Authentification externe AsyncOS avec Cisco Identity Service Engine (Radius)

Contenu

Introduction

Ce document décrit la configuration requise entre le dispositif de sécurité de la messagerie électronique (ESA)/dispositif de gestion de la sécurité (SMA) et Cisco Identity Services Engine (ISE) pour une implémentation réussie de l'authentification externe avec RADIUS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification, autorisation et comptabilité (AAA)
- Attribut RADIUS CLASS.
- Stratégies de gestion des identités et d'autorisation Cisco ISE.
- Rôles utilisateur Cisco ESA/SMA.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE 2.4
- Cisco ESA 13.5.1, 13.7.0

- Cisco SMA 13.6.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

La version en dehors de celles répertoriées dans la section des composants utilisés n'a pas été testée.

Informations générales

Attribut Radius CLASS

Utilisé pour Accounting, il s'agit d'une valeur arbitraire que le serveur RADIUS inclut dans tous les paquets de comptabilité.

L'attribut class est configuré dans ISE (RADIUS) par groupe.

Lorsqu'un utilisateur est considéré comme faisant partie du groupe ISE/VPN dont l'attribut 25 lui est lié, le NAC applique la stratégie en fonction des règles de mappage configurées dans le serveur ISE (Identity Services Engine).

Configuration

Diagramme du réseau

Identity Service Engine accepte les demandes d'authentification de ESA/SMA et les compare à une identité d'utilisateur et à un groupe.

Étape 1. Créez un groupe d'identités pour l'authentification.

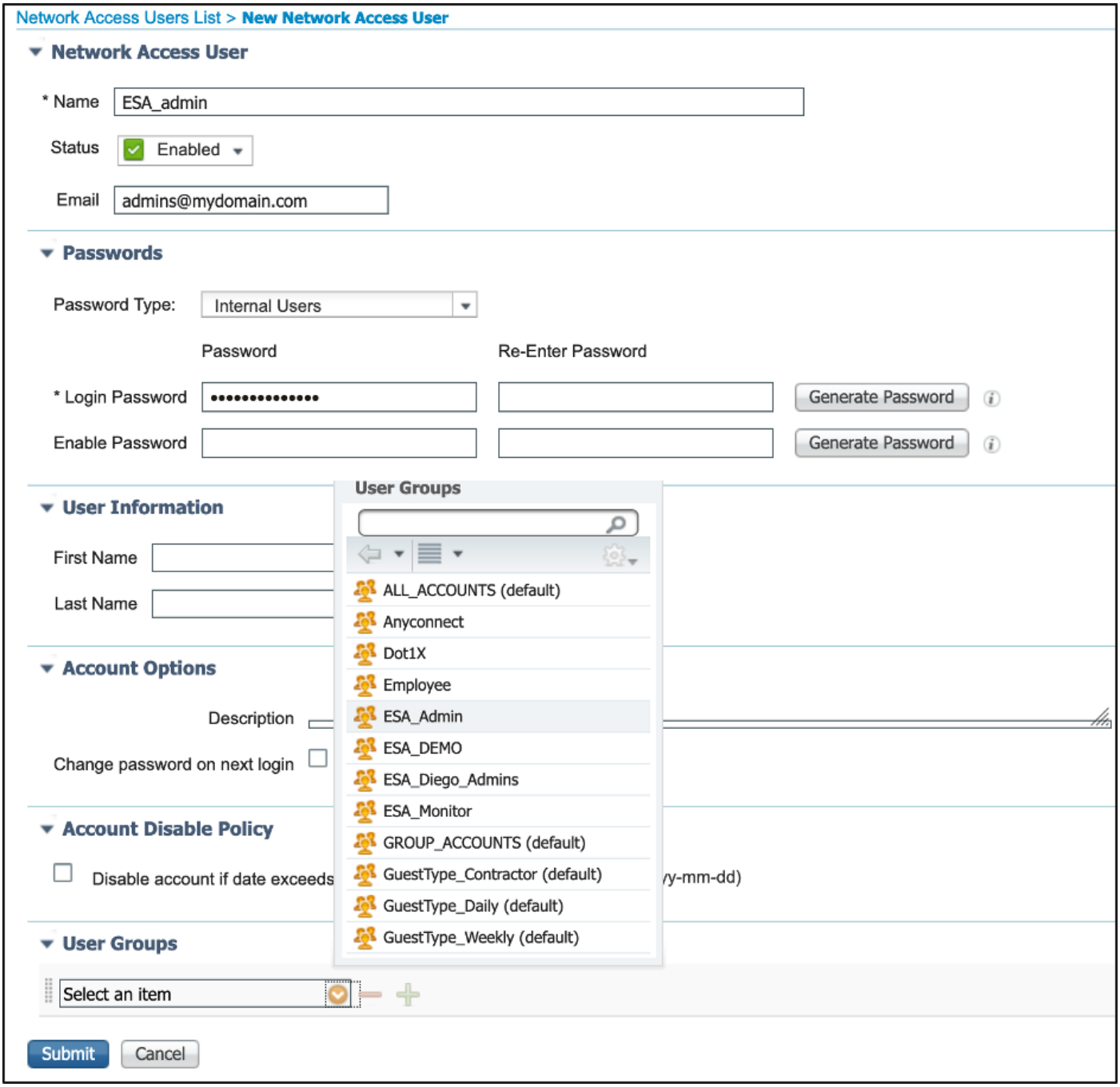
Connectez-vous au serveur ISE et créez un groupe d'identités :

