使用思科身份服務引擎(Radius)的AsyncOS外部身份驗證

目錄

簡介

本檔案介紹在郵件安全裝置(ESA)/安全管理裝置(SMA)和思科身份服務引擎(ISE)之間成功實施使用RADIUS的外部身份驗證所需的配置。

必要條件

需求

思科建議您瞭解以下主題：

- 驗證、授權及記帳(AAA)
- RADIUS類屬性。
- Cisco ISE身份管理和授權策略。
- Cisco ESA/SMA使用者角色。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

未測試「使用的元件」部分中列出的版本以外的版本。

背景資訊

Radius CLASS屬性

用於記帳，這是RADIUS伺服器包含在所有記帳資料包中的任意值。

類屬性在ISE(RADIUS)中按組配置。

當使用者被視為其屬性為25的ISE/VPN組的一部分時，NAC根據身份服務引擎伺服器(ISE)中配置的對映規則實施策略。

設定

網路圖表

身份服務引擎接受來自ESA/SMA的身份驗證請求，並將其與使用者身份和組進行匹配。

步驟1.建立身份驗證的身份組。

登入ISE伺服器並建立身份組：

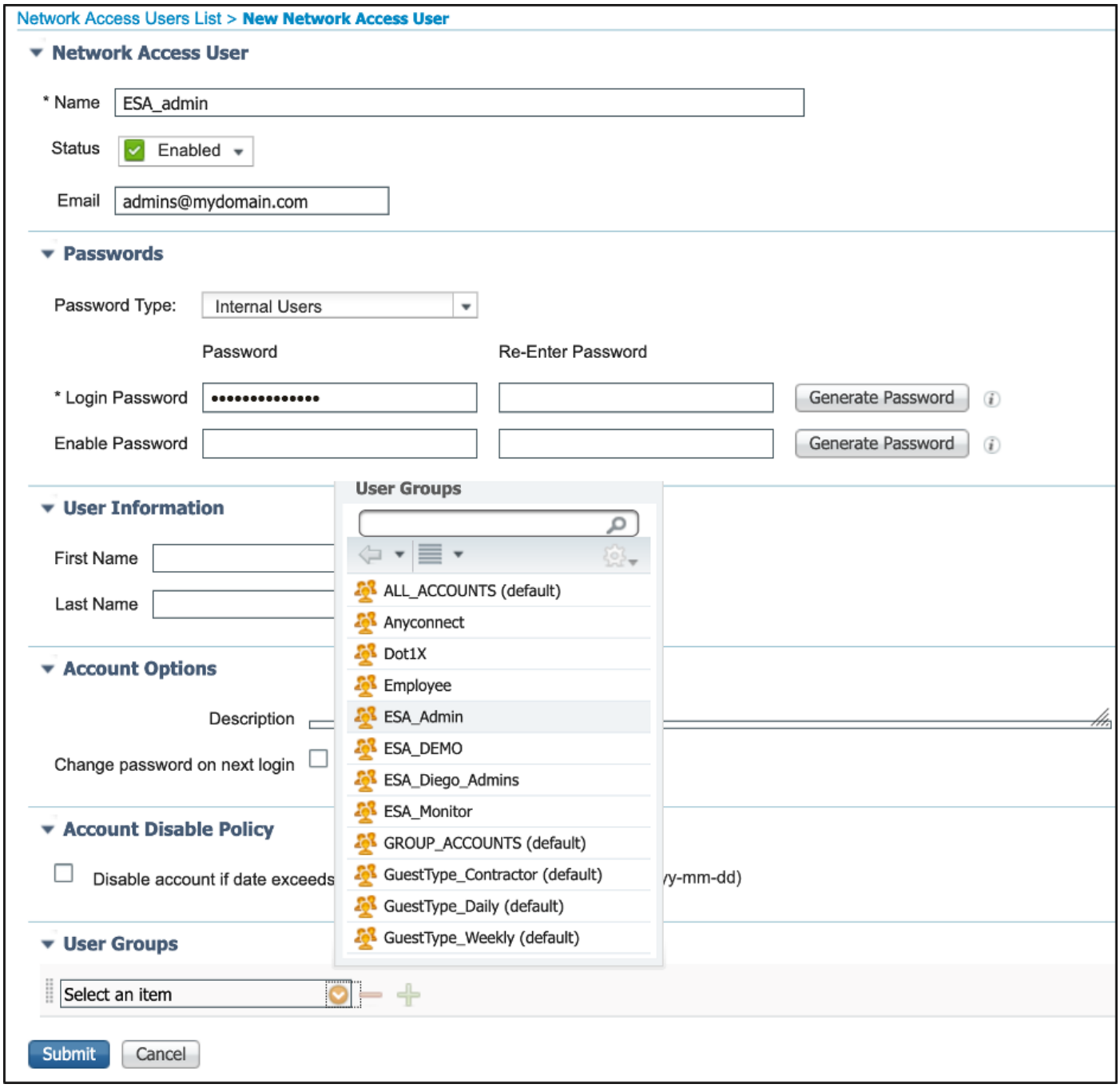
導航到Administration -> Identity Management -> Groups -> User Identity Group。如下圖所示。

