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

内容

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

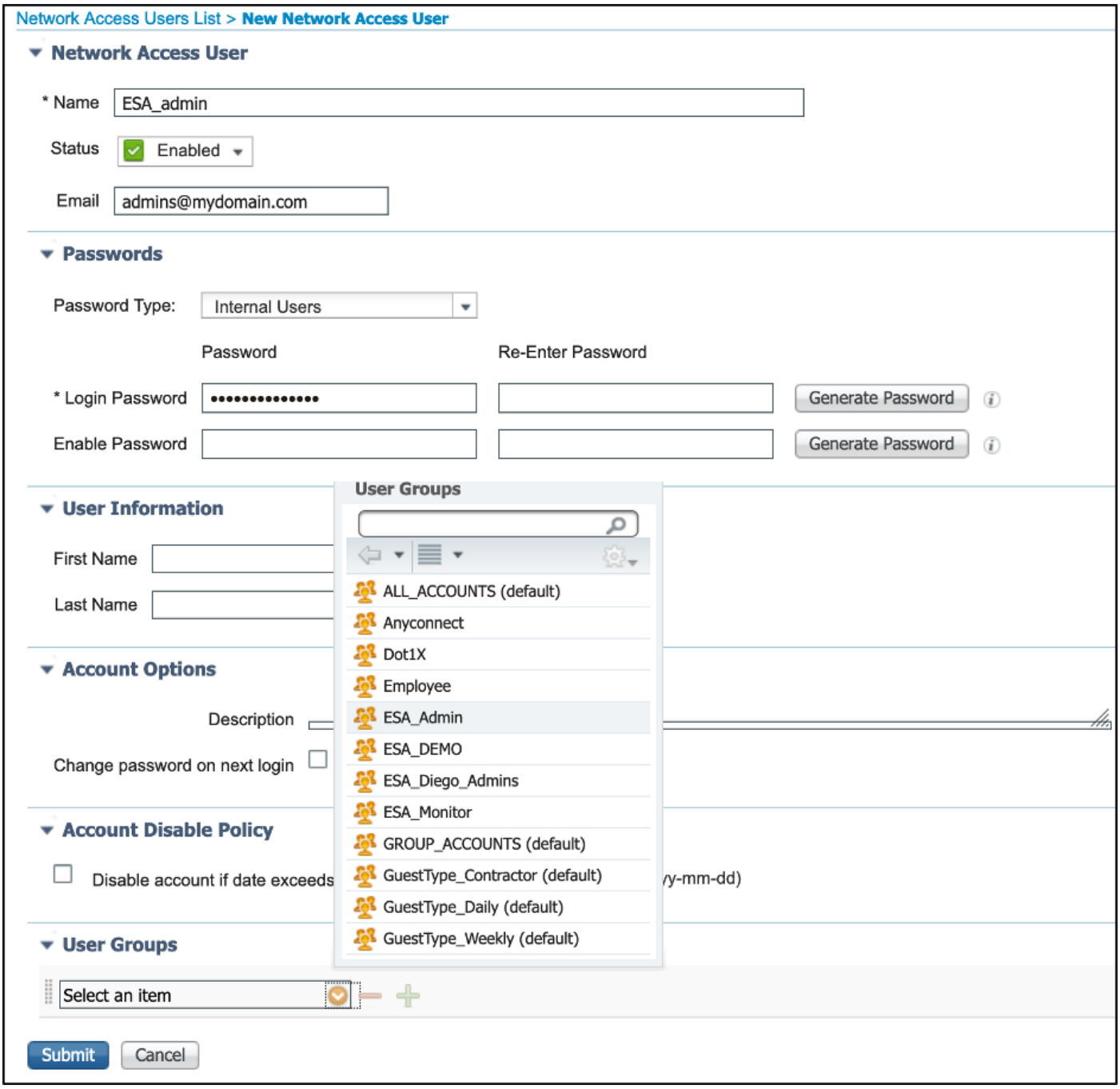
ISEサーバにログインし、IDグループを作成します。

[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

