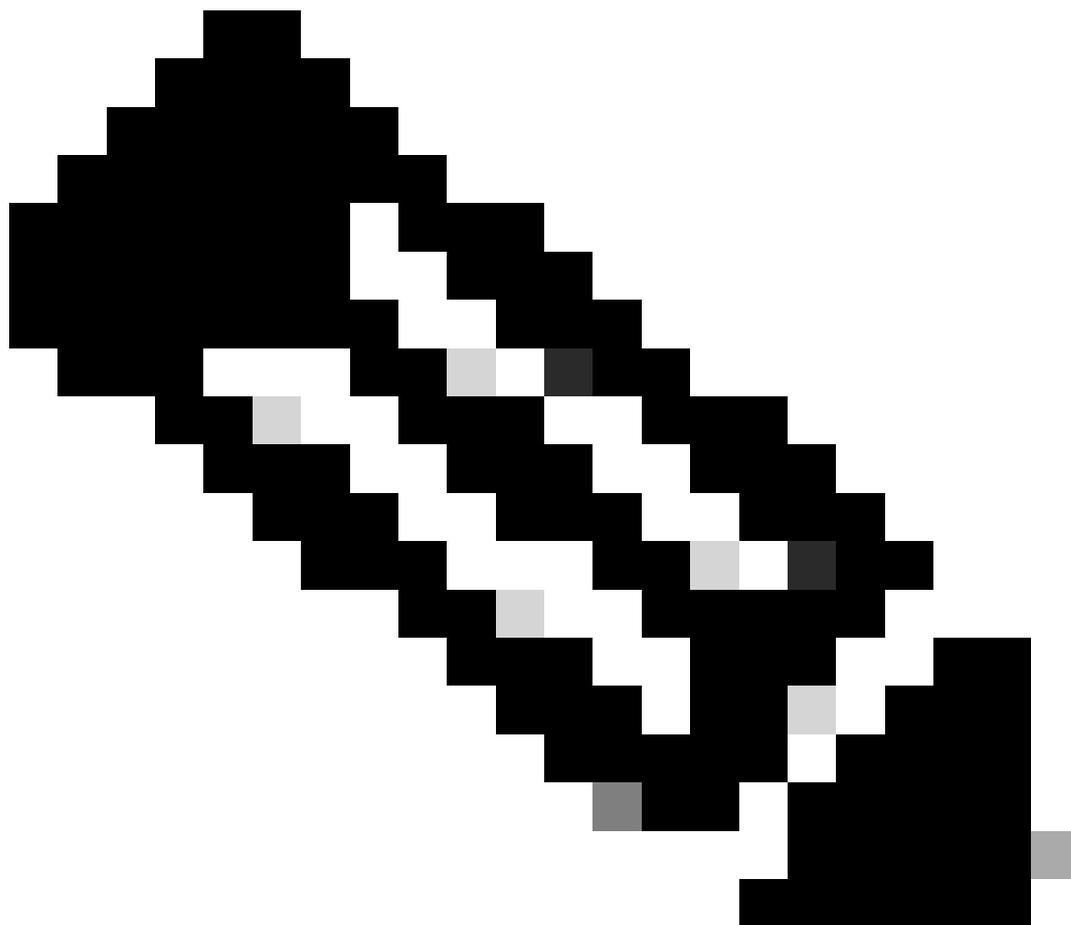
Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

To specify the default user role if user is not found in any group



注：タイムアウトの範囲はFTDとFMCとで異なります。そのため、オブジェクトを共有する場合にデフォルト値の30秒を変更するときは、FTDデバイスのタイムアウトの範囲を小さく（1～300秒）設定することを忘れないでください。タイムアウトを大きい値に設定すると、脅威対策のRADIUS設定が機能しません。

ステップ 4：CLIアクセスフィルタの下にあるAdministrator CLI Access User Listに、CLIアクセスを許可されるユーザ名を入力します。

完了したら、Saveをクリックします。

CLI Access Filter
 (For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

ステップ 5：新規オブジェクトを有効にします。これをFMCのシェル認証方式として設定し、Save and Applyをクリックします。

Firewall Management Center
 System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🌐 ⚙️ 👤 admin 🔒 **SECURE**

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Enabled (ISE_Radius) + Add External Authentication Object

Name	Method	Enabled	
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>	

FTD の設定

ステップ 1：FMC GUIで、Devices > Platform Settingsの順に移動します。アクセスするFTDが割り当てられていない場合は、現在のポリシーを編集するか、新しいポリシーを作成します。External Authenticationの下のRADIUSサーバをイネーブルにし、Saveをクリックします。

Firewall Management Center
 Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🌐 ⚙️ 👤 admin 🔒 **SECURE**