附註：Cisco建議為分配的每個ESA/SMA角色在ISE中使用身份組。

步驟2.建立本地使用者以進行身份驗證。

在此步驟中，建立新使用者或分配已存在的使用者到我們在步驟1中建立的身份組。請登入到ISE並

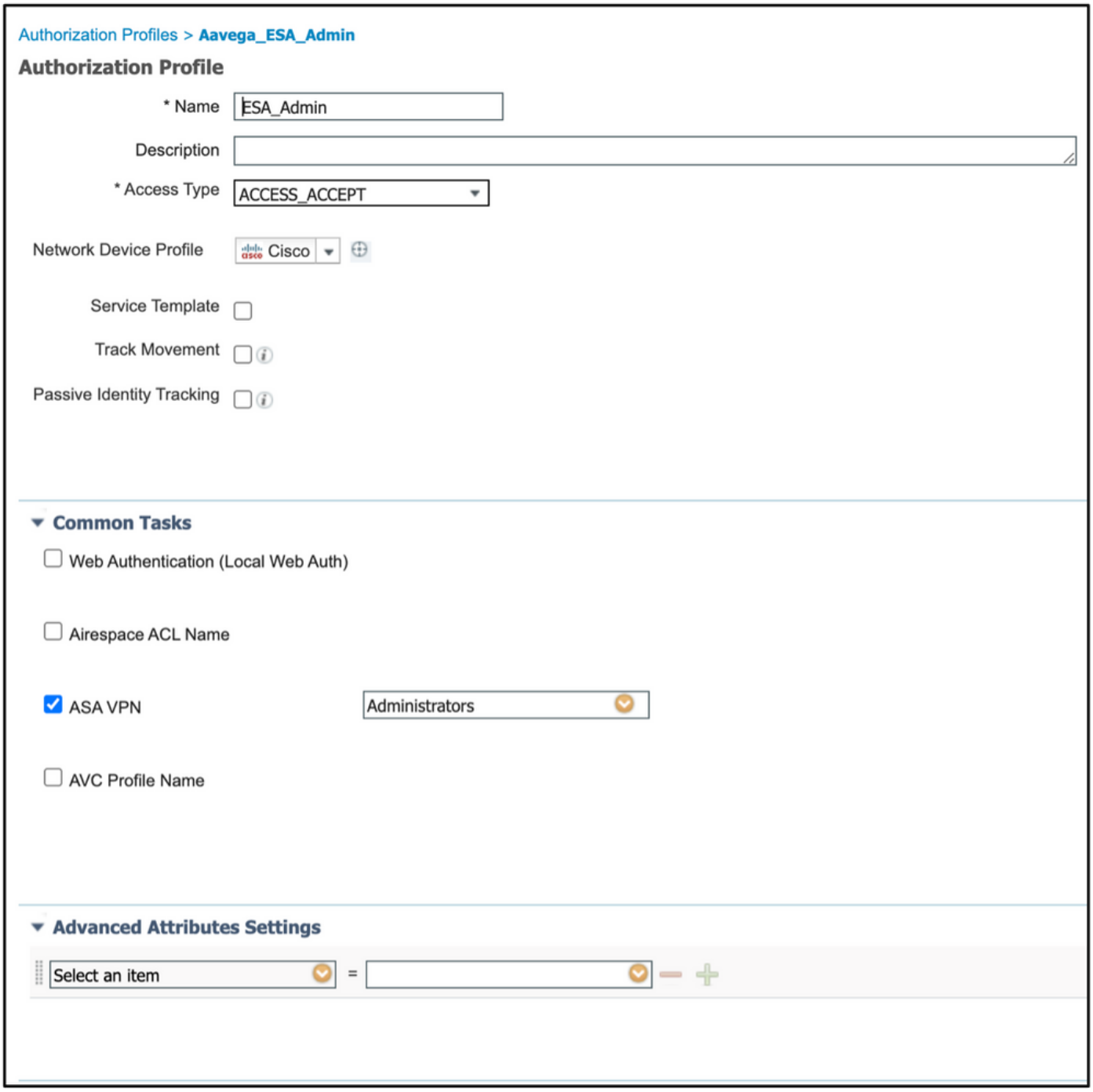
導航到Administration->Identity Management->Identities，然後建立新使用者或分配給您建立的組中的用戶。如下圖所示。



