Configuration du NAM du client sécurisé pour Dot1x à l'aide de Windows et ISE 3.2

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Network Access Manager
- Configurer
  - Diagramme du réseau
- Configurations
  - Télécharger et installer le NAM (Network Access Manager) du client sécurisé
  - Téléchargez et installez l'éditeur de profil NAM du client sécurisé
  - Configurations générales par défaut
  - Scénario 1 : Configuration du demandeur NAM du client sécurisé pour l'authentification des utilisateurs PEAP (MS-CHAPv2)
  - Scénario 2 : Configurer le demandeur NAM du client sécurisé pour l'authentification simultanée des utilisateurs et des machines EAP-FAST
  - Scénario 3 : Configurer le demandeur NAM du client sécurisé pour l'authentification du certificat utilisateur EAP TLS
  - Configurer ISR 1100 et ISE pour autoriser les authentifications en fonction du scénario 1 PEAP MSCHAPv2
  - Configuration des stratégies d'authentification et d'autorisation
  - Politique d'autorisation
- Vérifier
- Dépannage
  - Problème 1 : Profil NAM non utilisé par le client sécurisé
  - Problème 2 : Les journaux doivent être collectés pour une analyse plus approfondie
  - Reproduisez le problème
  - Collecter l'offre groupée Secure Client DART
- Informations connexes

Introduction

Ce document décrit comment configurer le module NAM (Secure Client Network Analysis Module) sous Windows.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base d'un demandeur RADIUS
- Point1x
- PEAP
- PKI

Composants utilisés

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

- Windows 10 Professionnel Version 22H2 Construit 19045.3930
- ISE 3.2
- Cisco C1117 Logiciel Cisco IOS® XE Version 17.12.02
- Active Directory 2016

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.

Informations générales

Ce document décrit comment configurer le NAM du client sécurisé sous Windows. L'option de pré-déploiement et l'Éditeur de profil pour effectuer l'authentification dot1x sont utilisés. Des exemples de la façon d'y parvenir sont également fournis.

Dans le domaine des réseaux, un demandeur est une entité située à une extrémité d’un segment de réseau local point à point, qui cherche à être authentifiée par un authentificateur relié à l’autre extrémité de cette liaison.

La norme IEEE 802.1X utilise le terme demandeur pour désigner le matériel ou le logiciel. En pratique, un demandeur est une application logicielle installée sur l'ordinateur d'un utilisateur final. L'utilisateur appelle le demandeur et envoie ses informations d'identification pour connecter l'ordinateur à un réseau sécurisé. Si l'authentification réussit, l'authentificateur permet généralement à l'ordinateur de se connecter au réseau.

Network Access Manager

Network Access Manager est un logiciel client qui fournit un réseau de couche 2 sécurisé conformément à ses politiques. Il détecte et sélectionne le réseau d'accès de couche 2 optimal et procède à l'authentification des périphériques pour l'accès aux réseaux filaires et sans fil. Network Access Manager gère l'identité des utilisateurs et des périphériques, ainsi que les protocoles d'accès réseau requis pour un accès sécurisé. Il fonctionne de manière intelligente pour empêcher les utilisateurs finaux d'établir des connexions en violation des stratégies définies par l'administrateur.

Le gestionnaire d'accès réseau est conçu comme un réseau à résidence unique, permettant une seule connexion réseau à la fois. En outre, les connexions filaires ont une priorité plus élevée que les connexions sans fil. Par conséquent, si vous êtes connecté au réseau avec une connexion filaire, la carte sans fil est désactivée sans adresse IP.

Configurer

Diagramme du réseau

Il est essentiel de comprendre que pour les authentifications dot1x, 3 parties sont requises :

1. Le demandeur qui peut utiliser dot1x.
2. L'authentificateur est également appelé NAS/NAD, qui sert de proxy encapsulant le trafic dot1x à l'intérieur du RADIUS.
3. Et le serveur d'authentification.

Dans cet exemple, le demandeur est installé et configuré de différentes manières. Plus tard, un scénario avec la configuration du périphérique réseau et le serveur d'authentification est présenté.

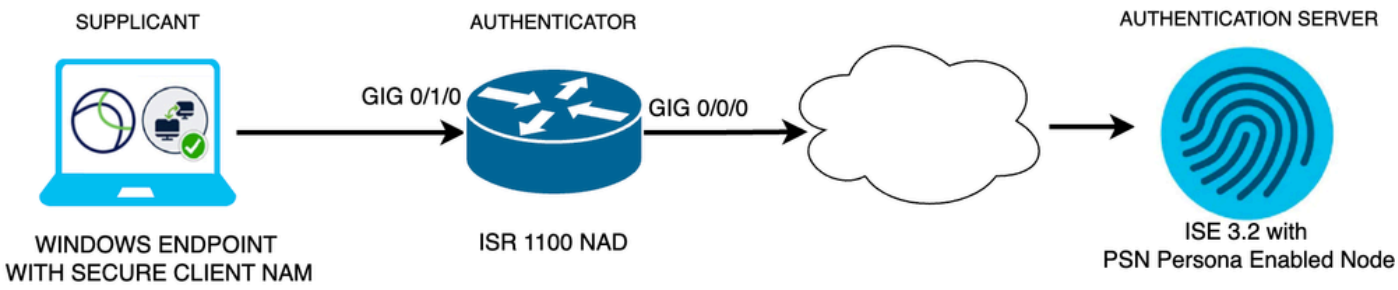


Diagramme du réseau

Configurations

1. Téléchargez et installez Secure Client NAM (Network Access Manager).
2. Téléchargez et installez Secure Client NAM Profile Editor.
3. Configurations générales par défaut.
4. Scénario 1 : Configurez le demandeur NAM du client sécurisé pour l'authentification utilisateur PEAP (MS-CHAPv2).
5. Scénario 2 : Configurez le demandeur NAM du client sécurisé pour EAP-FAST simultanément à la configuration de l'authentification de l'utilisateur et de la machine.
6. Scénario 3 Partie 1 : Configurez le demandeur NAM du client sécurisé pour EAP-TLS.
7. Scénario 3 Partie 2 : Configurez la démonstration NAD et ISE.

Télécharger et installer le NAM (Network Access Manager) du client sécurisé

Téléchargement de logiciels Cisco

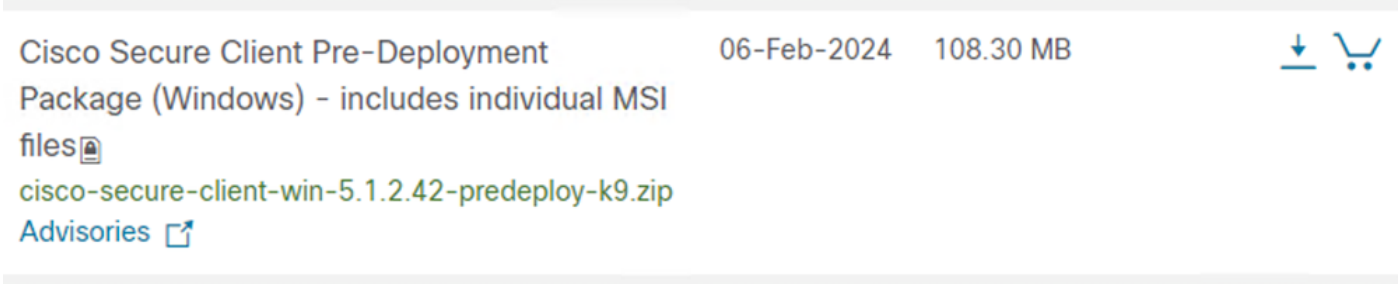
1. Dans la barre de recherche du nom du produit, tapez Secure Client 5.

Téléchargements Accueil > Sécurité > Clients VPN et de sécurité des terminaux > Client sécurisé (y compris AnyConnect) > Client sécurisé 5 > Logiciel client VPN AnyConnect.

2. Dans cet exemple de configuration, la version 5.1.2.42 est utilisée.

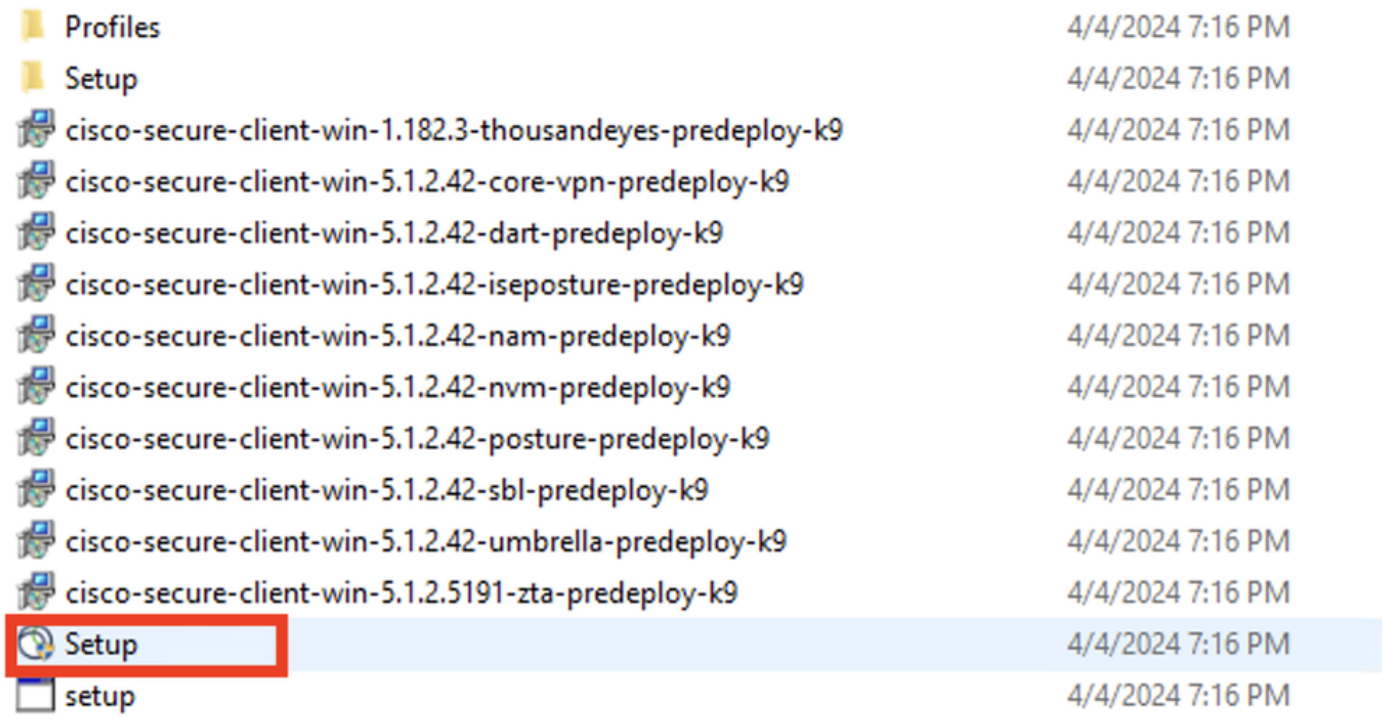
Il existe plusieurs façons de déployer le client sécurisé sur les périphériques Windows ; de SCCM, du moteur de service d'identité et de la tête de réseau VPN. Cependant, dans cet article, la méthode d'installation utilisée est la méthode de pré-déploiement.

