Configuration de l'authentification externe AsyncOS avec ISE (RADIUS)

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Produits associés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Étape 1 : création d'un groupe d'identités pour l'authentification
  - Étape 2. Créer des utilisateurs locaux pour l'authentification
  - Étape 3. Créer des profils d'autorisation
  - Étape 4. Création d'une stratégie d'autorisation
  - Étape 5 : activation de l'authentification externe sur l'appliance
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit la configuration de l'authentification externe RADIUS entre Cisco Secure Email Gateway et Cisco Identity Services Engine.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification, autorisation et comptabilité (AAA)
- Attribut RADIUS CLASS.
- Gestion des identités et politiques d'autorisation Cisco ISE.

- Rôles utilisateur Cisco Secure Email Gateway (ESA) et Secure Email and Web Manager (SMA)

Composants utilisés

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

- Cisco ISE 2.4
- Passerelle de messagerie sécurisée Cisco (ESA) 13.5.1, 13.7.0
- Cisco Secure Email and Web Manager (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 associés

Les versions autres que celles répertoriées dans la section Composants utilisés n'ont pas été testées.

Informations générales

Attribut de classe RADIUS

L'attribut Class est une valeur arbitraire que le serveur RADIUS renvoie dans la réponse Access-Accept et inclut dans les paquets de comptabilité. Il est configuré dans Cisco ISE par groupe.

Lorsqu'un utilisateur correspond à un groupe ISE auquel est associé l'attribut 25, ISE renvoie la valeur Class sur Access-Accept. La passerelle de messagerie sécurisée lit ensuite cette valeur et applique le rôle local défini dans sa table de mappage.



Remarque : Dans le profil d'autorisation ISE, la tâche commune VPN ASA est utilisée comme conteneur qui remplit l'attribut RADIUS 25 (classe). La valeur entrée ici correspond à ce que l'appliance lit pour le mappage de rôles.

Configurer

Diagramme du réseau



Cisco Identity Services Engine accepte les demandes d'authentification de l'appliance et les compare à une identité d'utilisateur et à un groupe.

