AsyncOS externe verificatie met Cisco Identity Services Engine (RADIUS)

Inhoud

Inleiding

Dit document beschrijft de configuratie die vereist is tussen de E-mail security applicatie (ESA)/security applicatie (SMA) en Cisco Identity Services Engine (ISE) voor een succesvolle implementatie van externe verificatie met RADIUS.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Verificatie, autorisatie en accounting (AAA)
- RADIUS-CLASS kenmerk.
- Cisco ISE-beleid voor identiteitsbeheer en autorisatie.
- Cisco ESA/SMA-gebruikersrollen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE 2.4
- Cisco ESR 13.5.1, 13.7.0
- Cisco SMA 13.6.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Verwante producten

Versie buiten de genoemde onderdelen in het gebruikte deel werd niet getest.

Achtergrondinformatie

RADIUS-CLASS kenmerken

Gebruikt voor accounting, is het een willekeurige waarde die de RADIUS server in alle accounting pakketten bevat.

De klasseneigenschap wordt in ISE (RADIUS) ingesteld per groep.

Wanneer een gebruiker geacht wordt deel uit te maken van de ISE/VPN-groep die 25 aan de groep heeft gekoppeld, dwingt NAC het beleid af op basis van de geconfigureerde mapping-regels in de server van Identity Services Engine (ISE).

Configureren

Netwerkdiagram

Identity Services Engine accepteert de verificatieverzoeken van ESA/SMA en past ze aan met een gebruikersidentiteit en -groep.

Stap 1. Maak een identiteitsgroep voor verificatie.

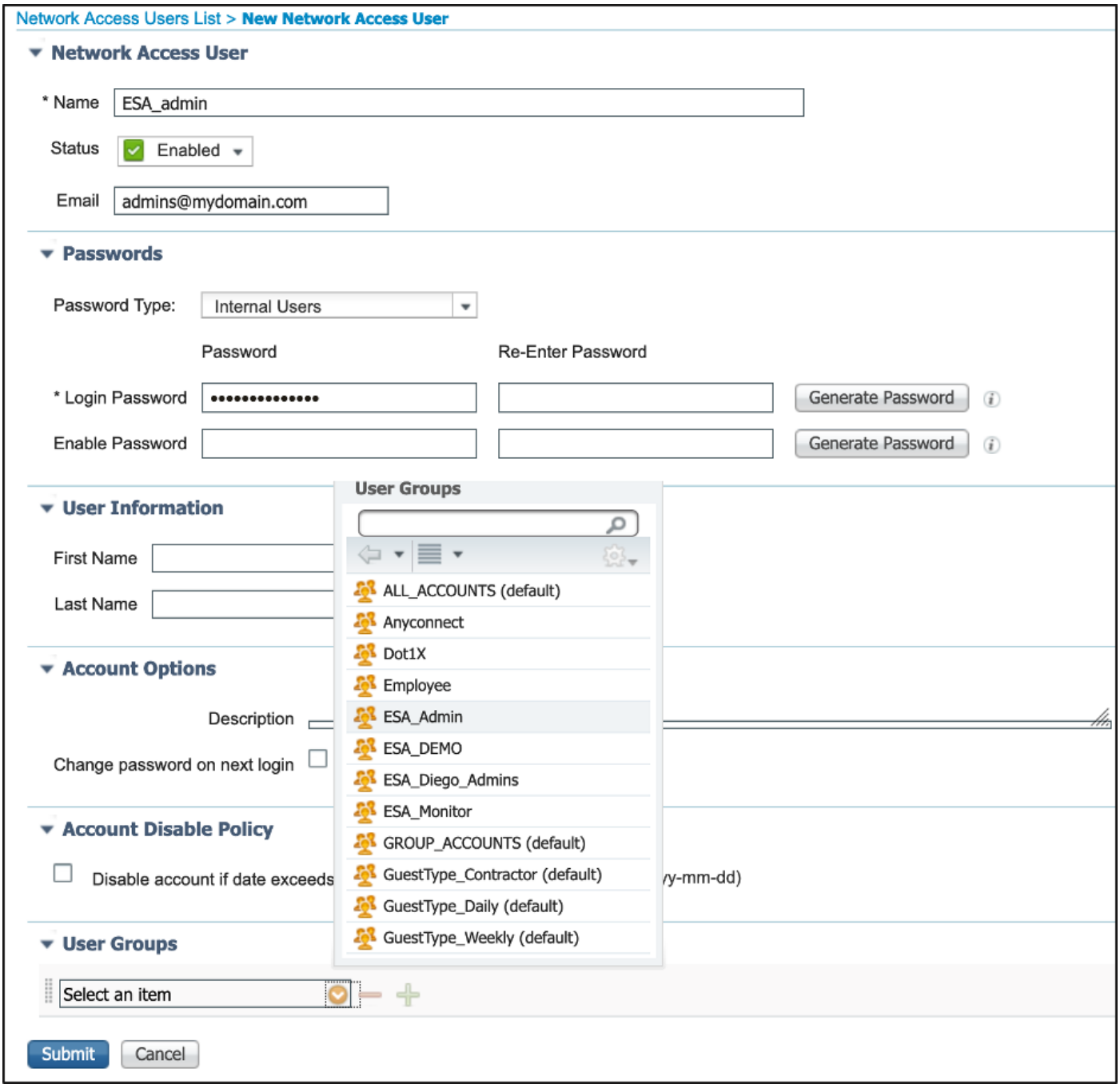
Inloggen op de ISE-server en een identiteitsgroep maken:

Navigeren in naar Administratie->identiteitsbeheer->Groepen->Gebruikersgroep. Zoals in de afbeelding wordt weergegeven.

Opmerking: Cisco raadt een identiteitsgroep in ISE aan voor elke ESA/SMA toegewezen rol.

Stap 2. Maak lokale gebruikers voor verificatie.

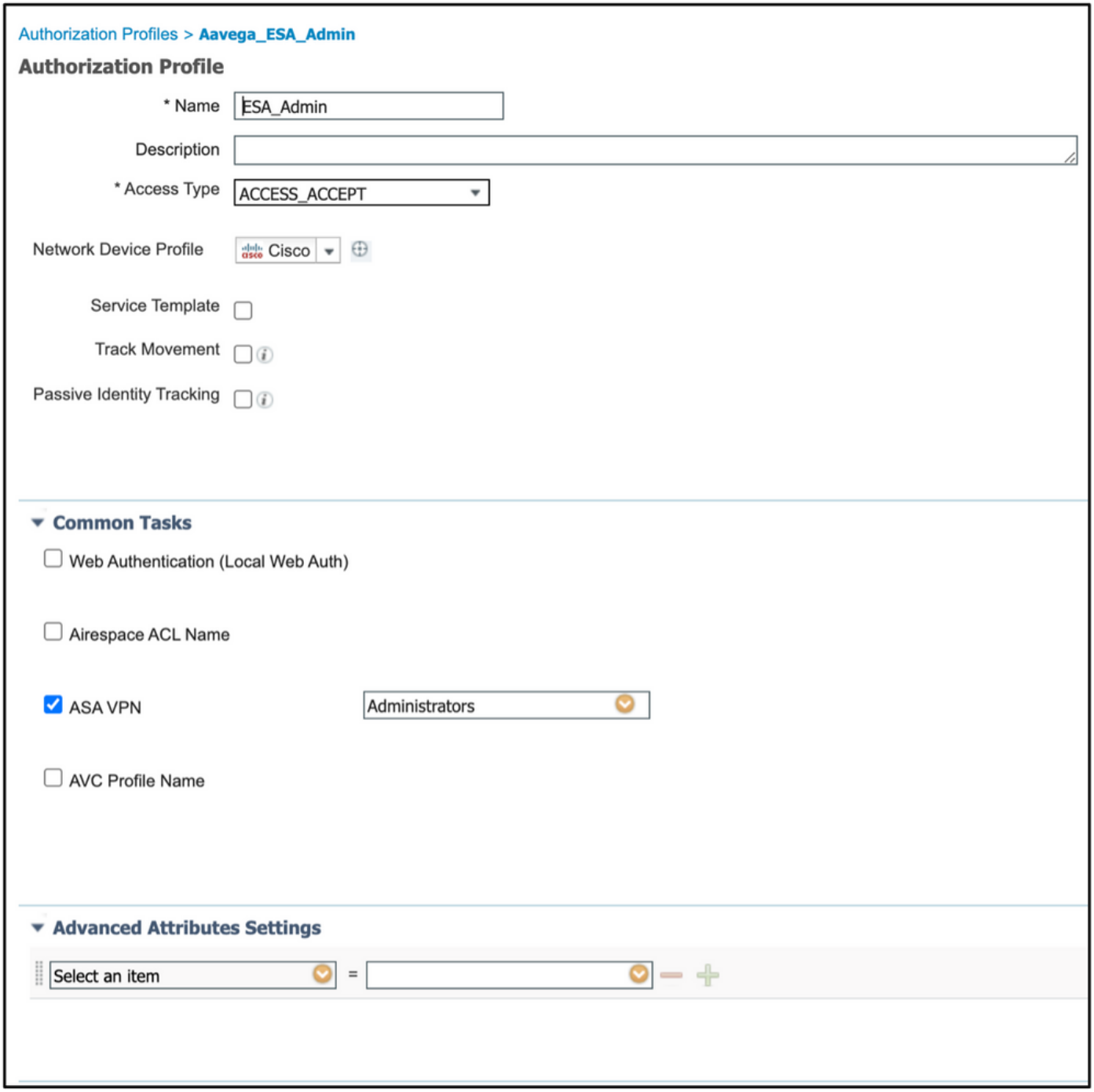
In deze stap kunt u nieuwe gebruikers maken of gebruikers toewijzen die al bestaan aan de Identity Group die we in Stap 1 hebben gemaakt. Meld u aan bij ISE en **navigeer naar Administration->Identity Management->**Identificaties en maakt u nieuwe gebruikers of toewijzen aan gebruikers in de groep(en) die u hebt gemaakt. Zoals in de afbeelding wordt weergegeven.