Accédez à Administration->Identity Management->Groups->User Identity Group. Comme le montre l'image.

Note: Cisco recommande un groupe d'identités dans ISE pour chaque rôle ESA/SMA attribué.

Étape 2. Créer des utilisateurs locaux pour l'authentification.

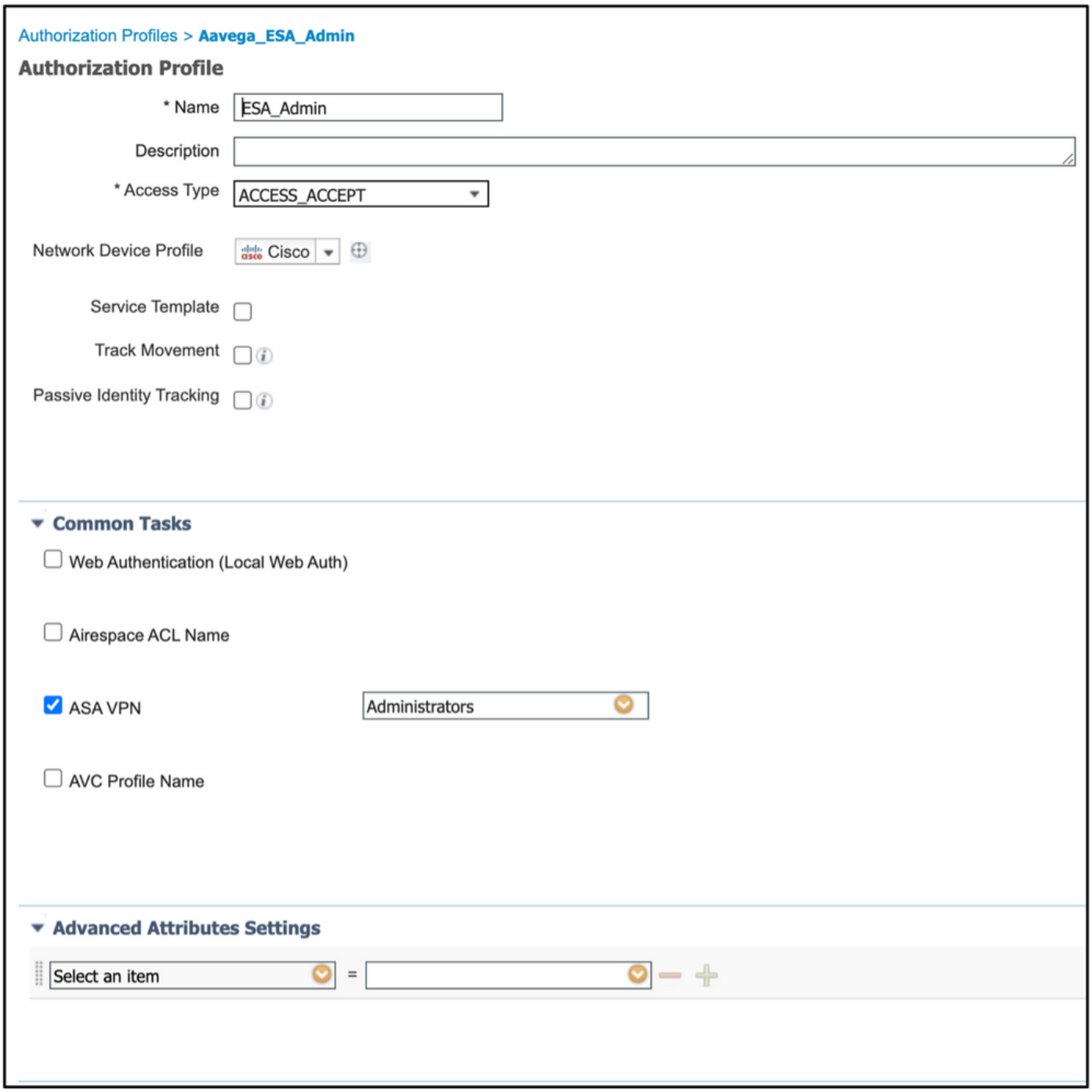
Au cours de cette étape, créez de nouveaux utilisateurs ou affectez des utilisateurs qui existent déjà au groupe d'identités que nous avons créé à l'étape 1. Connectez-vous à ISE et **accédez à Administration->Gestion des identités->Identités** et créez de nouveaux utilisateurs ou affectez-les aux utilisateurs du ou des groupes que vous avez créés. Comme le montre l'image.