Étape 1 : création d’un groupe d’identités pour l’authentification

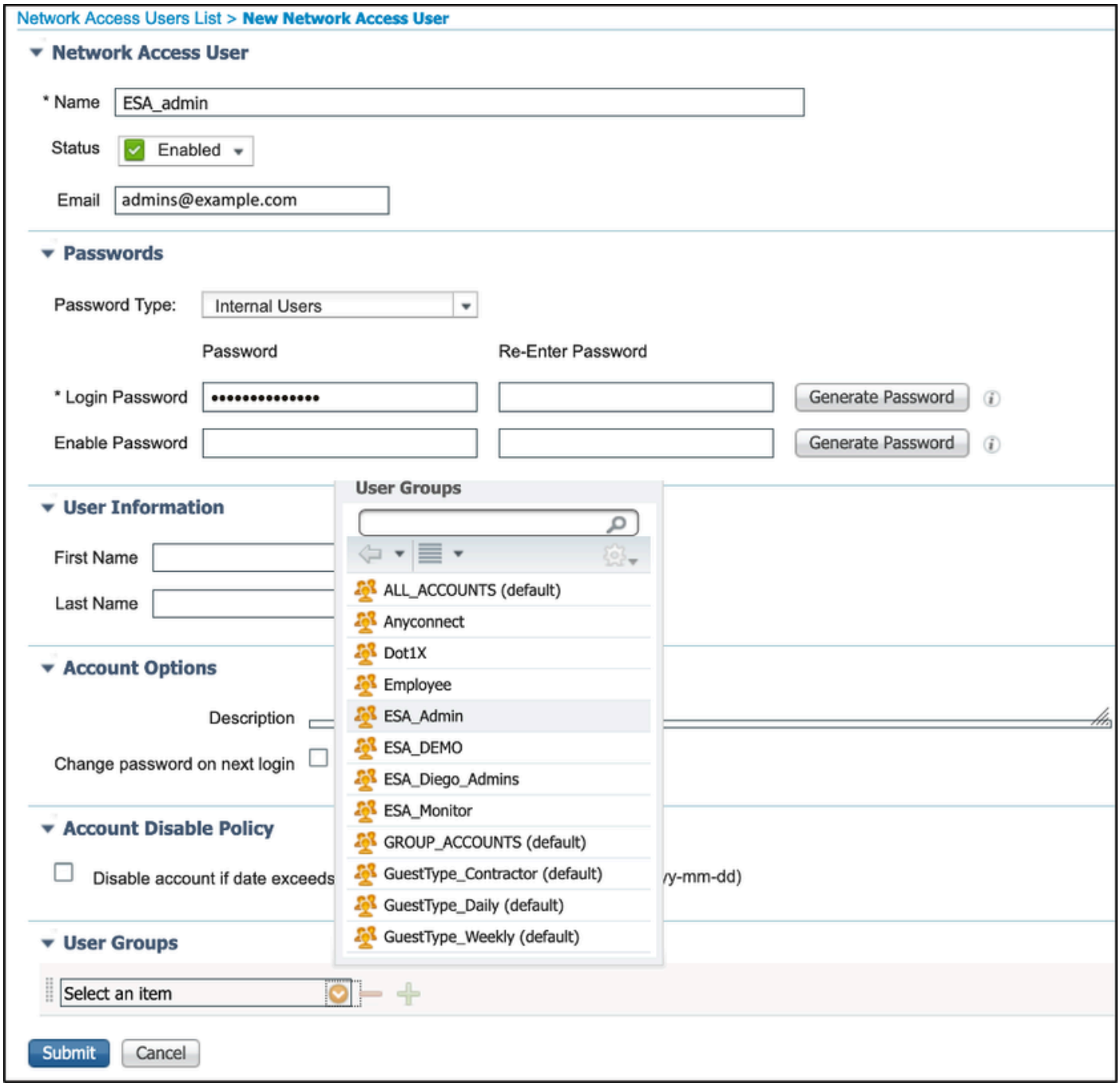
Connectez-vous au serveur ISE. Accédez à Administration > Identity Management > Groups > User Identity Group et créez un groupe d'identité.



Remarque : Cisco recommande un groupe d'identité dans ISE pour chaque rôle d'appliance à attribuer.