Stap 3. Maak vergunningsprofielen.

RADIUS-verificatie kan met succes worden voltooid zonder autorisatie profielen, maar er worden geen rollen toegewezen. Voor een volledige installatie **kunt u** navigeren **naar Policy->Policy-Elementen->Resultaten->autorisatie-profiel.**

Opmerking: Eén autorisatieprofiel per te toewijzen rol maken.



Opmerking: Zorg ervoor dat u de eigenschap Straalklasse 25 gebruikt en geef een naam. Deze naam moet overeenkomen met de configuratie op AsyncOS (ESA/SMA). Afbeelding 3 Administrateurs is de CLASS-attributennaam.

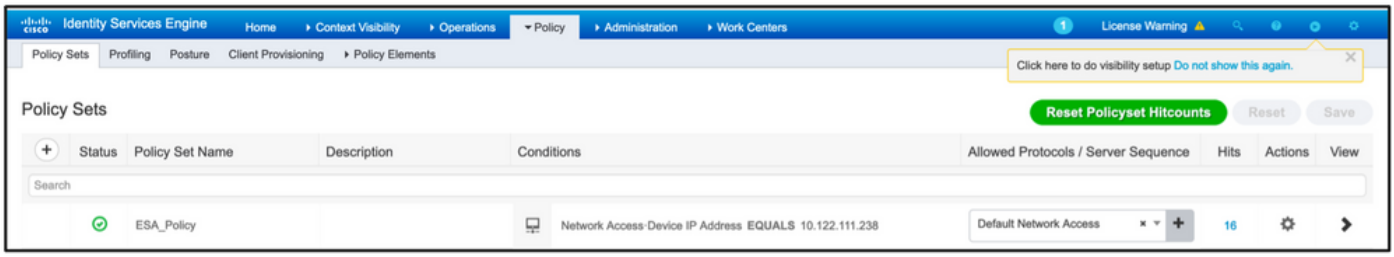
Stap 4. Maak een vergunningenbeleid.