Étape 3. Créer des profils d'autorisation.

L'authentification RADIUS peut être effectuée sans profil d'autorisation, mais aucun rôle ne peut être attribué. Pour une configuration complète, accédez **à Policy->Policy Elements->Results->Authorization->Authorization profile.**

Note: Créez un profil d'autorisation par rôle à attribuer.



Note: Assurez-vous d'utiliser l'attribut de classe radius 25 et de donner un nom. Ce nom doit correspondre à la configuration sur AsyncOS (ESA/SMA). À la Figure 3, Administrateurs indique le nom de l'attribut CLASS.

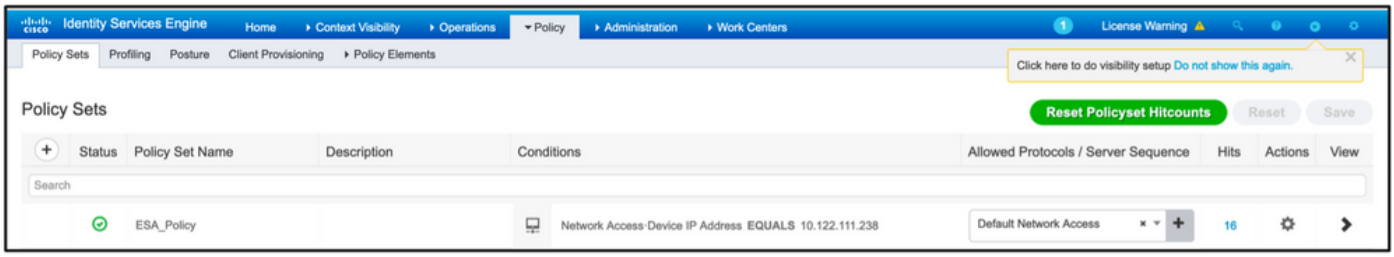
Étape 4. Créez une stratégie d'autorisation.

Cette dernière étape permet au serveur ISE d'identifier les tentatives de connexion de l'utilisateur et de les mapper au profil d'autorisation approprié.

En cas d'autorisation réussie, ISE renvoie un access-accept le long de la valeur CLASS définie dans le profil d'autorisation.

Naviguez jusqu'à Stratégie > Jeux de stratégies > Ajouter (+ symbole)

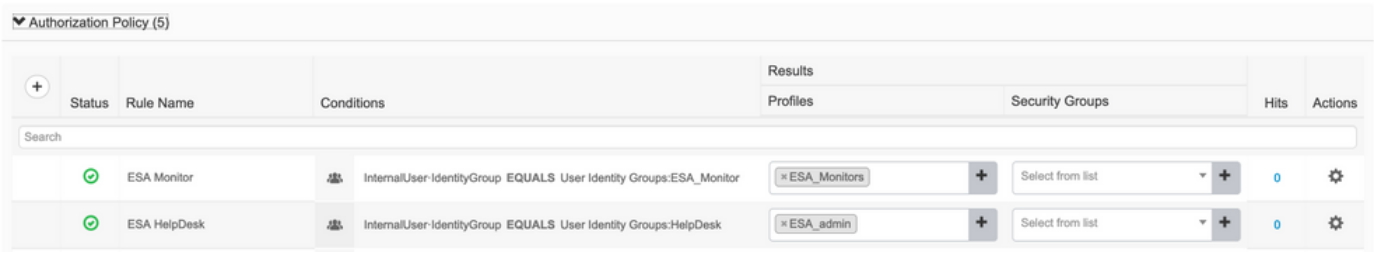
Attribuez un nom et sélectionnez le symbole plus pour ajouter les conditions requises. Cet environnement de travaux pratiques utilise un rayon. Adresse IP NAS. Enregistrez la nouvelle stratégie.