Étape 2. Créer des utilisateurs locaux pour l’authentification

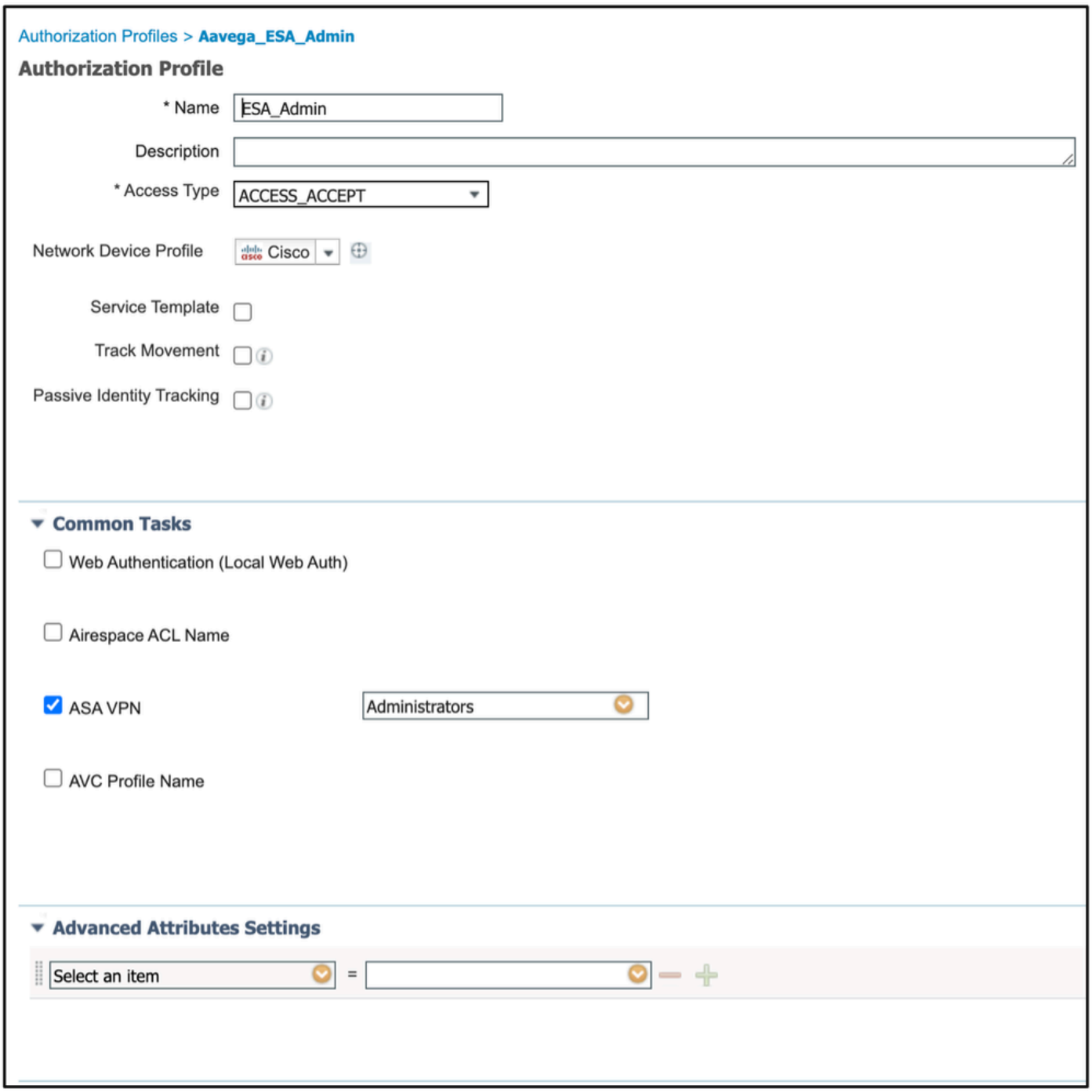
Créez de nouveaux utilisateurs ou affectez des utilisateurs existants au groupe d'identités créé à l'étape 1. Accédez à Administration > Identity Management > Identities et créez ou affectez des utilisateurs au groupe.



Étape 3. Créer des profils d’autorisation

L'authentification RADIUS peut réussir sans profil d'autorisation ; cependant, aucun rôle n'est attribué. Pour attribuer des rôles, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles.

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



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

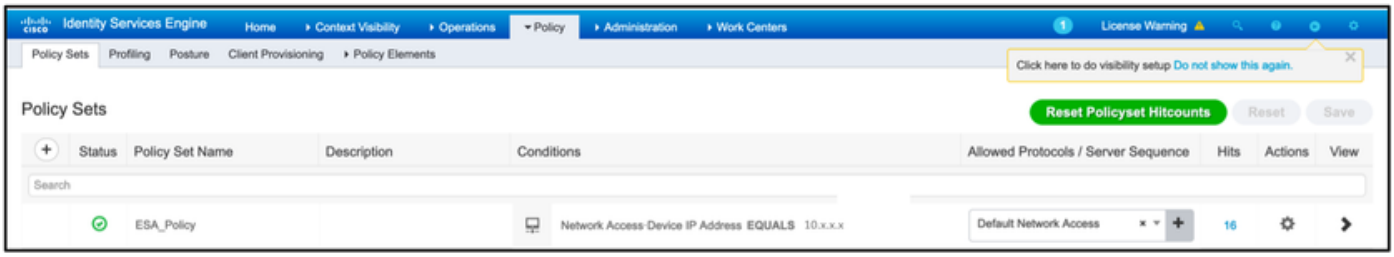
Étape 4. Création d’une stratégie d’autorisation

Cette étape permet à ISE d'identifier les tentatives de connexion et de les mapper au profil d'autorisation approprié. En cas de correspondance réussie, ISE renvoie Access-Accept avec la valeur Class définie dans le profil.