步驟3.建立授權配置檔案。

無需授權配置檔案即可成功完成RADIUS身份驗證，但不會分配角色。要完成設定，請導覽至Policy->Policy Elements->Results->Authorization->Authorization profile。

附註：為每個要分配的角色建立一個授權配置檔案。



附註：確保使用radius類屬性25並指定名稱。此名稱必須與AsyncOS(ESA/SMA)上的配置匹配。 在圖3中，管理員是CLASS屬性名稱。

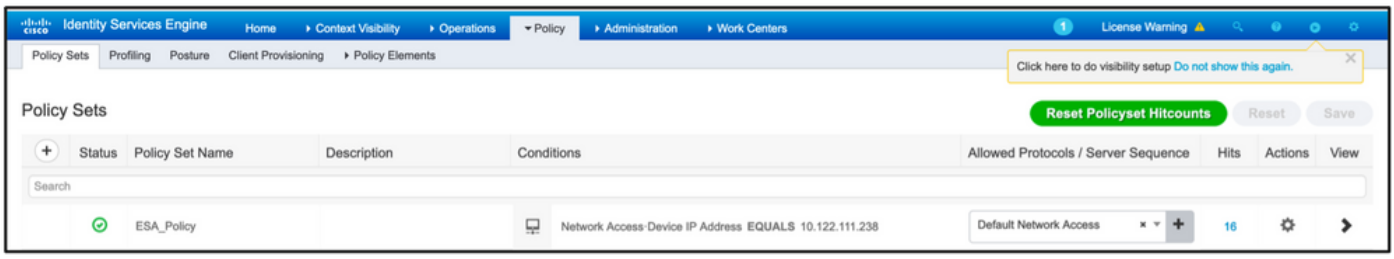
步驟4.建立授權策略。

最後一步允許ISE伺服器識別使用者登入嘗試並對映到正確的授權配置檔案。

在授權成功的情況下，ISE會返回一個訪問接受並沿授權配置檔案中的CLASS值定義。

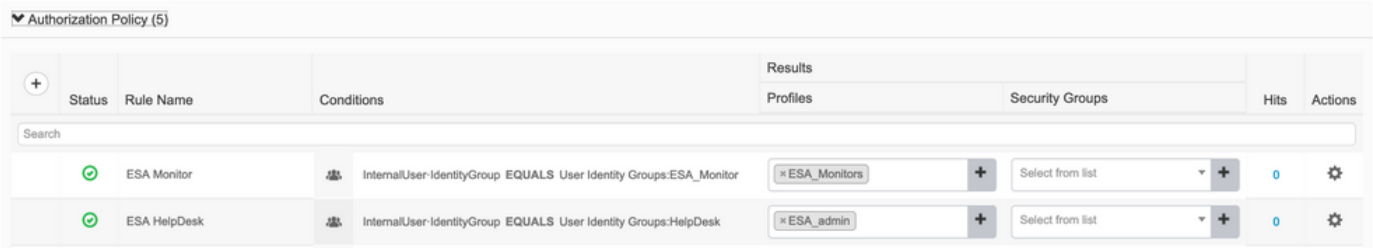