3. Sur cette page, recherchez le fichier Cisco Secure Client Headend Deployment Package (Windows).



Fichier zip Msi

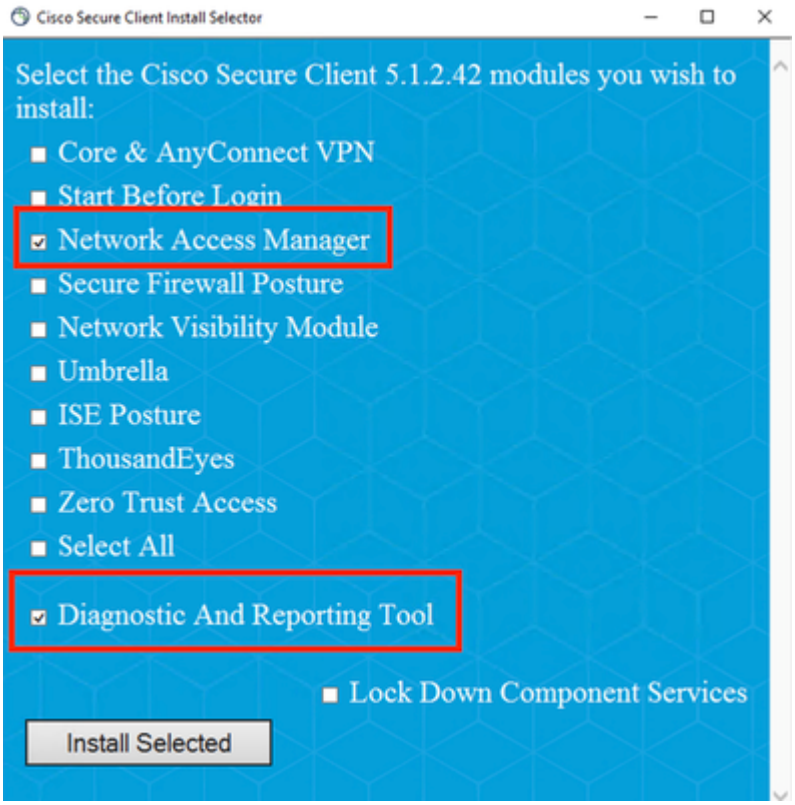
4. Une fois téléchargé et extrait, cliquez sur Setup.



Fichiers client sécurisés

5. Installez les modules Network Access Manager et Outil de diagnostic et de création de rapports.

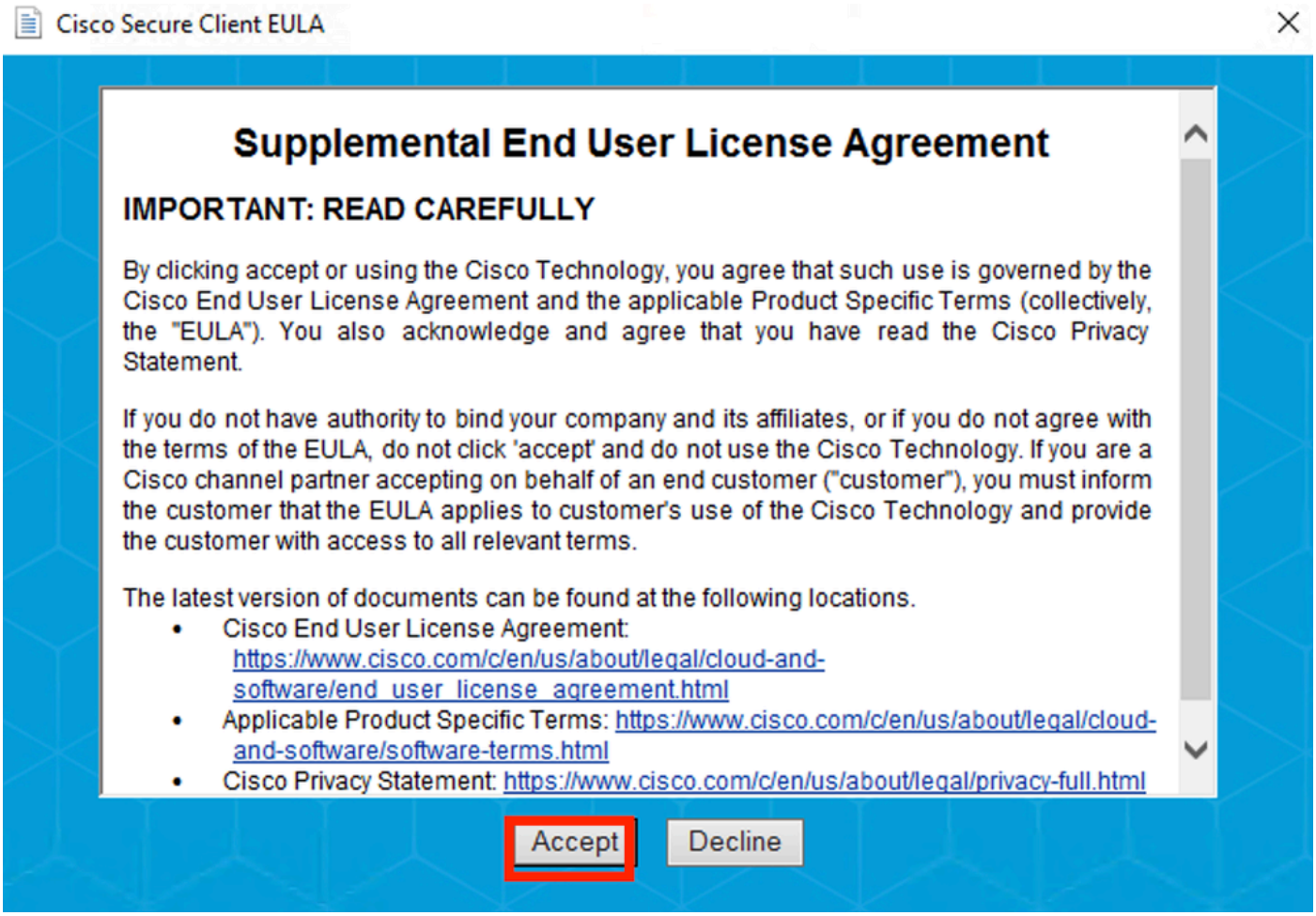
Avertissement : Si vous utilisez l'Assistant Cisco Secure Client, le module VPN est installé automatiquement et masqué dans l'interface utilisateur graphique. NAM ne fonctionne pas si le module VPN n'est pas installé. Si vous utilisez des fichiers MSI individuels ou une autre méthode d'installation, veillez à installer le module VPN.



Sélecteur d'installation

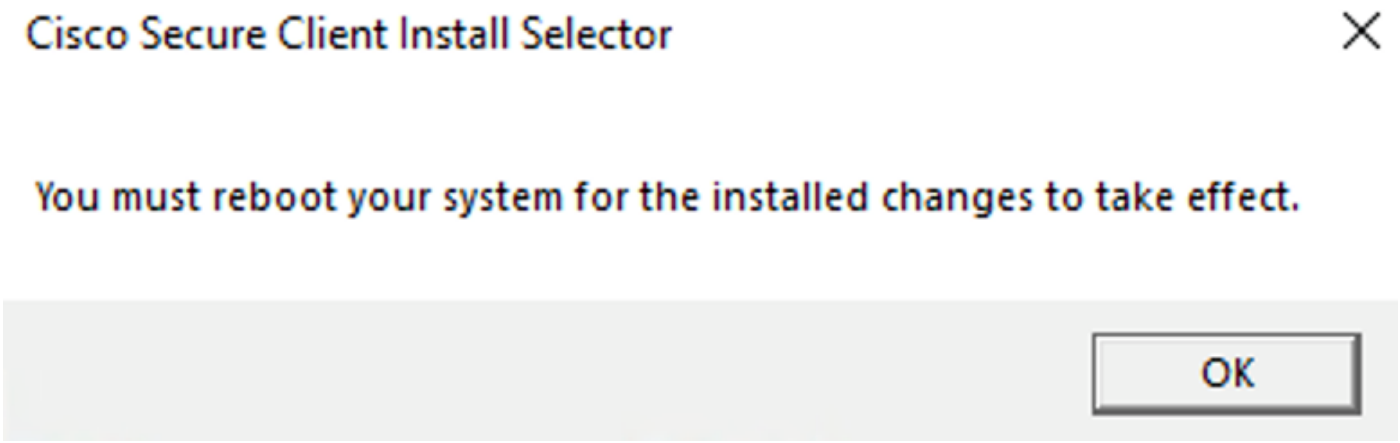
6. Cliquez sur Installer la sélection.