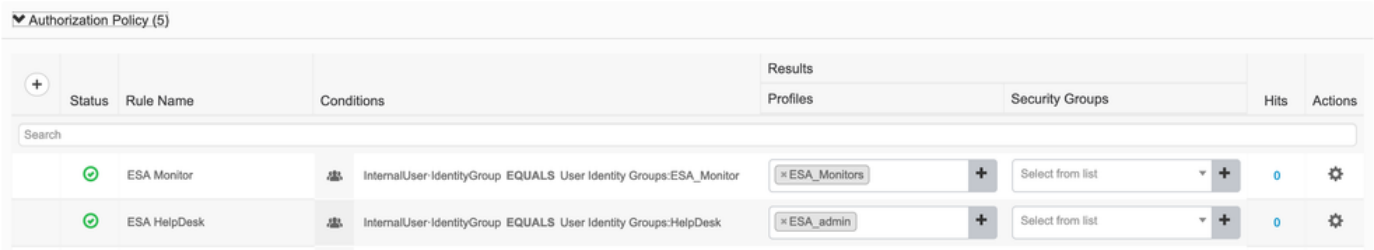
Accédez à Policy > Policy Sets et sélectionnez Add (+ symbol).



Attribuez un nom et sélectionnez le symbole plus pour ajouter les conditions requises. Cet environnement de travaux pratiques utilise une condition d'adresse IP NAS Radius. Enregistrez la nouvelle stratégie.



Pour faire correspondre correctement les demandes d'autorisation, ajoutez les conditions. Sélectionnez le symbole > et ajoutez des conditions. Cet environnement de travaux pratiques utilise InternalUser-IdentityGroup et correspond à chaque profil d'autorisation.