導航到Policy > Policy Sets > Add（ +符號 ）

指定名稱並選擇加號以新增所需的條件。本實驗環境使用Radius。NAS-IP-Address。儲存新策略。



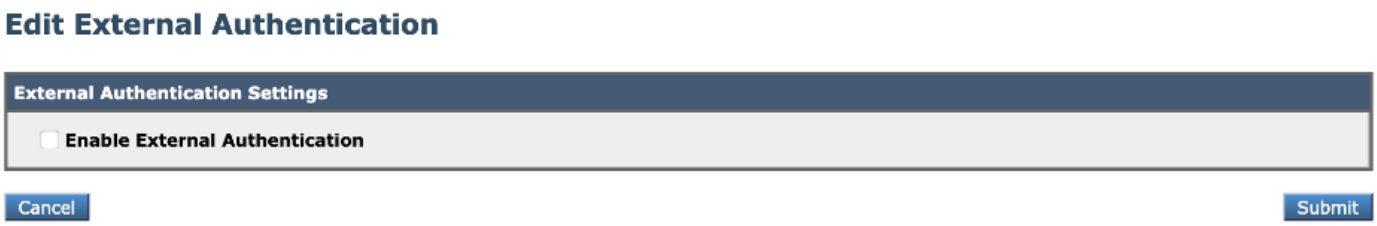
為了正確匹配授權請求，必須新增條件。**選擇** 圖示並新增條件。

實驗室環境使用InternalUser-IdentityGroup並匹配每個授權配置檔案。



步驟5.啟用對AsyncOS ESA/SMA的外部身份驗證。

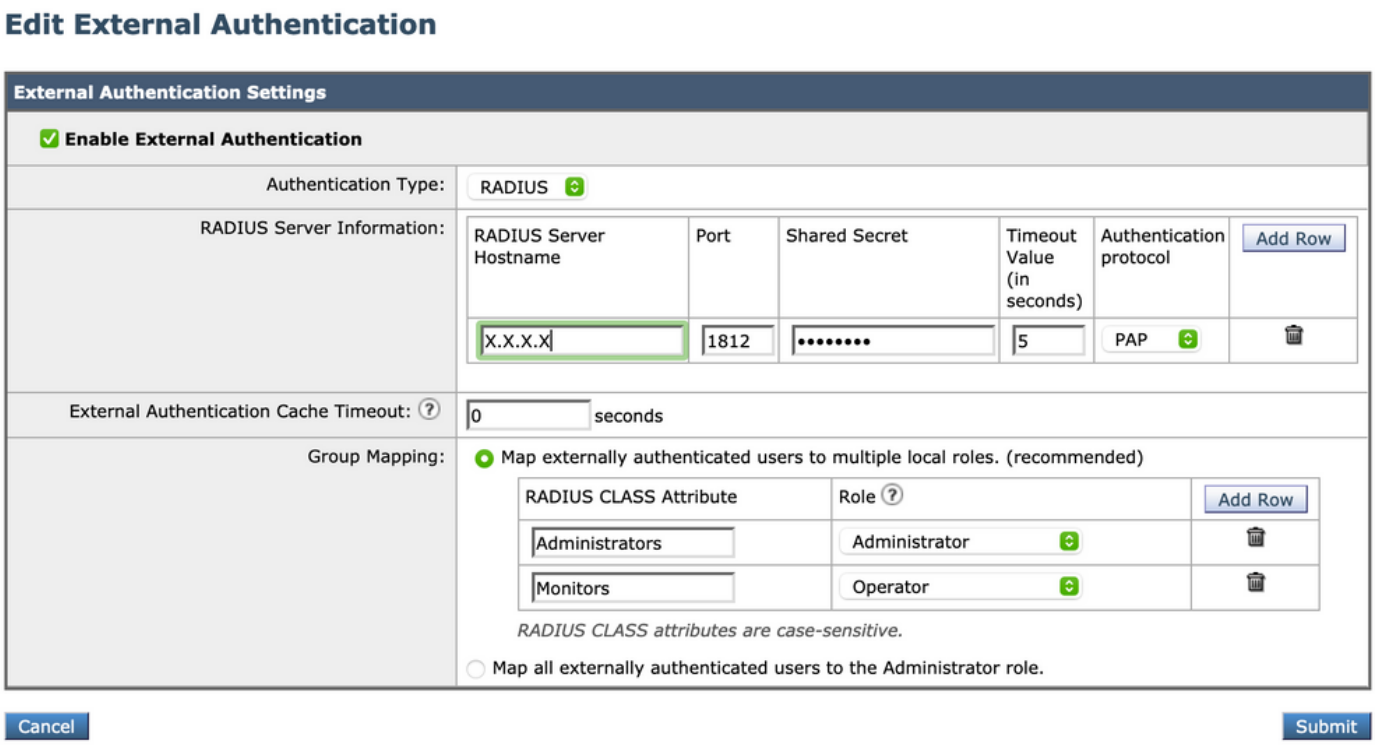
登入AsyncOS裝置(ESA/SMA/WSA)。 並**導航到System Administration > Users > External Authentication > Enable External Authentication** on ESA。



