# Cisco Identity Service Engine(Radius)を使用した AsyncOS外部認証

# 内容

```
概要
前提条件
要件
使用するコンポーネント
背景説明
設定
ネットワーク図
ステップ1:認証用のIDグループの作成
ステップ2:認証用のローカルユーザの作成
ステップ3:許可プロファイルを作成します。
ステップ4:許可ポリシーを作成します。
確認
トラブルシュート
関連情報
```

# 概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)/セキュリティ管理アプライ アンス(SMA)とCisco Identity Services Engine(ISE)の間で、RADIUSによる外部認証の正常な実装 に必要な設定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。

- •認証、許可、アカウンティング(AAA)
- RADIUSクラス属性。
- Cisco ISE Identity Management and Authorization Policies]を参照してください。
- Cisco ESA/SMAのユーザロール。

## 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。

- Cisco ISE 2.4
- Cisco ESA 13.5.1、13.7.0
- Cisco SMA 13.6.2

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、初期(デフォルト)設定の状態から起動しています 。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。

#### 関連製品

使用するコンポーネントのセクションに記載されていないバージョンはテストされていません。

# 背景説明

RADIUS CLASS属性

アカウンティングに使用される値は、RADIUSサーバがすべてのアカウンティングパケットに含める任意の値です。

クラス属性は、グループごとにISE(RADIUS)で設定されます。

ユーザが、属性25が関連付けられたISE/VPNグループの一部であると見なされると、NACは Identity Services Engine(ISE)サーバで設定されたマッピングルールに基づいてポリシーを適用し ます。

# 設定

#### ネットワーク図



Identity Service Engine(ISE)は、ESA/SMAからの認証要求を受け入れ、ユーザIDおよびグループ と照合します。

### ステップ1:認証用のIDグループの作成

ISEサーバにログインし、IDグループを作成します。

[Administration] > [Identity Management] > [Groups] > [User Identity Group]に移動します。図に示 すように。



**注**:割り当てられた各ESA/SMAロールに対して、ISEのアイデンティティグループを使用することを推奨します。

#### ステップ2:認証用のローカルユーザの作成

この手順では、新しいユーザを作成するか、ステップ1で作成したIDグループにすでに存在するユ ーザを割り当てます。ISEにログインし、[Administration] > [Identity Management] -> [Identities]に 移動し、新しいユーザを作成するか、グループのユーザにを割割割割指定します。図に示すよう に。

Network Access Users List > New Networ	k Access User	
<ul> <li>Network Access User</li> </ul>		
* Name ESA admin		
Status 🔽 Enabled 👻		
Email admins@mydomain.com		
▼ Passwords		
Password Type: Internal Users	•	
Password	Re-Enter Password	
* Login Password		Generate Password (i)
Enable Password		Generate Password
<ul> <li>User Information</li> </ul>	User Groups	
First Name		
Last Name	ALL_ACCOUNTS (default)	
	Anyconnect	
<ul> <li>Account Options</li> </ul>	Dot1X	
	Employee	
Description	ESA_Admin	///
Change password on next login $\Box$	ESA_DEMO	
	ESA_Diego_Admins	
<ul> <li>Account Disable Policy</li> </ul>		
	GROUP_ACCOUNTS (default)	
Disable account if date exceeds	SuestType_Contractor (default)	/y-mm-dd)
▼ User Groups		
Select an item		
Submit Cancel		

#### ステップ3:許可プロファイルを作成します。

RADIUS認証は、許可プロファイルなしで正常に完了できますが、ロールは割り当てられません 。設定を完了するには、[ポリシー] -> [ポリシー要素] -> [結果] -> [承認] -> [承認プロファイル]に 移動します。 **注**:割り当てるロールごとに1つの認可プロファイルを作成します。

Authorization Profiles > Aav	ega_ESA_Admin
Authorization Profile	
* Name	ESA_Admin
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	dalle Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
- Common Tacks	
Web Authentication (	Local Web Auth)
Airespace ACL Name	•
🗹 ASA VPN	Administrators
AVC Profile Name	
Advanced Attribute	es Settings
Select an item	

**注**:radiusクラス属性25を使用して名前を付けます。この名前は、AsyncOS(ESA/SMA)の 設定と一致している必要があります。 図3から、AdministratorsはCLASS属性名です。

### ステップ4:許可ポリシーを作成します。

この最後の手順では、ISEサーバがユーザログインの試行を識別し、正しい認可プロファイルに マッピングできるようにします。

認可が成功すると、ISEは認可プロファイルに定義されたCLASS値に沿ってaccess-acceptを返し ます。 [Policy] > [Policy Sets] > [Add] (+記号)に移動します。

l	+	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence	Hits	Actions	View
I	Search									
	/	ø	New Policy Set 1			+	Select from list		٥	>

名前を割り当て、プラス記号を選択して必須条件を追加します。このラボ環境では、RADIUSを 使用します。nas-ip-address.新しいポリシーを保存します。

-1] C	sco Ide	entity Se	rvices Engine	Home >	Context Visibility	Operations	▼ Policy	Administration	Work Centers		1	License Warr	ning 🔺			0	
	Policy Se	ets Pro	filing Posture	Client Provisionin	ng	ents					Click here to	do visibility setur	Do not s	how thi	is again.	,	×
P	olicy	Sets									Reset	Policyset Hit	counts		Reset	Save	0
	+	Status	Policy Set Nan	10	Description		Condition	ns		Allow	ed Protocols /	Server Seque	nce	Hits	Actions	Vie	w
	Search																
		0	ESA_Policy				₽ N	etwork Access-Device I	P Address EQUALS 10.122	.111.238 Defa	ult Network Acce	HSS X Y	+	16	٥	>	•