Étape 5 : activation de l'authentification externe sur l'appliance

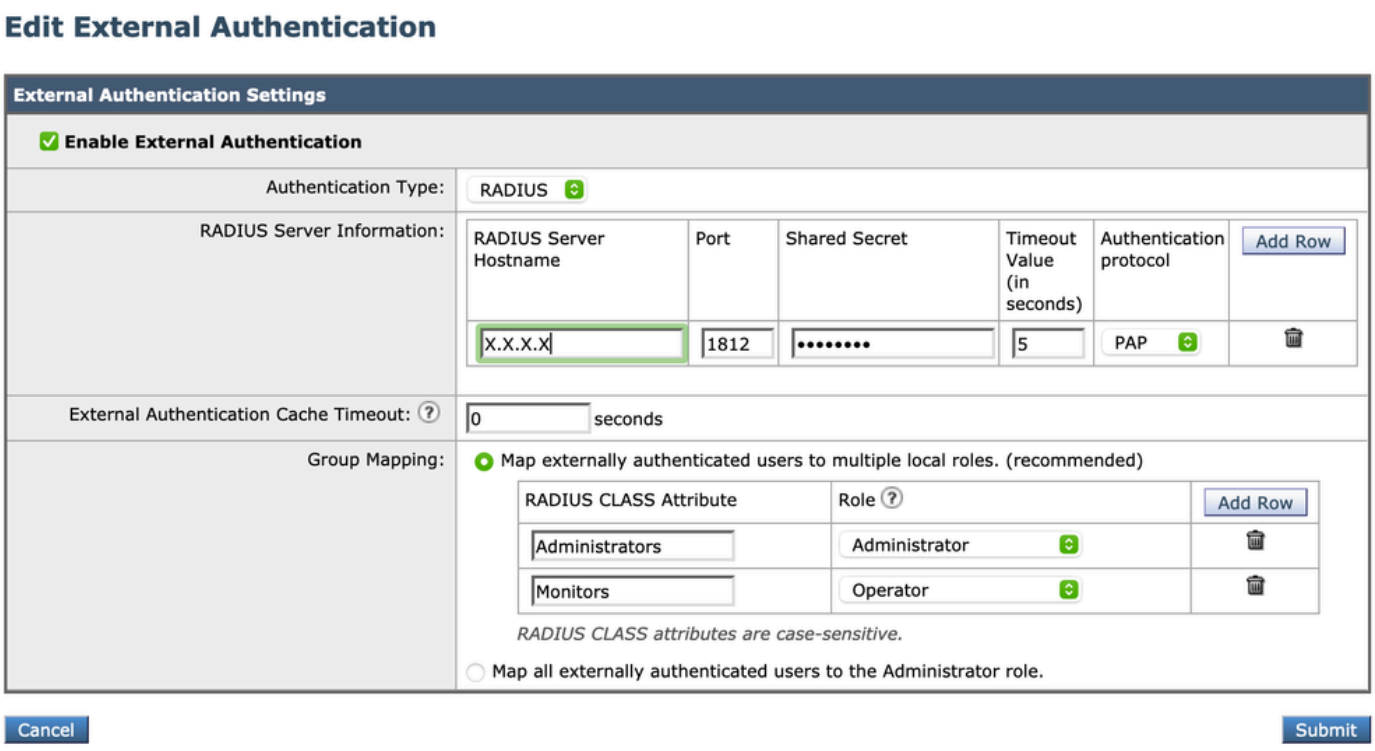
Connectez-vous à l'appliance. Accédez à Administration système > Utilisateurs > Authentification externe et sélectionnez Activer l'authentification externe.



Entrez les valeurs suivantes :

- Nom d'hôte du serveur RADIUS
- Port
- Secret partagé
- Valeur du délai d'attente (en secondes)
- Protocole d'authentification

Sélectionnez Mapper les utilisateurs authentifiés en externe à plusieurs rôles locaux (recommandé).



Remarque : la valeur de la classe RADIUS doit correspondre à la valeur définie à l'étape 3 (entrée dans la tâche commune VPN ASA), y compris la casse.