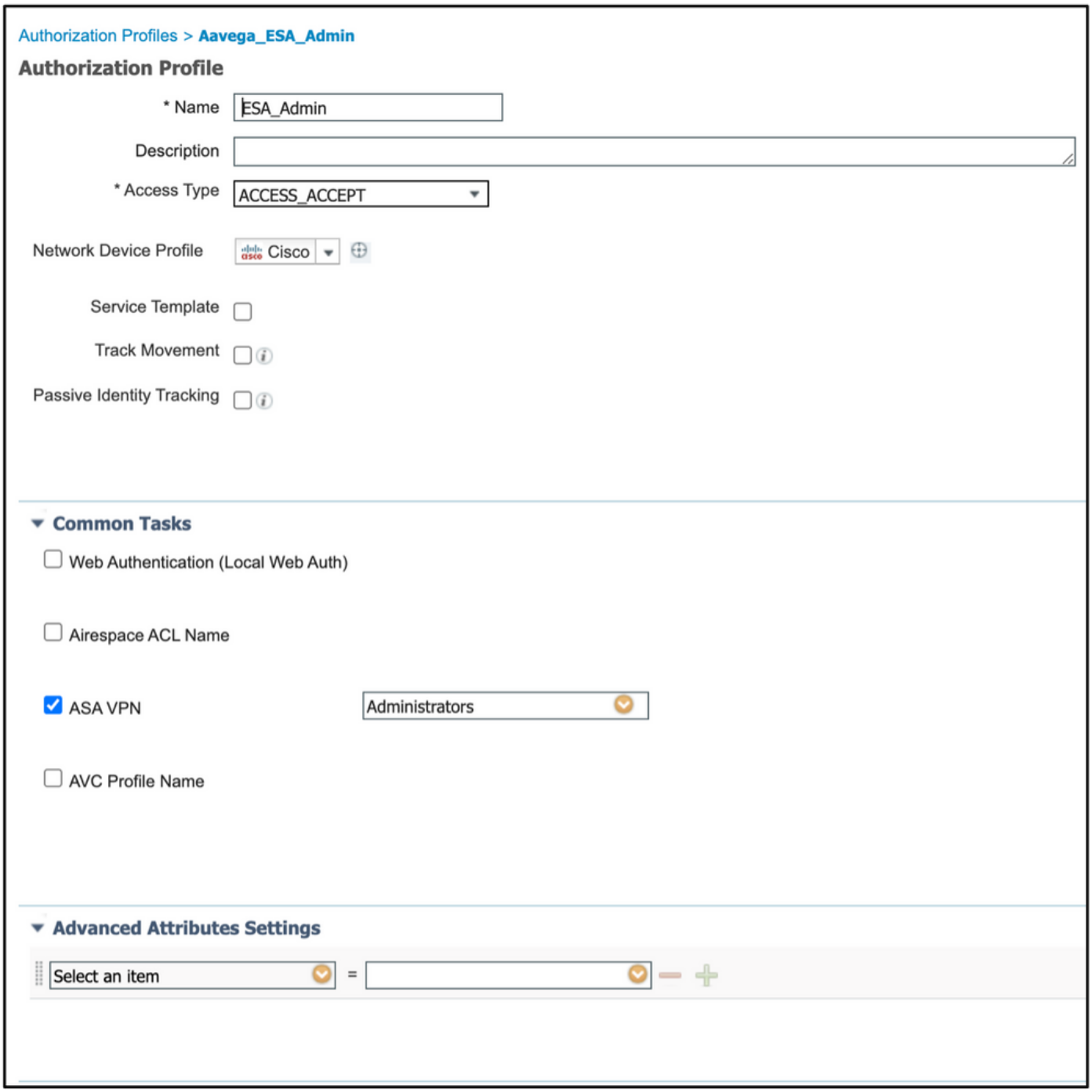
この手順では、新しいユーザを作成するか、ステップ1で作成したIDグループにすでに存在するユーザを割り当てます。ISEにログインし、**[Administration] > [Identity Management] -> [Identities]に移動し、新しいユーザを作成するか、グループのユーザにを割割割割指定します。**図に示すように。