In deze laatste stap kan ISE-server het gebruikerslogbestand in pogingen identificeren en in kaart brengen naar het juiste machtigingsprofiel.

In het geval van een geslaagde vergunning, geeft ISE een toegangsaanvaarding terug volgens de CLASS-waarde die in het machtigingsprofiel is gedefinieerd.

Navigeren in naar beleid > Beleidssets > Toevoegen (+ symbool)

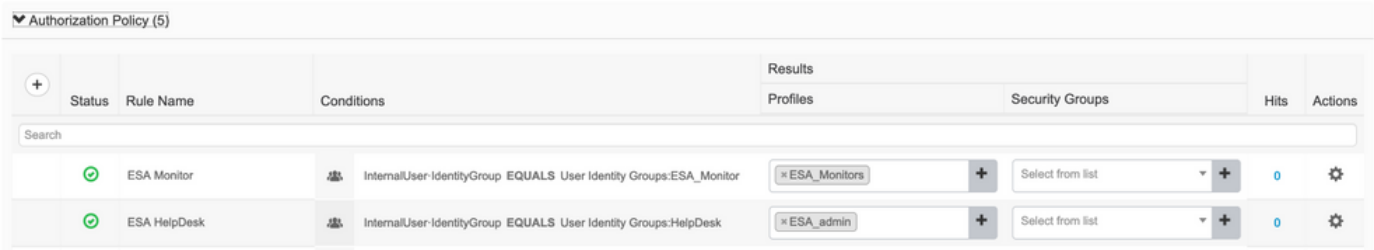
Pas een naam aan en selecteer het plus-symbool om de gewenste voorwaarden toe te voegen. Deze labomgeving gebruikt een Straal. NAS-IP-Address. Bewaar het nieuwe beleid.



Om aan de vergunningsaanvragen te voldoen, moeten de voorwaarden worden toegevoegd.

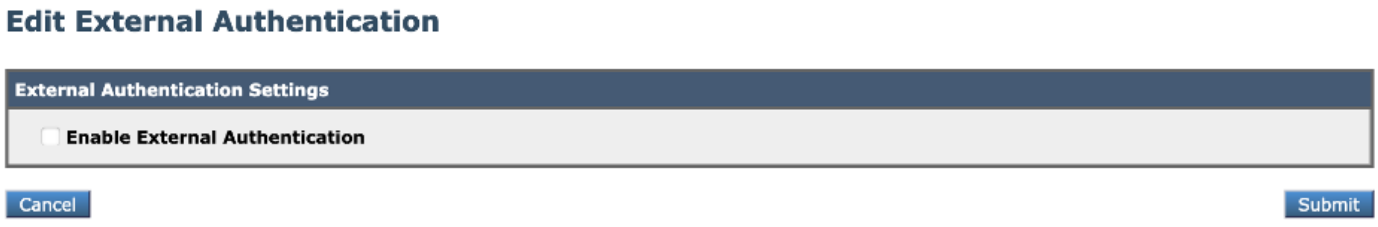
Selecteren pictogram en voeg voorwaarden toe.

Lab-omgeving gebruikt interne gebruiker-IdentityGroup en overeenkomsten voor elk autorisatieprofiel.



Stap 5. Schakel externe verificatie in AsyncOS ESA/SMA.