提供以下值：

- RADIUS伺服器主機名
- 連接埠
- 共用金鑰
- 超時值（秒）
- 驗證通訊協定

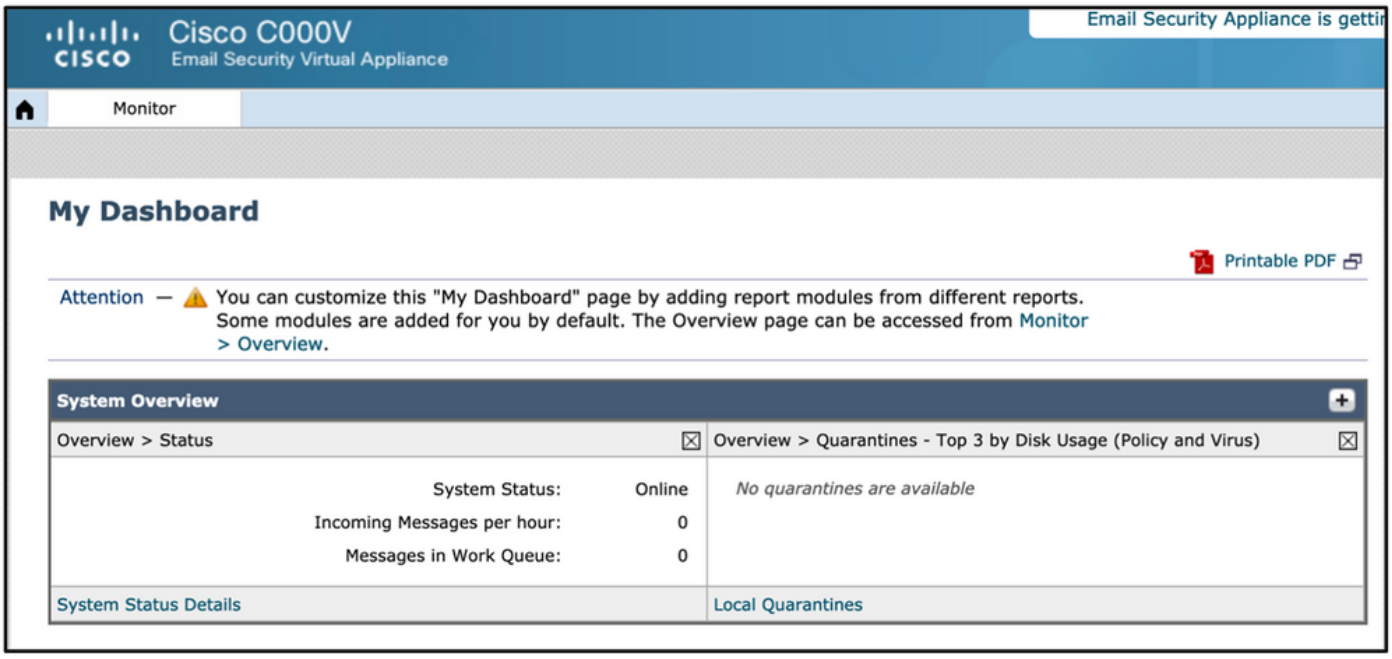
選擇**將外部身份驗證的使用者對映到多個本地角色（推薦）**。 如下圖所示。



附註：Radius CLASS Attribute MUST Match with the attribute Name defined in Step 3（在對映為ASA VPN的常見任務下）。

驗證

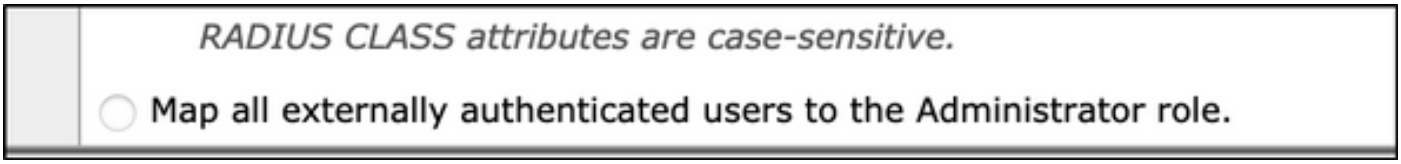
請登入您的AsyncOS裝置，確認已授予訪問許可權且已正確分配分配的角色。如圖所示，具有訪客使用者角色。



疑難排解

如果登入嘗試在ESA上失敗，則顯示消息「無效使用者名稱或密碼」。問題可能出在授權策略上。

登入到ESA，從External Authentication選擇Map all external authenticated users to the Administrator role。



提交並提交更改。進行新的登入嘗試。如果登入成功，請仔細檢查ISE Radius授權配置檔案（CLASS屬性25）和授權策略設定。

- ISE 2.4
- AsyncOS