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。



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。

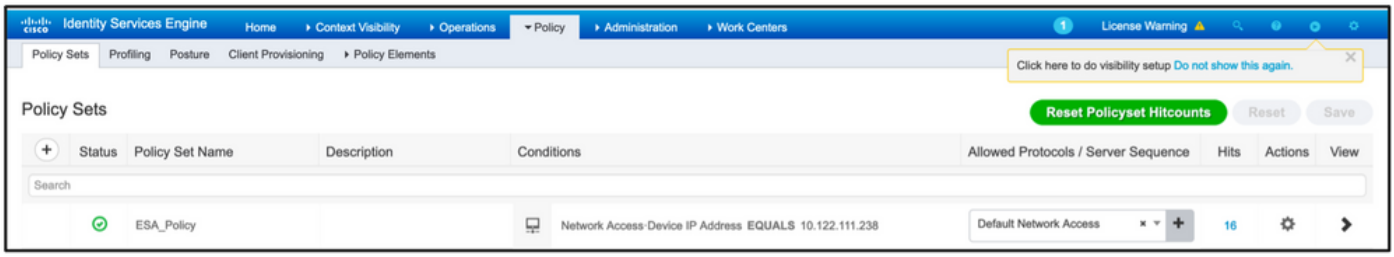
ステップ4：許可ポリシーを作成します。

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。

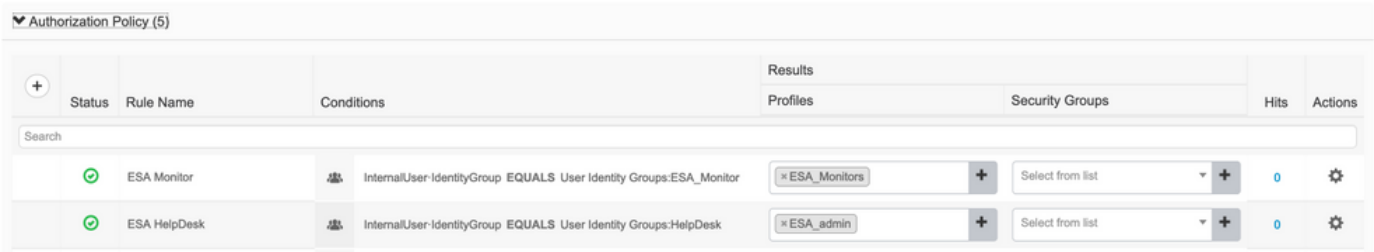
[Policy] > [Policy Sets] > [Add]（+記号）に移動します。

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。



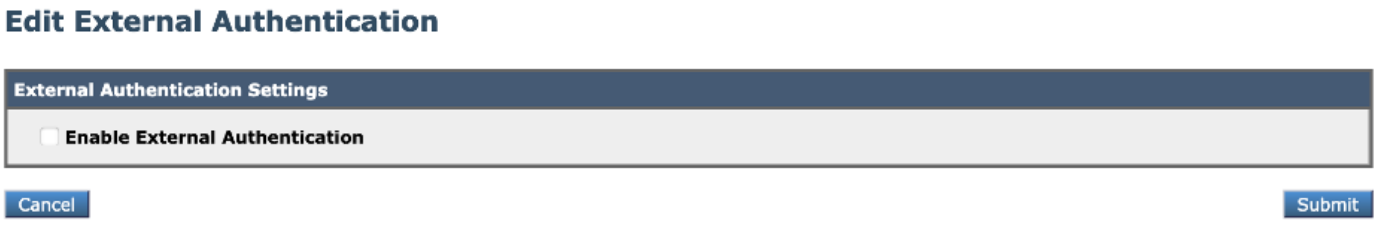
認可要求を正しく一致させるには、条件を追加する必要があります。**選択** アイコンと条件の追加