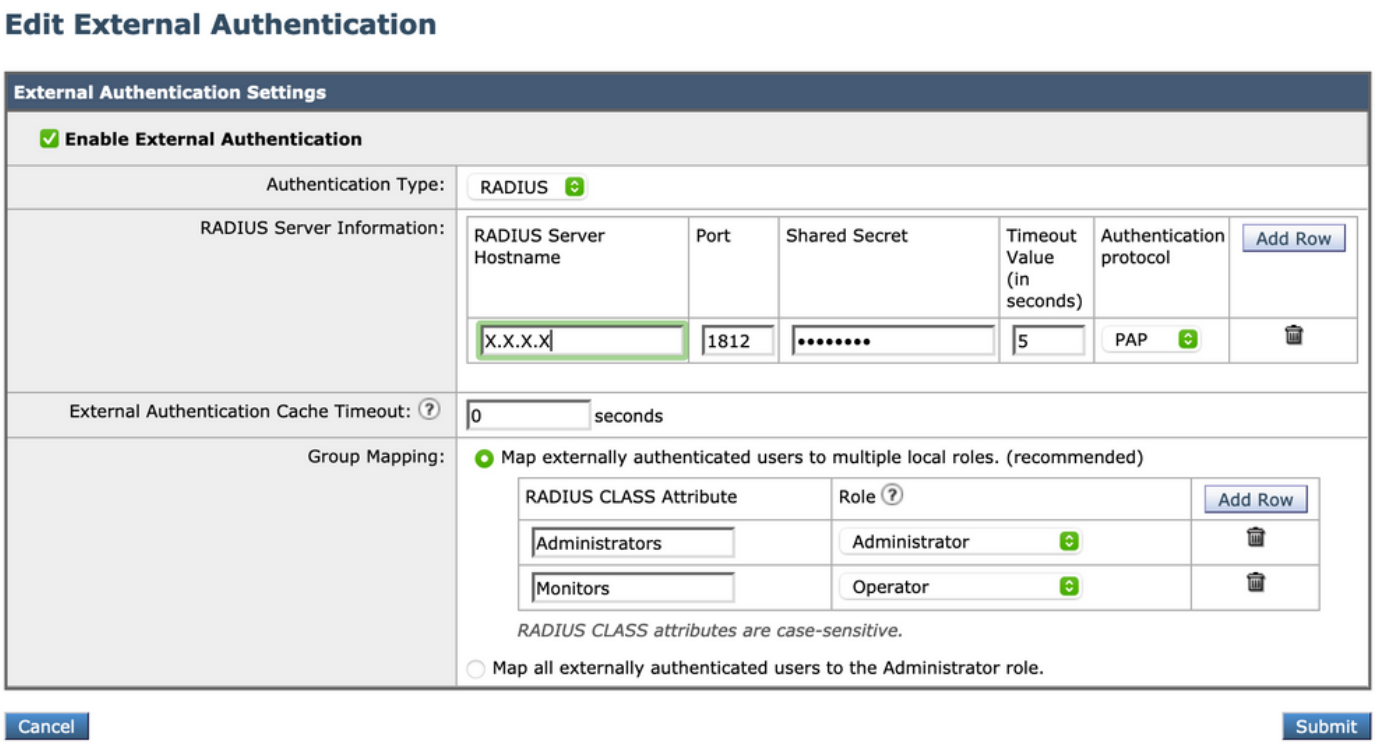
Log in op AsyncOS-apparaat (ESA/SMA/WSA). En **navigeer naar Systeembeheer > Gebruikers > Externe verificatie > Externe verificatie inschakelen** voor **verificatie** op ESA.



Geef deze waarden op:

- Hostnaam voor RADIUS-servers
- Port
- Gedeeld geheim
- Time-outwaarde (in seconden)
- Verificatieprotocol

Selecteer **Map extern geauthentiseerde gebruikers op meerdere lokale rollen (aanbevolen)**. Zoals in de afbeelding wordt weergegeven.