7. Acceptez le CLUF.



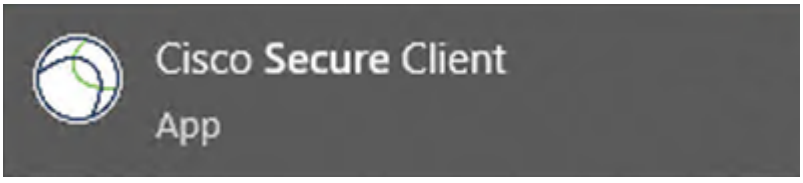
Fenêtre CLUF

8. Un redémarrage est nécessaire après l'installation de NAM.



Fenêtre Conditions de redémarrage

9. Une fois installé, il peut être trouvé et ouvert à partir de la barre de recherche Windows.

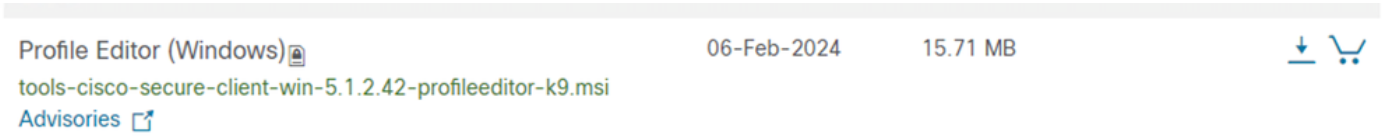


Téléchargez et installez l'éditeur de profil NAM du client sécurisé

1. Cisco Network Access Manager Profile Editor est requis pour configurer les préférences Dot1x.

2. L'option Éditeur de profil est disponible à partir de la même page où le client sécurisé est téléchargé.

3. Cet exemple utilise l'option avec la version 5.1.2.42.



Éditeur de profil

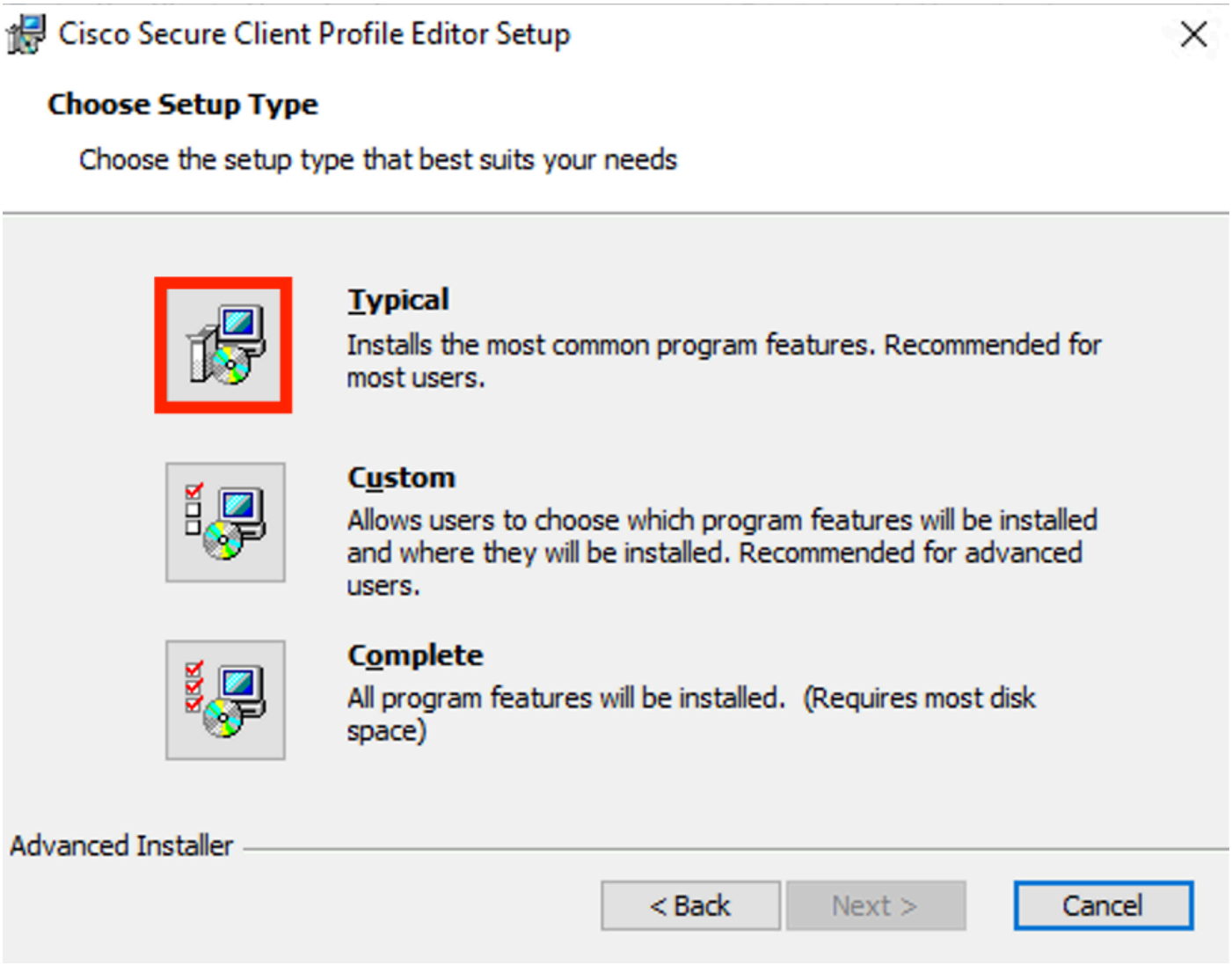
4. Une fois téléchargé, poursuivez l'installation.