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。



ステップ5:AsyncOS ESA/SMAへの外部認証を有効にします。

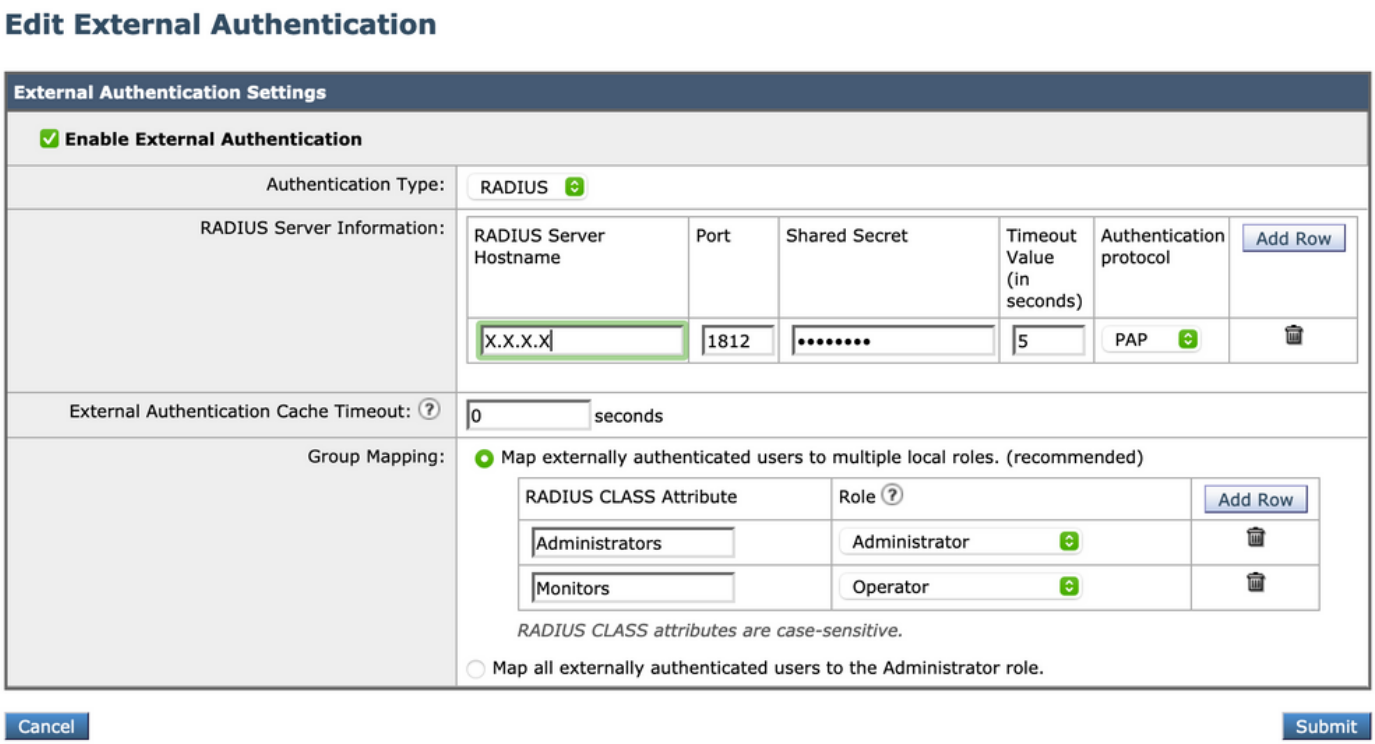
AsyncOSアプライアンス(ESA/SMA/WSA)にログインします。 次に、**[System Administration] > [Users] > [External Authentication] > [Enable External Authentication on** ESA]に移動します。