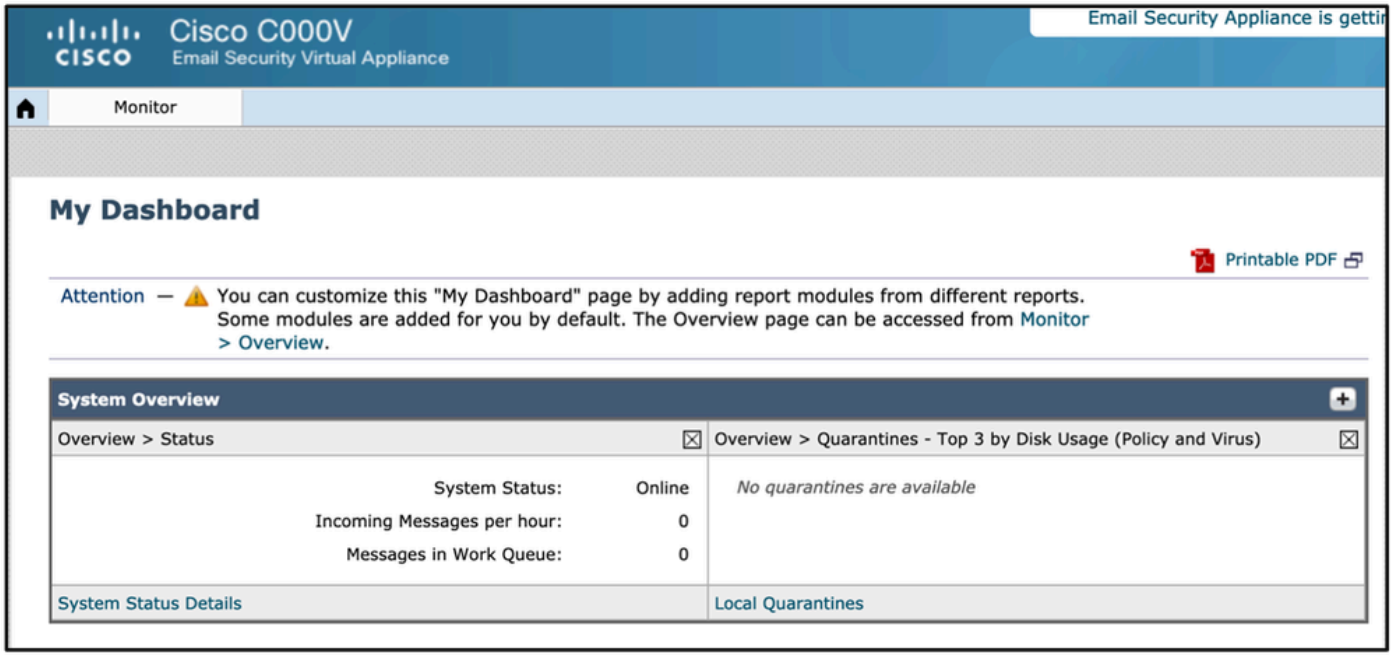
Remarque : Le protocole d'authentification sélectionné ici (par exemple, PAP) doit correspondre aux protocoles autorisés dans l'ensemble de stratégies ISE. Une non-correspondance entraîne l'échec de l'authentification.

Envoyez et validez les modifications.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Connectez-vous à l'appliance avec un utilisateur authentifié en externe.
2. Confirmez que l'accès est accordé.
3. Vérifiez que le rôle attribué correspond au rôle attendu à partir de la valeur Class renvoyée.
4. Dans ISE, vérifiez que la règle d'autorisation attendue a été atteinte et que la valeur Class correcte a été renvoyée (Operations > RADIUS > Live Logs).



Dépannage

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

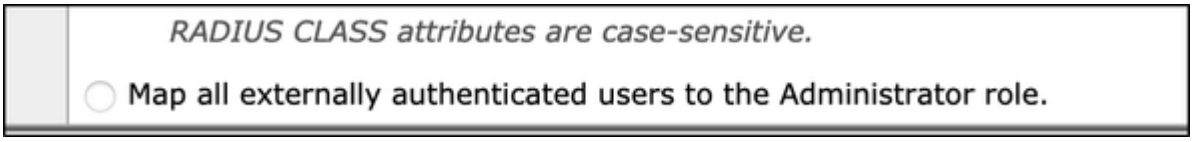
Symptôme : La connexion échoue sur l'appliance avec le message « Nom d'utilisateur ou mot de passe non valide ».

Cause probable : Non-concordance dans la stratégie d'autorisation, la valeur Class renvoyée ou le protocole d'authentification.

Résolution :

1. Dans les paramètres d'authentification externe de l'appliance, sélectionnezMapper

temporairement tous les utilisateurs authentifiés en externe au rôle Administrateur.(Image 11)
2. Envoyez et validez les modifications, puis essayez une nouvelle connexion.
3. Si la connexion réussit maintenant, le problème se situe au niveau du mappage des rôles. Vérifiez à nouveau le profil d'autorisation ISE (Classe / Attribut 25) et la configuration de la stratégie d'autorisation.
4. ReviewOperations > RADIUS > Live Login ISE pour confirmer le profil d'autorisation correspondant et la valeur Class renvoyée.



Informations connexes

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.