5. Exécutez le fichier msi.

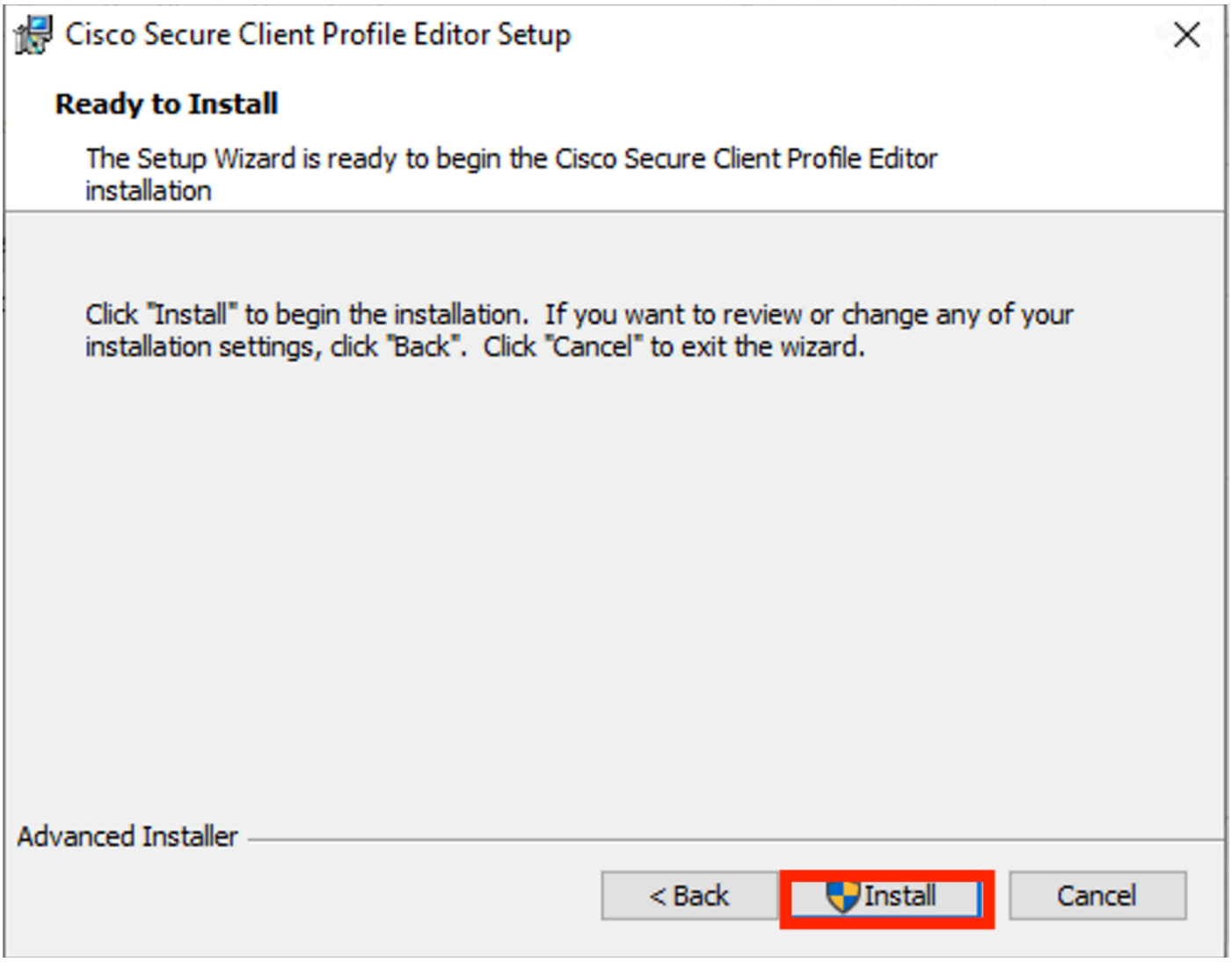


Fenêtre Configuration de Profile Editor

6. Utilisez l'option de configuration Standard.

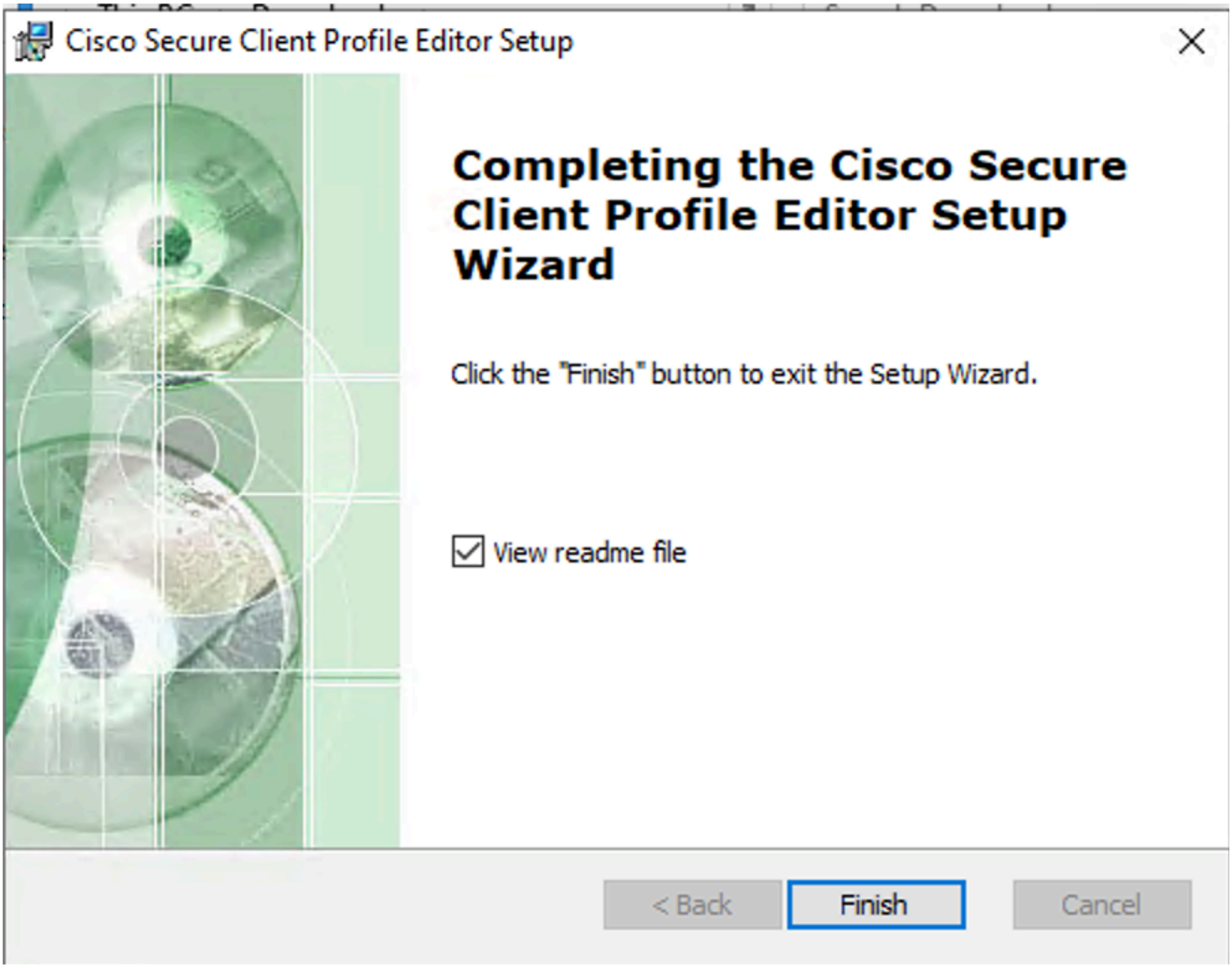


Configuration de Profile Editor



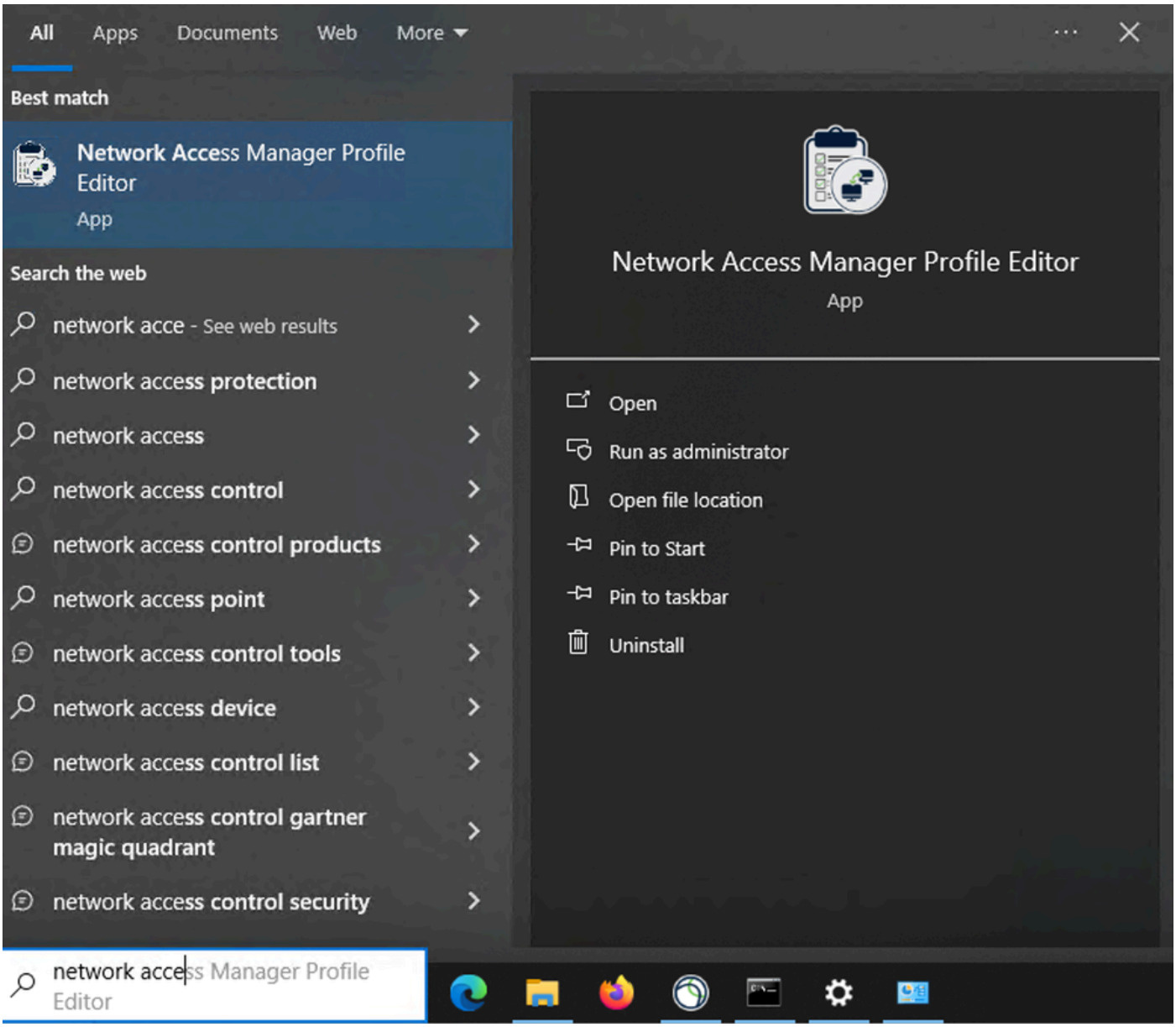
Fenêtre d'installation

7. Cliquez sur Terminer.



Fin de la configuration de Profile Editor

8. Une fois installé, ouvrez l'Éditeur de profil Network Access Manager à partir de la barre de recherche.



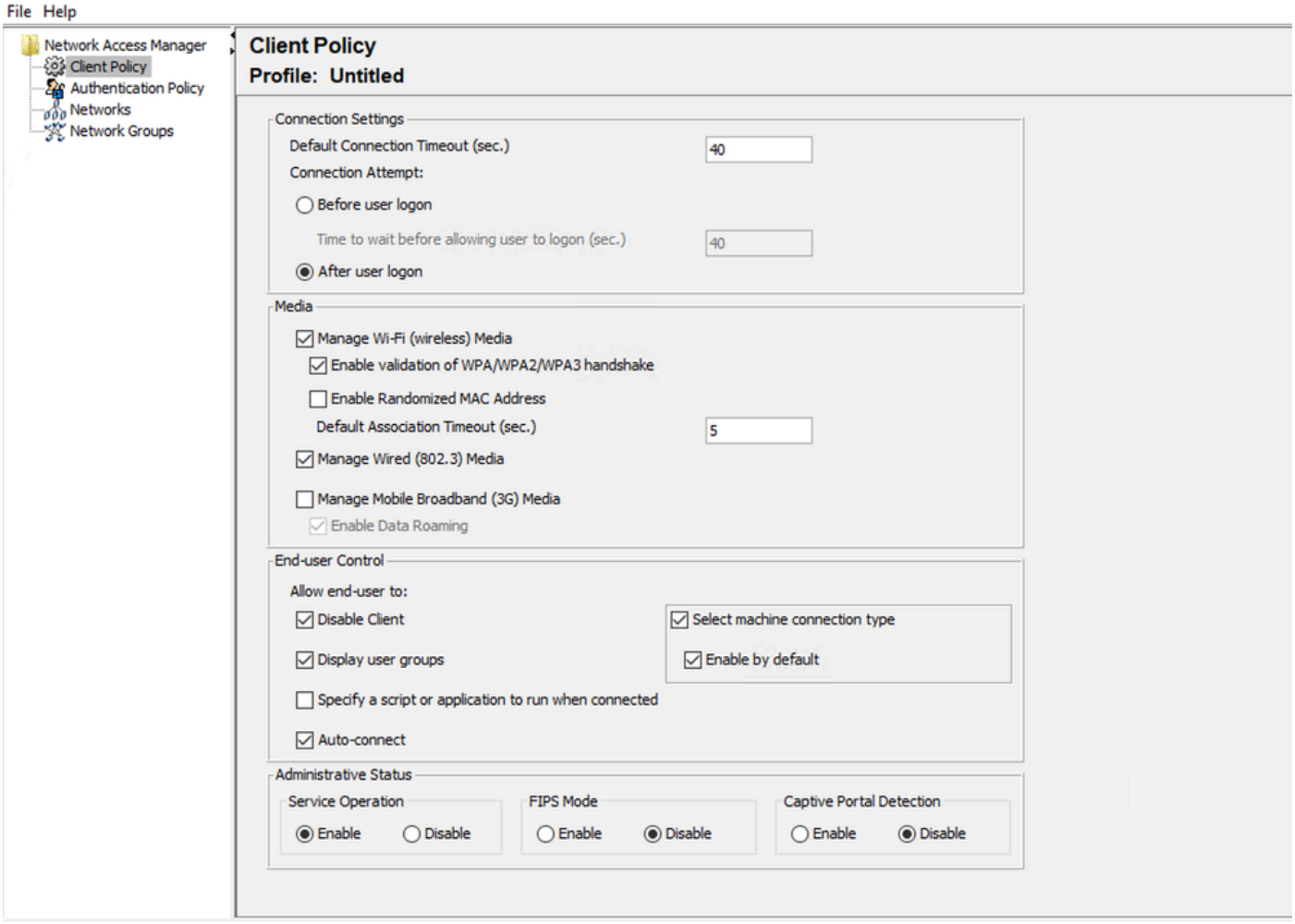
Éditeur de profil pour NAM dans la barre de recherche