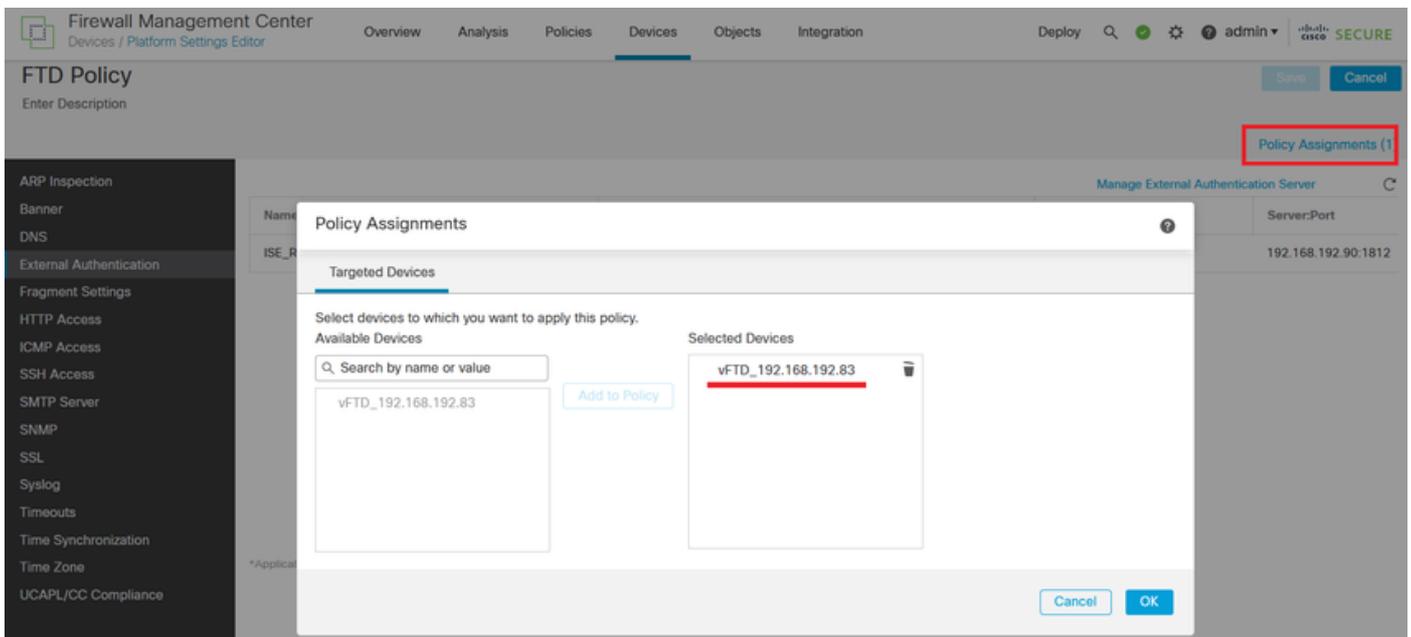
FTD Policy
 Enter Description

You have unsaved changes

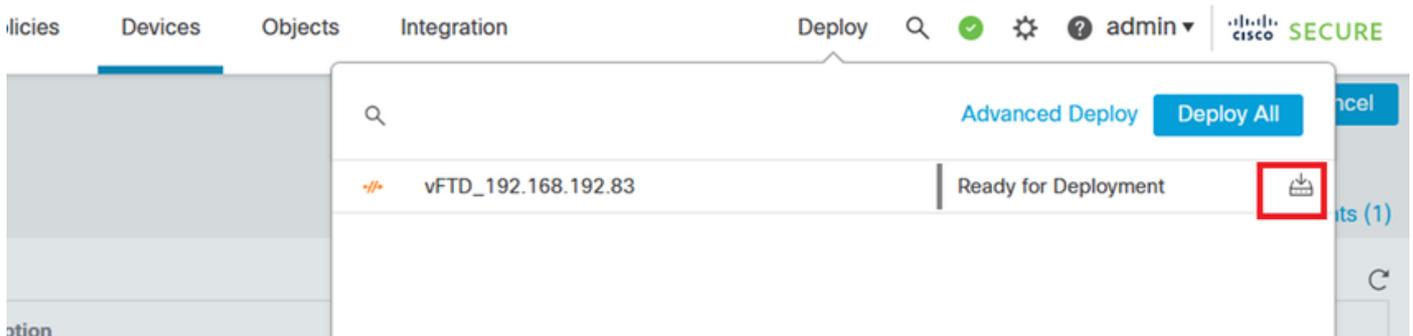
Policy Assignments (1)

Manage External Authentication Server					
Name	Description	Method	Server/Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

ステップ 2：アクセスする必要があるFTDがPolicy Assignments as a Selected Deviceの下に表示されていることを確認します。



ステップ 3 : 変更を展開します。



確認

- 新しい展開が正常に動作していることをテストします。
- FMCのGUIで、RADIUSサーバの設定に移動し、Additional Test Parametersセクションまでスクロールダウンします。
- ISEユーザのユーザ名とパスワードを入力し、Testをクリックします。



- テストに成功すると、ブラウザウィンドウの上部に「Success Test Complete」というメッセージが緑色で表示されます。



Success
Test Complete.

External Authentication Object

Authentication Method

Name *

- 詳細は、テスト出力の下のDetailsを展開すると表示されます。

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

Test Output

Show Details ▾

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

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。