Afin de répondre correctement aux demandes d'autorisation, les conditions doivent être ajoutées.

Sélectionner > et ajouter des conditions.

L'environnement de travaux pratiques utilise InternalUser-IdentityGroup et correspond à chaque profil d'autorisation.



Étape 5. Activez l'authentification externe dans AsyncOS ESA/ SMA.

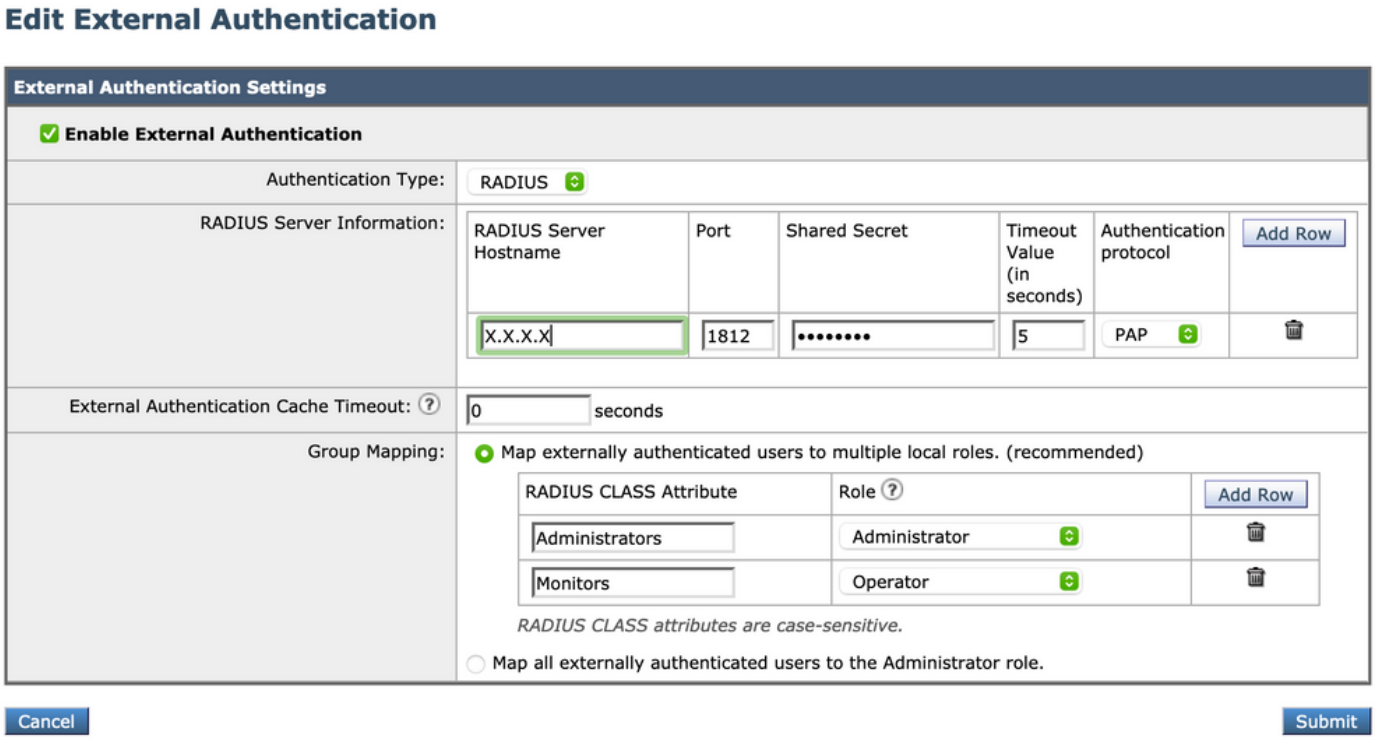
Connectez-vous à l'appliance AsyncOS (ESA/SMA/WSA). Et **accédez à Administration système > Utilisateurs > Authentification externe > Activer l'authentification externe** sur ESA.

Indiquez ces valeurs :

- Nom d'hôte du serveur RADIUS

- Port
- Secret partagé
- Délai d'attente (en secondes)
- Protocole d'authentification

Sélectionnez **Mapper les utilisateurs authentifiés en externe à plusieurs rôles locaux (recommandé)**. Comme le montre l'image.