9. L'installation de Network Access Manager et de Profile Editor est terminée.

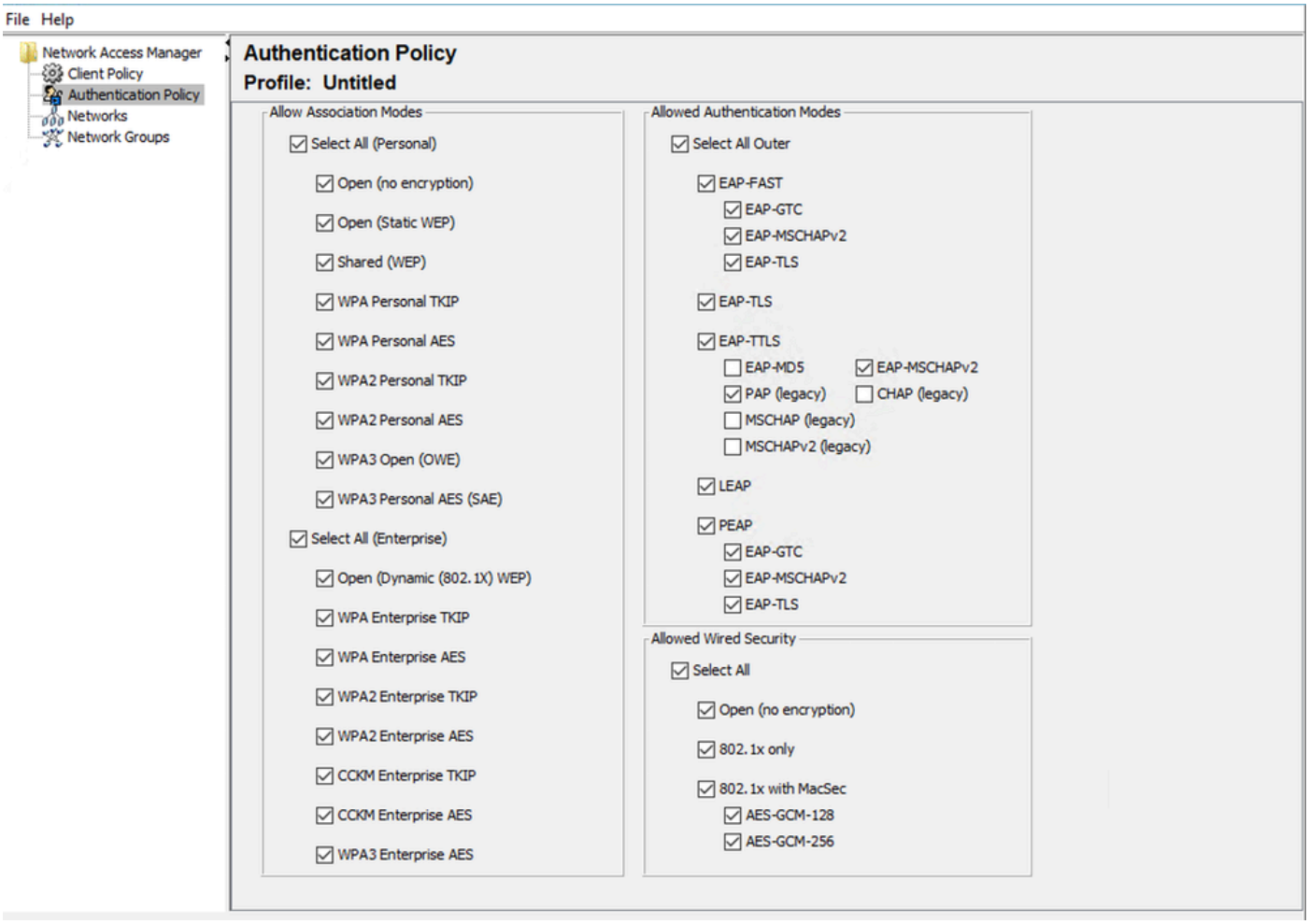
Configurations générales par défaut

1. Tous les scénarios présentés dans cet article contiennent des configurations pour :

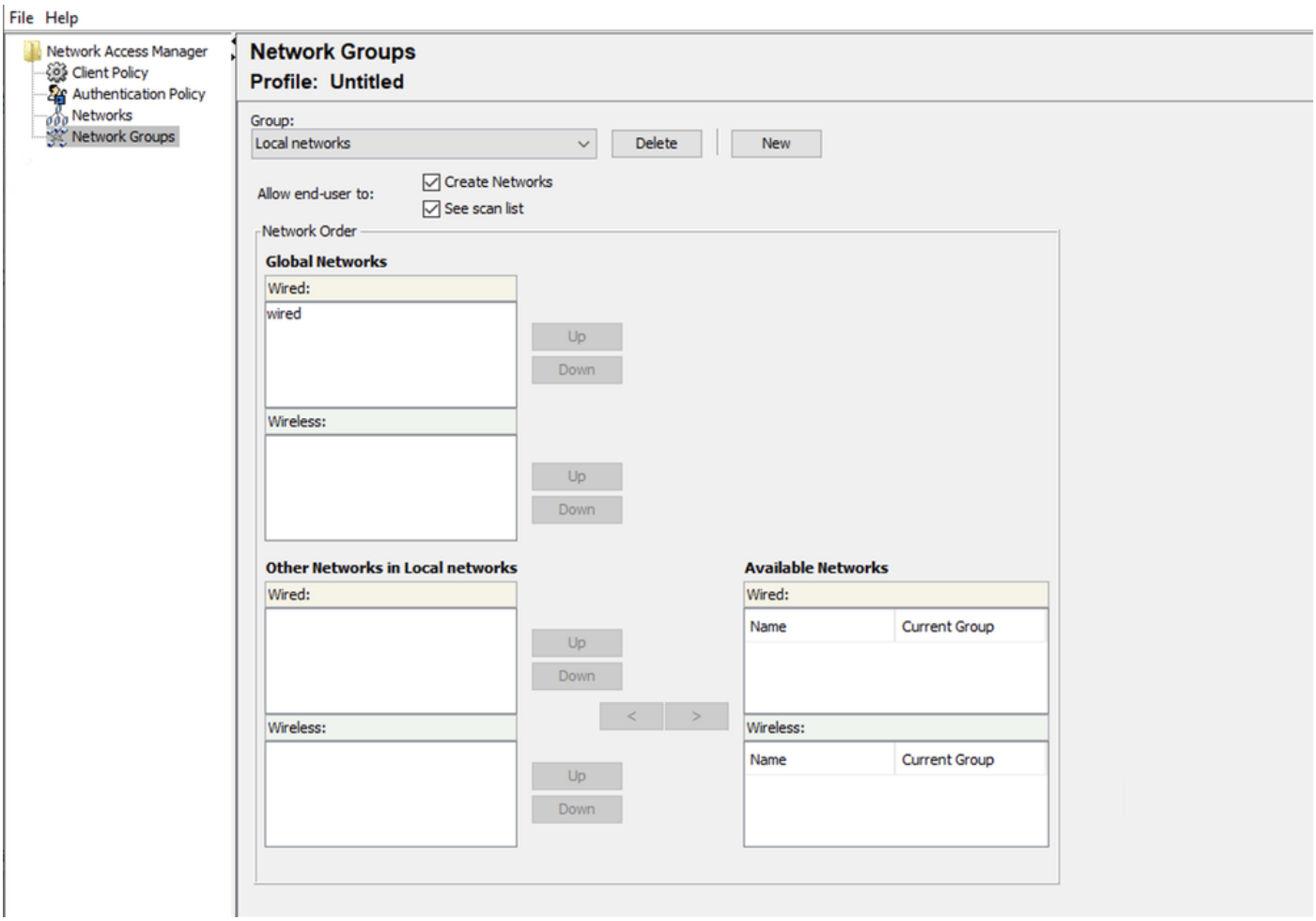
- Stratégie client
- Stratégie d'authentification
- Groupes réseau



Stratégie du client Éditeur de profil NAM



Stratégie d'authentification NAM Profile Editor



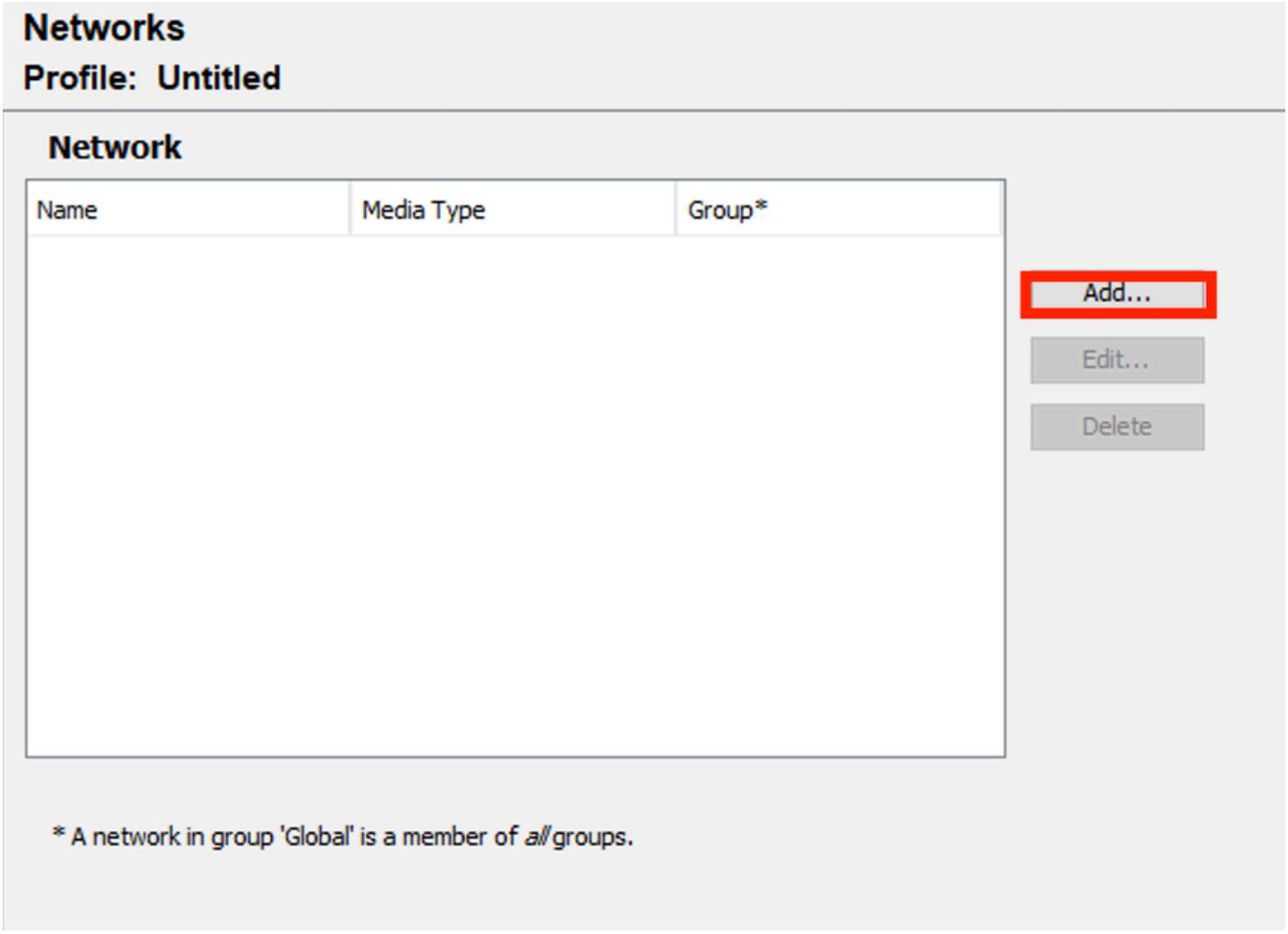
Onglet Groupes de réseaux

Scénario 1 : Configuration du demandeur NAM du client sécurisé pour l'authentification des utilisateurs PEAP (MS-CHAPv2)

1. Accédez à la section Réseaux.

2. Le profil réseau par défaut peut être supprimé.

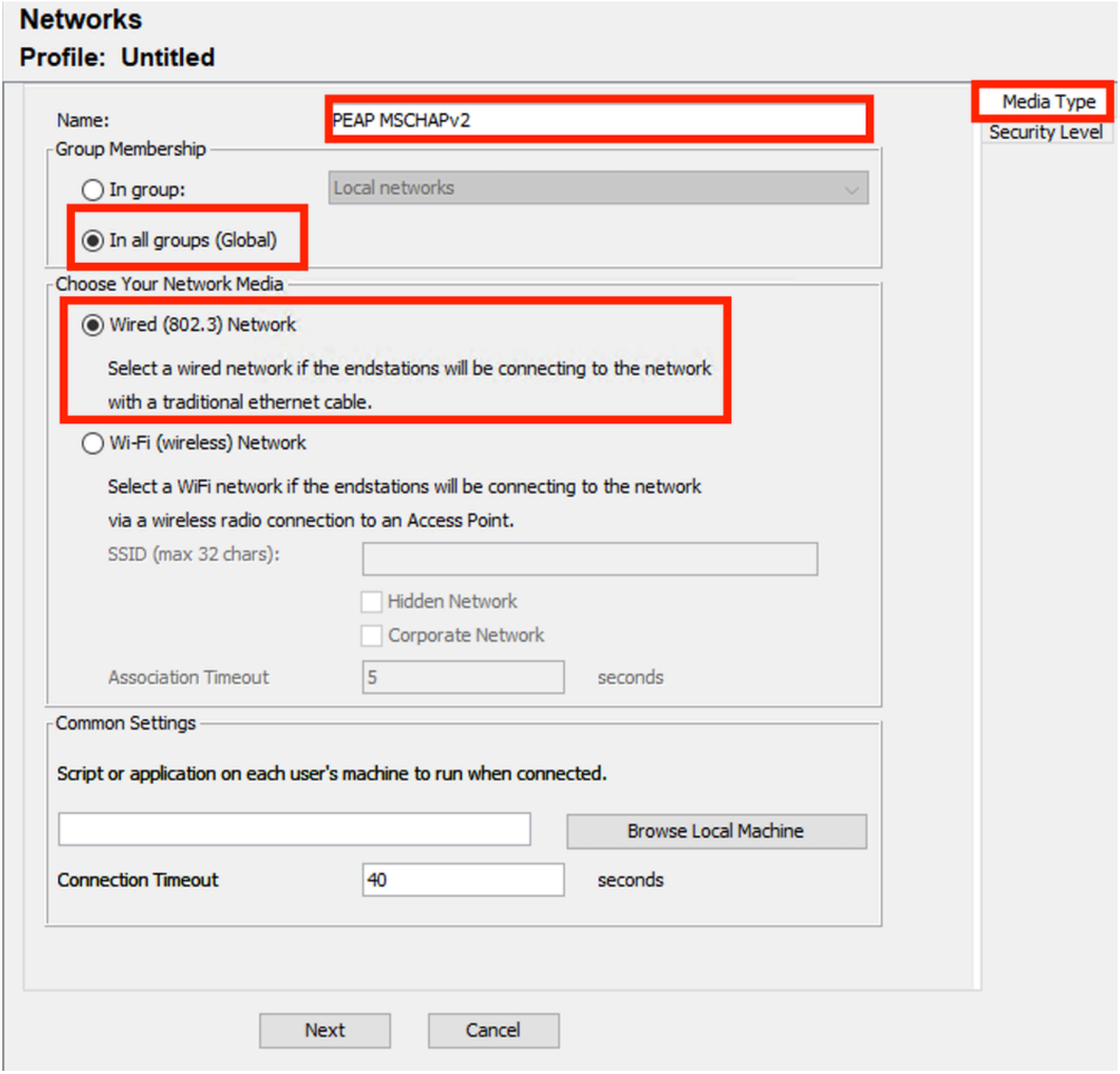
3. Cliquez sur Ajouter.