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

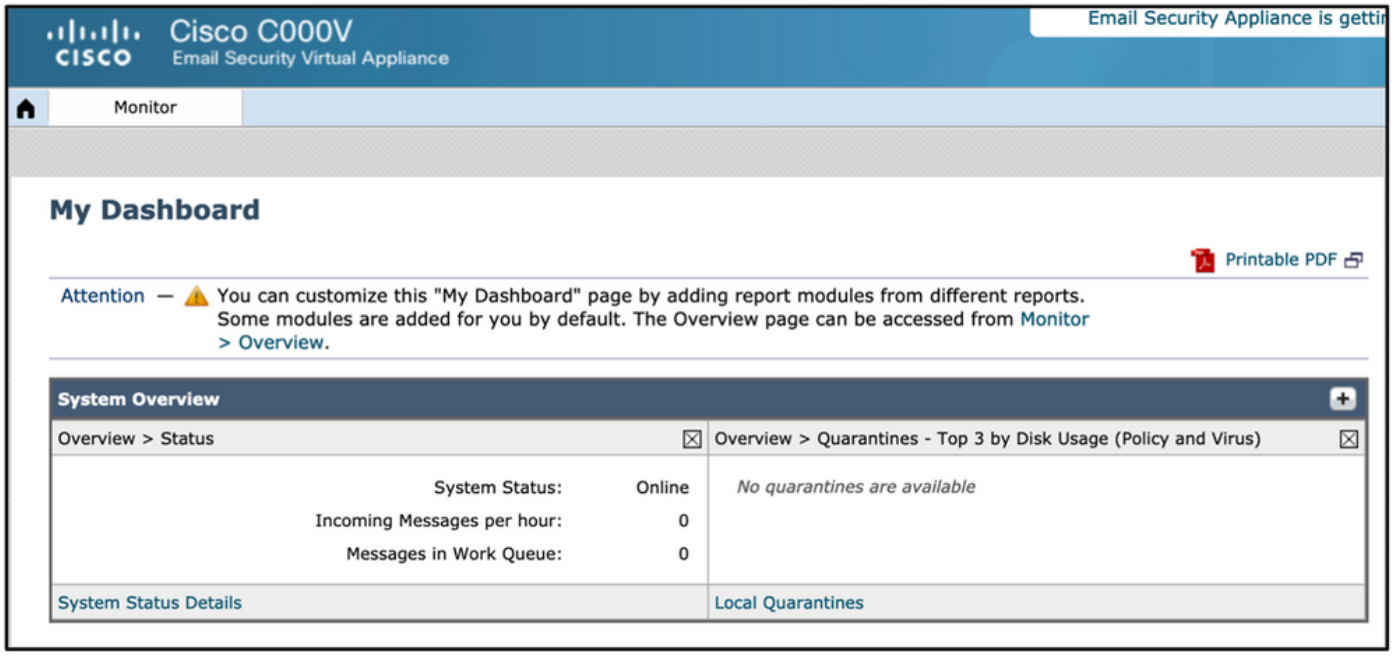
[外部認証さ**れたユーザーを複数のローカルロールにマップする（推奨）]を選択します。** 図に示すように。



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

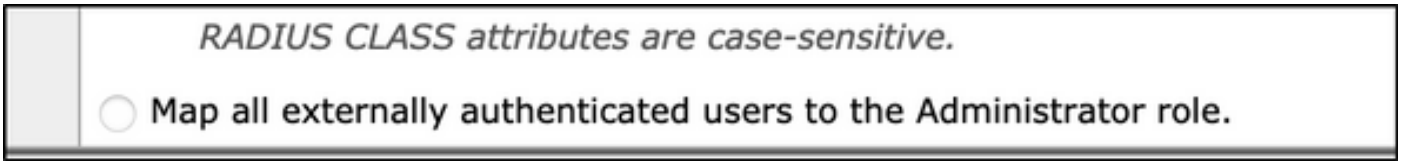
AsyncOSアプライアンスにログインし、アクセスが許可され、割り当てられたロールが正しく割り当てられていることを確認してください。図に示すように、ゲストユーザロールを使用します。



トラブルシュート

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。



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。

- ISE 2.4
- AsyncOS