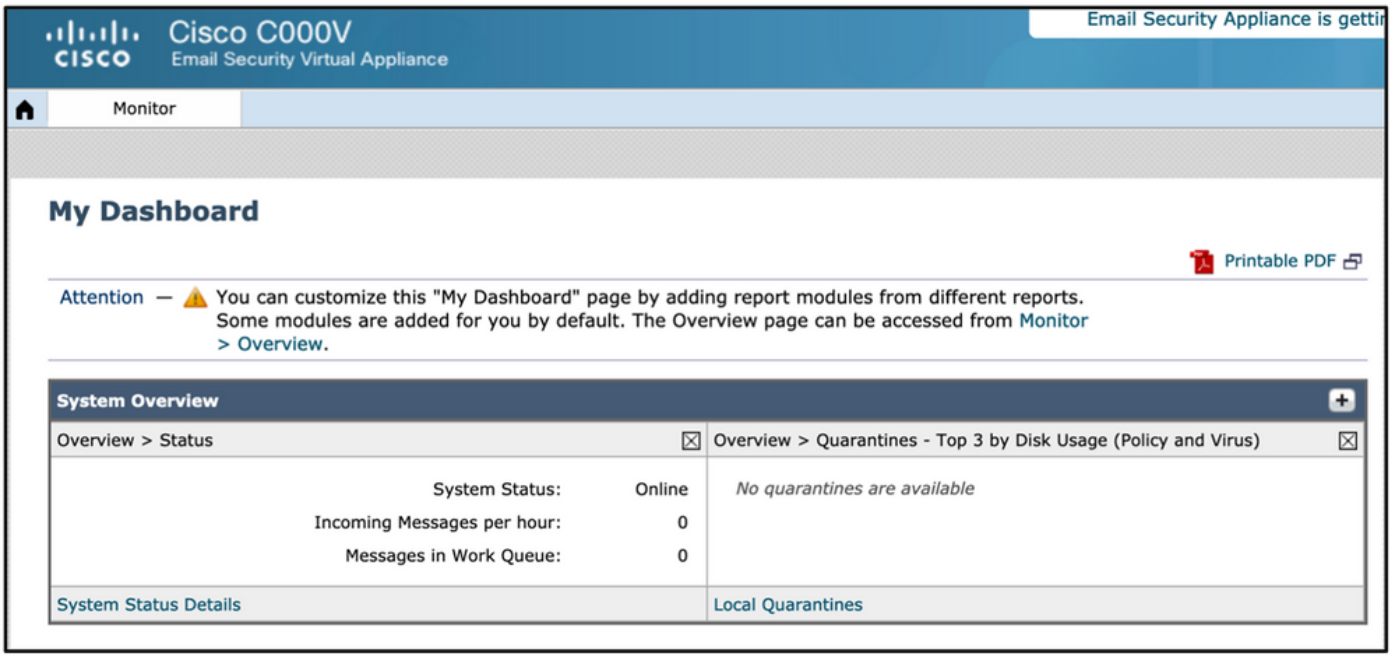


Opmerking: RADIUS-CLASS kenmerk MOET overeenkomen met de eigenschap naam die in stap 3 is gedefinieerd (onder gemeenschappelijke taken die als ASA VPN zijn ingedeeld).

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Log in op uw AsyncOS-apparaat en controleer of er toegang is verleend en de toegewezen rol is correct toegewezen. Zoals in de afbeelding wordt weergegeven met de rol van de gastgebruiker.

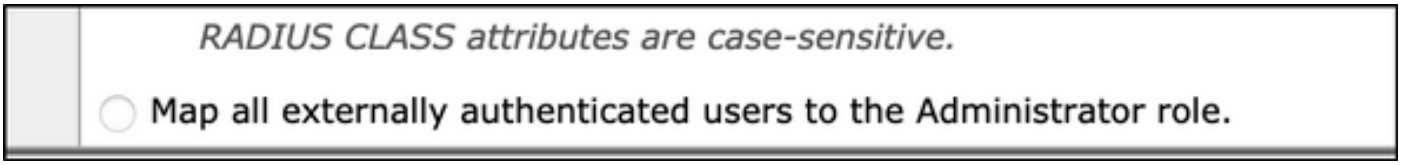


Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Indien loggen in poging niet werkt aan ESA met het bericht "Ongeldige gebruikersnaam of wachtwoord". De kwestie zou op het vergunningenbeleid kunnen liggen.

Meld u aan bij ESA en selecteer vanuit Externe Verificatie Alle extern geauthentiseerde gebruikers naar de Administrator-rol in kaart.



Breng de wijzigingen aan en begaan ze. Doe een nieuwe inlogpoging. In het geval van een succesvol inlogbestand, dubbelcontrole ISE Radius Authorization Profile (CLASS attribuut 25) en Authorization Policy Setup.

Gerelateerde informatie

- **ISE 2.4 gebruikershandleiding**
- **AsyncOS-gebruikershandleiding**