Création de profils réseau

4. Nommez le profil réseau.

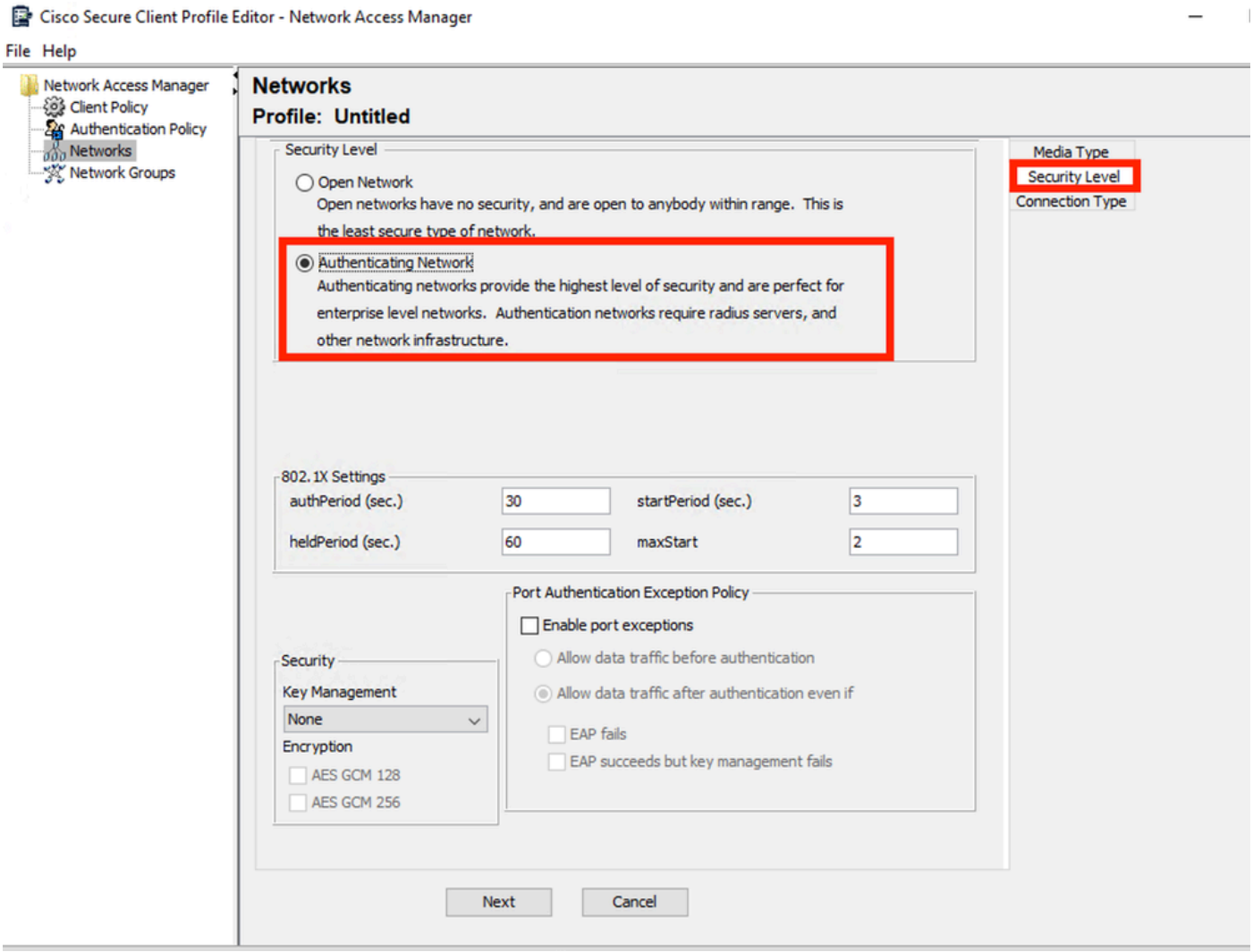
5. Sélectionnez Global pour Appartenance au groupe. Sélectionnez Média réseau câblé.



Section Network Profile Media Type

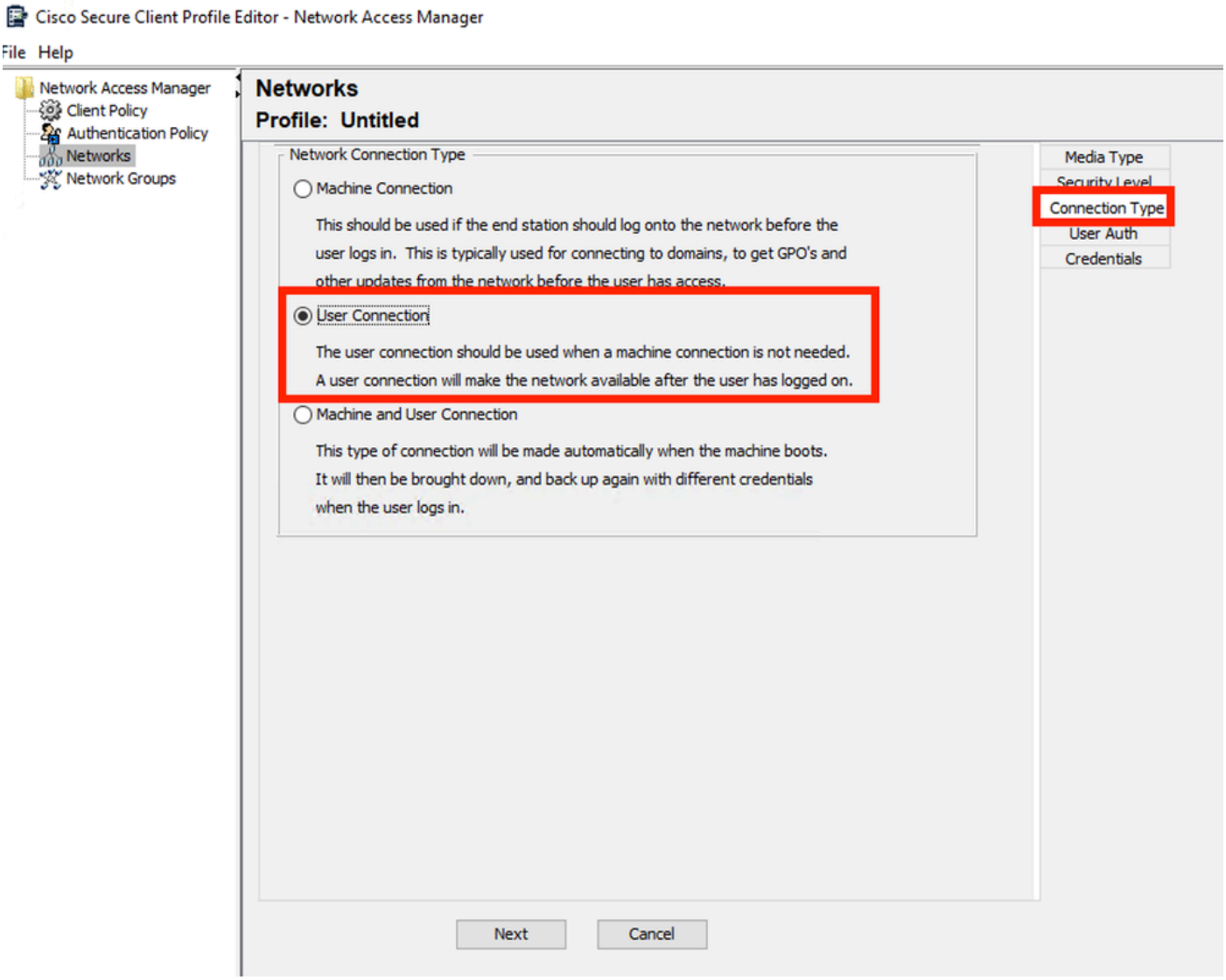
6. Cliquez sur Suivant.

7. Sélectionnez Authenticating Network et utilisez la valeur par défaut pour les autres options de la section Security Level.