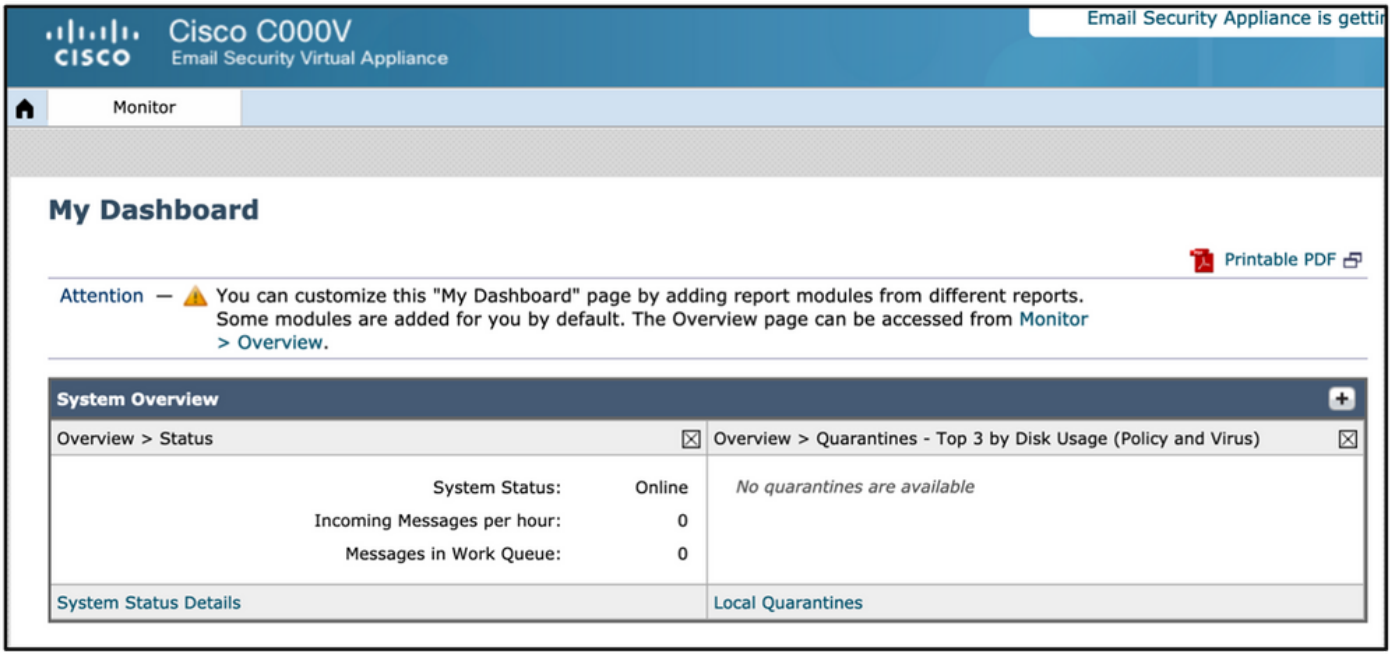


Note: L'attribut Radius CLASS DOIT correspondre au nom de l'attribut défini à l'étape 3 (sous les tâches courantes mappées en tant que VPN ASA).

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Connectez-vous à votre appareil AsyncOS et confirmez que l'accès a été accordé et que le rôle assigné a été correctement attribué. Comme l'illustre l'image avec le rôle d'utilisateur invité.

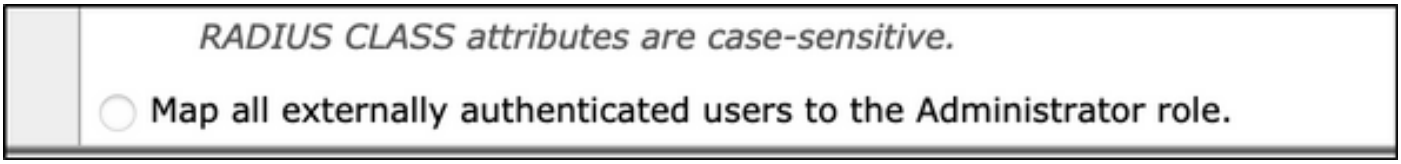


Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si la tentative de connexion échoue sur ESA avec le message “ Nom d'utilisateur ou ” mot de passe non valide. Le problème peut être lié à la stratégie d'autorisation.

Connectez-vous à ESA et depuis Authentification externe sélectionnez Mapper tous les utilisateurs authentifiés en externe au rôle Administrateur.



Envoyez et validez les modifications. Effectuez une nouvelle tentative de connexion. En cas de connexion réussie, double-vérifiez le profil d'autorisation de radius ISE (attribut CLASS 25) et la configuration de la stratégie d'autorisation.

Informations connexes

- **Guide d'utilisation ISE 2.4**
- **Guide d'utilisation AsyncOS**