認可要求を正しく一致させるには、条件を追加する必要があります。**選択** アイコンと条 件の追加

ラボ環境では、InternalUser-IdentityGroupを使用し、各認可プロファイルに一致します。

► Auth	orization F	Policy (5)							
					Results				
+	Status	Rule Name	Cond	itions	Profiles	Security Groups		Hits	Actions
Searc	h								
	Ø	ESA Monitor	幽	InternalUser-IdentityGroup EQUALS User Identity Groups:ESA_Monitor	×ESA_Monitors +	Select from list	- +	0	٥
	0	ESA HelpDesk	忠	InternalUser-IdentityGroup EQUALS User Identity Groups:HelpDesk	KESA_admin +	Select from list	• +	0	¢

ステップ5:AsyncOS ESA/SMAへの外部認証を有効にします。

AsyncOSアプライアンス(ESA/SMA/WSA)にログインします。 次に、[System Administration] > [Users] > [External Authentication] > [Enable External Authentication on ESA]に移動します。

#### **Edit External Authentication**

External Authentication Settings	
Enable External Authentication	
Cancel	Submit

次の値を指定します。

- RADIUSサーバのホスト名
- ポート
- 共有秘密
- •タイムアウト値(秒)
- 認証プロトコル

[外部認証さ**れたユーザーを複数のローカルロールにマップする(推奨)]を選択します**。 図に示 すように。

#### **Edit External Authentication**

External Authentication Settings								
C Enable External Authentication								
Authentication Type:	RADIUS 🟮							
RADIUS Server Information:	RADIUS Server Hostname	Port	Share	ed Secret	Timeout Value (in seconds)	Authent	ication I	Add Row
	x.x.x.x	1812	••••	••••	5	PAP	0	Ŵ
External Authentication Cache Timeout: $\textcircled{O}$	0 seconds							
Group Mapping:	Map externally auther	nticated u	sers to	multiple local ro	oles. (recomme	ended)		
	RADIUS CLASS Att	ribute		Role 🥐			A	dd Row
	Administrators			Administrator	r 🟮			Ŵ
	Monitors			Operator	0			Ŵ
	RADIUS CLASS attr	ibutes are	e case-s	ensitive.				
	<ul> <li>Map all externally auth</li> </ul>	enticated	users t	o the Administr	ator role.			

**注**:RADIUS CLASS属性は、ステップ3で定義した属性Nameと一致する必要があります (ASA VPNとしてマップされる共通タスクの下)。

# 確認

ο

AsyncOSアプライアンスにログインし、アクセスが許可され、割り当てられたロールが正しく割 り当てられていることを確認してください。図に示すように、ゲストユーザロールを使用します

CISCO Email Sect	C000V urity Virtual Appliance			Email Security Applian	ce is getti
Monitor					
My Dashboard					
				🃜 Printable	PDF 🗗
					_
Attention — 📥 You o Somo > Ov	can customize this "My Dashboard" e modules are added for you by defa rerview.	page by addi ault. The Ove	ng report modules from different repo erview page can be accessed from Mor	orts. nitor	
Attention – A You Some > Ov	can customize this "My Dashboard" e modules are added for you by defa rerview.	page by addi ault. The Ove	ng report modules from different repo erview page can be accessed from Mor	nitor	
Attention – A You o Som > Ov System Overview Overview > Status	can customize this "My Dashboard" e modules are added for you by defa rerview.	page by addi ault. The Ove	ng report modules from different repo erview page can be accessed from Mor Overview > Quarantines - Top 3 by Disk	orts. nitor : Usage (Policy and Virus)	•
Attention – A You o Somo Somo > Ov System Overview Overview > Status	can customize this "My Dashboard" e modules are added for you by defa rerview. System Status:	page by addi ault. The Ove	ng report modules from different repo erview page can be accessed from Mor Overview > Quarantines - Top 3 by Disk No quarantines are available	orts. nitor Usage (Policy and Virus)	Ð
Attention – A You Some > Ov System Overview Overview > Status	can customize this "My Dashboard" e modules are added for you by defa rerview. System Status: Incoming Messages per hour:	page by addi ault. The Ove	ng report modules from different repo erview page can be accessed from Mor Overview > Quarantines - Top 3 by Disk No quarantines are available	utsage (Policy and Virus)	+
Attention – A You G Som > Ov System Overview Overview > Status	can customize this "My Dashboard" e modules are added for you by defa rerview. System Status: Incoming Messages per hour: Messages in Work Queue:	page by addi ault. The Ove Solution Solution Online 0 0	ng report modules from different repo erview page can be accessed from Mor Overview > Quarantines - Top 3 by Disk No quarantines are available	orts. nitor	•



ログイン試行が「Invalid username or password」というメッセージでESAで動作しない場合。この問題は、認可ポリシーに関する問題である可能性があります。

ESAにログインし、[External Authentication]から[Map all externally authenticated users to the Administrator role]を選択します。

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

変更を送信し、保存します。新しいログインを試みます。ログインに成功した場合は、ISE RADIUS認可プロファイル(CLASS属性25)と認可ポリシーの設定を再確認します。

<u>ISE 2.4</u><u>AsyncOS</u>