Niveau de sécurité du profil réseau

8. Cliquez sur Suivant pour passer à la section Type de connexion.

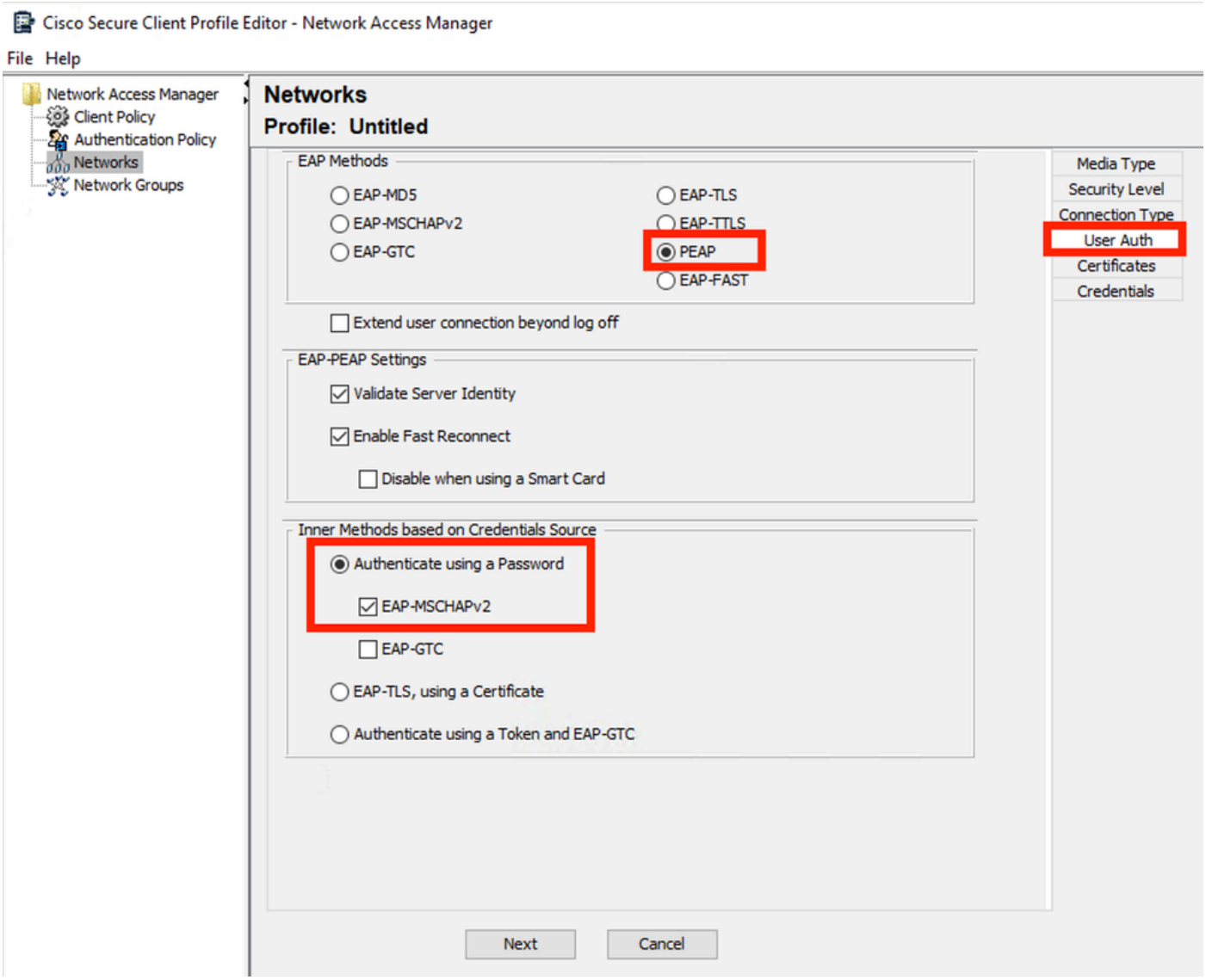


Type de connexion de profil réseau

9. Sélectionnez le type de connexion Connexion utilisateur.

10. Cliquez sur Next pour passer à la section User Auth, qui est désormais disponible.

11. Sélectionnez PEAP comme méthode EAP générale.



Authentification utilisateur profil réseau

12. Ne modifiez pas les valeurs par défaut dans les paramètres EAP-PEAP.

13. Poursuivez avec la section Méthodes internes basées sur la source des informations d'identification.

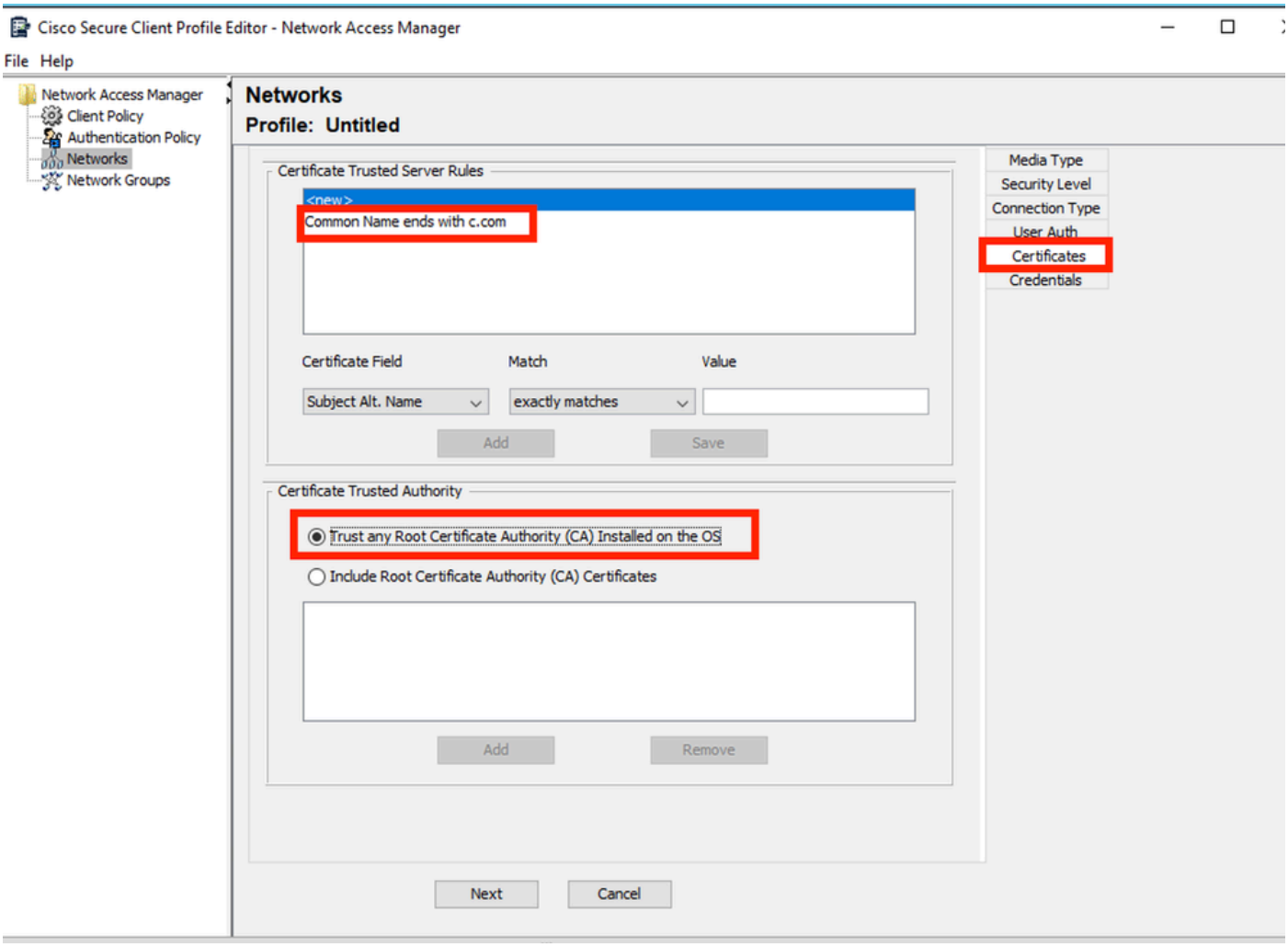
14. Parmi les multiples méthodes internes qui existent pour EAP PEAP, sélectionnez Authenticate using a Password et sélectionnez EAP-MSCHAPv2.

15. Cliquez sur Next pour passer à la section Certificate.

Remarque : La section Certificate s'affiche lorsque l'option Validate Server Identity dans les paramètres EAP-PEAP est sélectionnée. Pour EAP PEAP, il effectue l'encapsulation à l'aide du certificat du serveur.

---

16. Dans la section Certificates, Certificate Trusted Server Rules, la règle Common Name se termine par c.com est utilisée. Cette section de la configuration fait référence au certificat que le serveur utilise pendant le flux PEAP EAP. Si le moteur ISE (Identity Service Engine) est utilisé dans votre environnement, vous pouvez utiliser le nom commun du certificat EAP du noeud du serveur de stratégie.

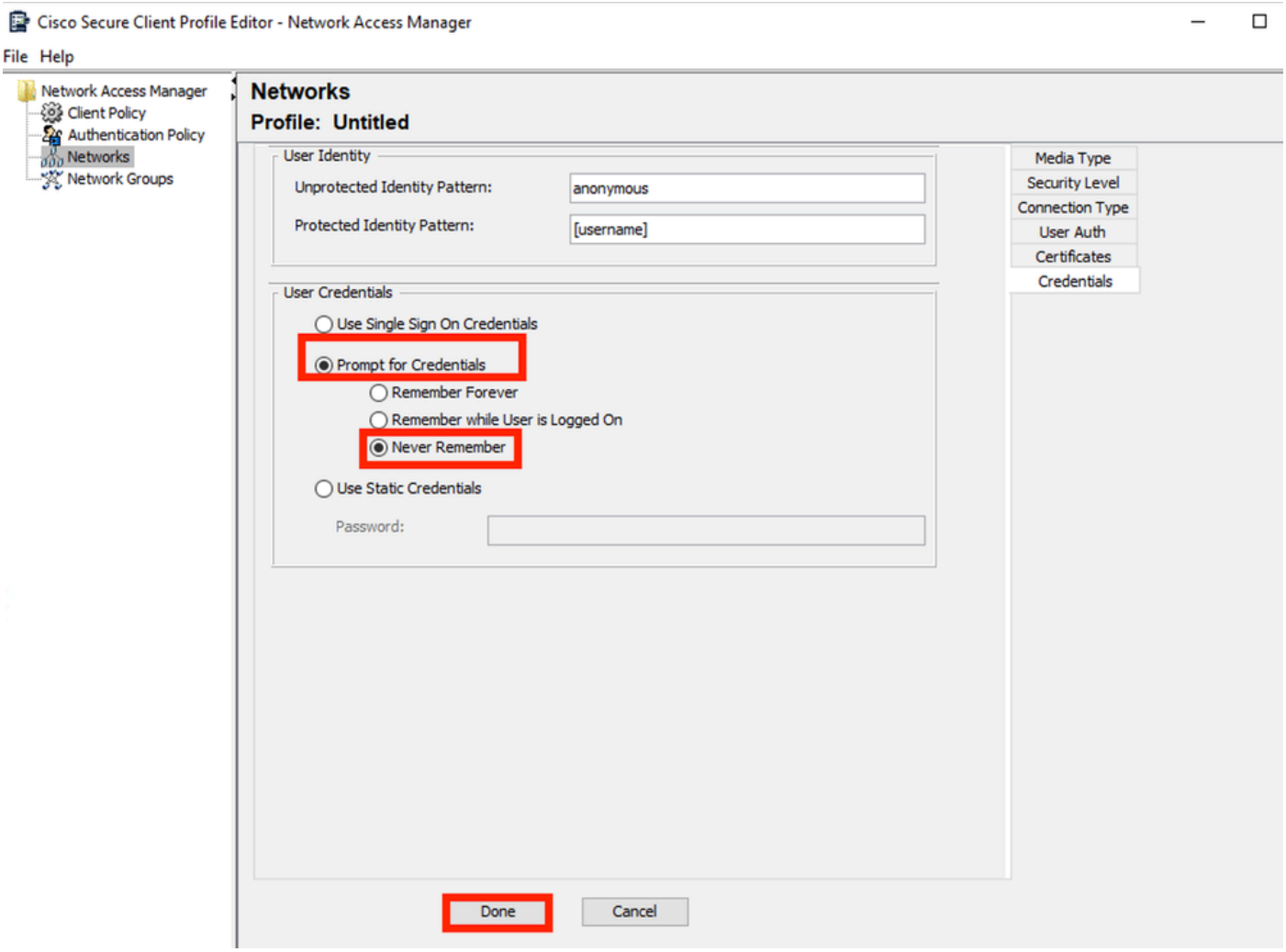


Section Certificat de profil réseau

17. Deux options peuvent être sélectionnées dans l'autorité de certification approuvée. Pour ce scénario, au lieu d'ajouter un certificat d'autorité de certification spécifique qui a signé le certificat RADIUS EAP, l'option Approuver toute autorité de certification racine installée sur le système d'exploitation est utilisée.

18. Avec cette option, le périphérique Windows approuve tout certificat EAP signé par un certificat inclus dans le programme Gérer les certificats utilisateur Certificats — Utilisateur actuel > Autorités de certification racine de confiance > Certificats.

19. Cliquez sur Next.



Section Network Profile Credentials

20. Dans la section Informations d'identification, seule la section Informations d'identification utilisateur est modifiée.

21. L'option Demander les informations d'identification > Ne jamais se souvenir est sélectionnée. Dans chaque authentification, l'utilisateur qui sélectionne l'authentification doit entrer ses informations d'identification.

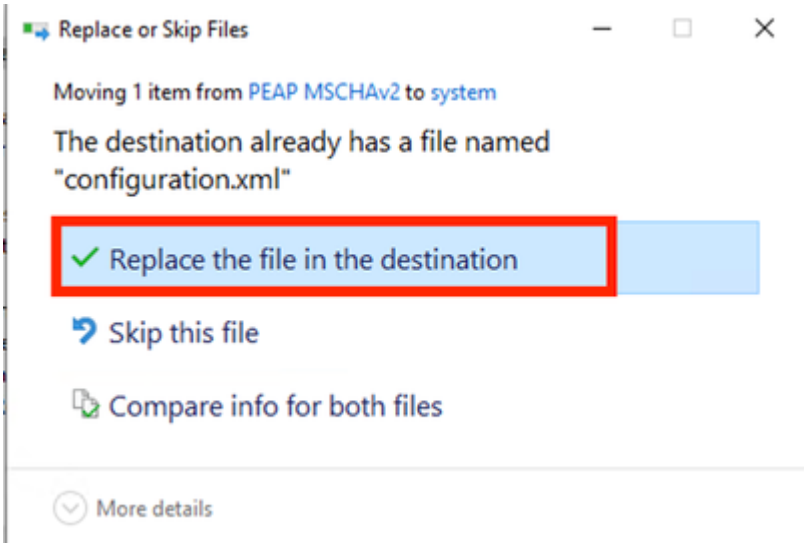
22. Cliquez sur Terminé.

23. Enregistrez le profil Secure Client Network Access Manager sous le nom configuration.xml avec l'option File > Save As.

24. Pour vous assurer que Secure Client Network Access Manager utilise le profil que vous venez de créer, remplacez le fichier configuration.xml dans le répertoire suivant par le nouveau :

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

Remarque : Le fichier doit être nommé configuration.xml, sinon il ne fonctionne pas.

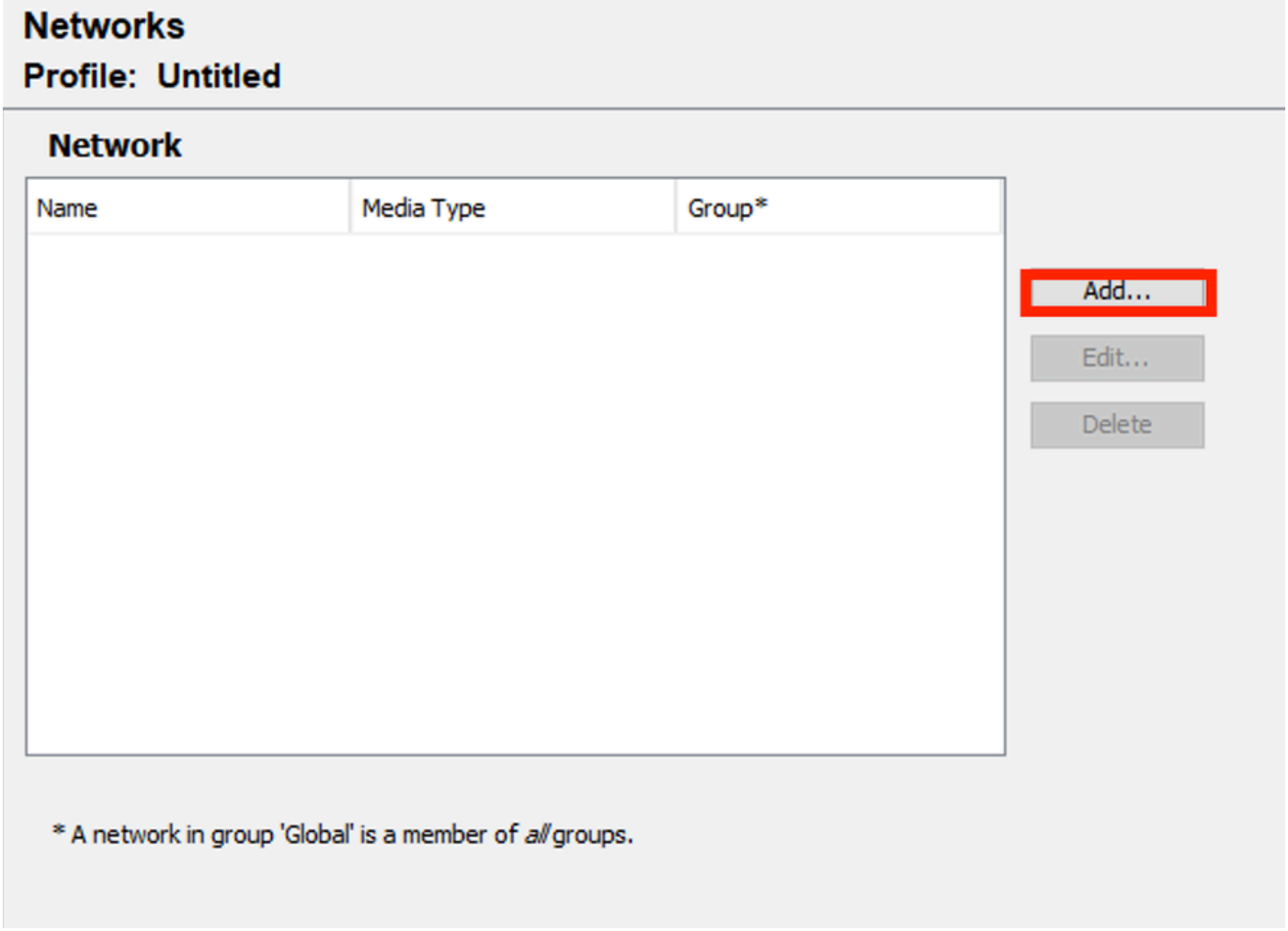


Remplacer la section de fichier

Scénario 2 : Configurer le demandeur NAM du client sécurisé pour l'authentification simultanée des utilisateurs et des machines EAP-FAST

1. Ouvrez l'Éditeur de profil NAM et accédez à la section Réseaux.

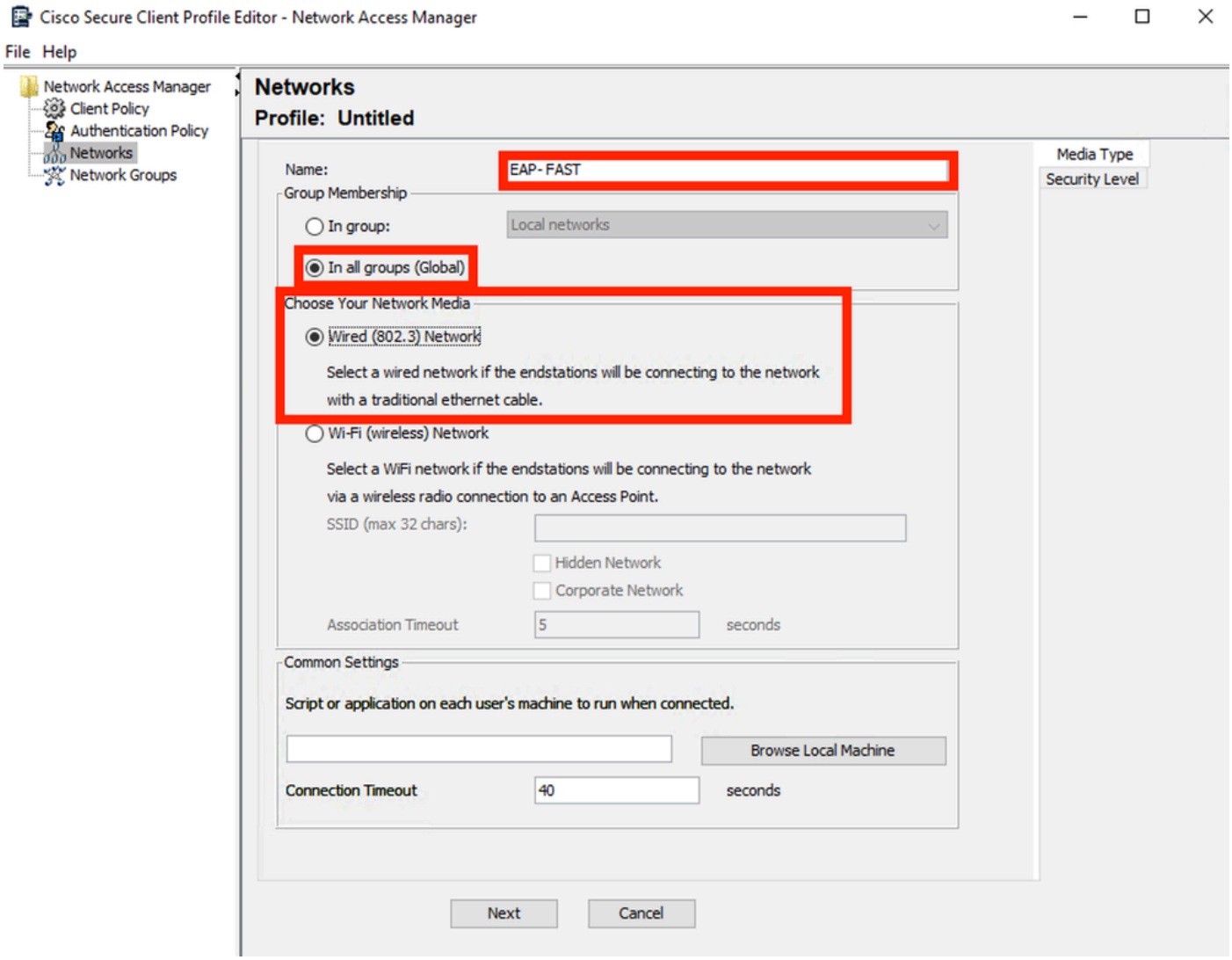
2. Cliquez sur Ajouter.



Onglet Réseau de NAM Profile Editor

3. Entrez un nom dans le profil réseau.

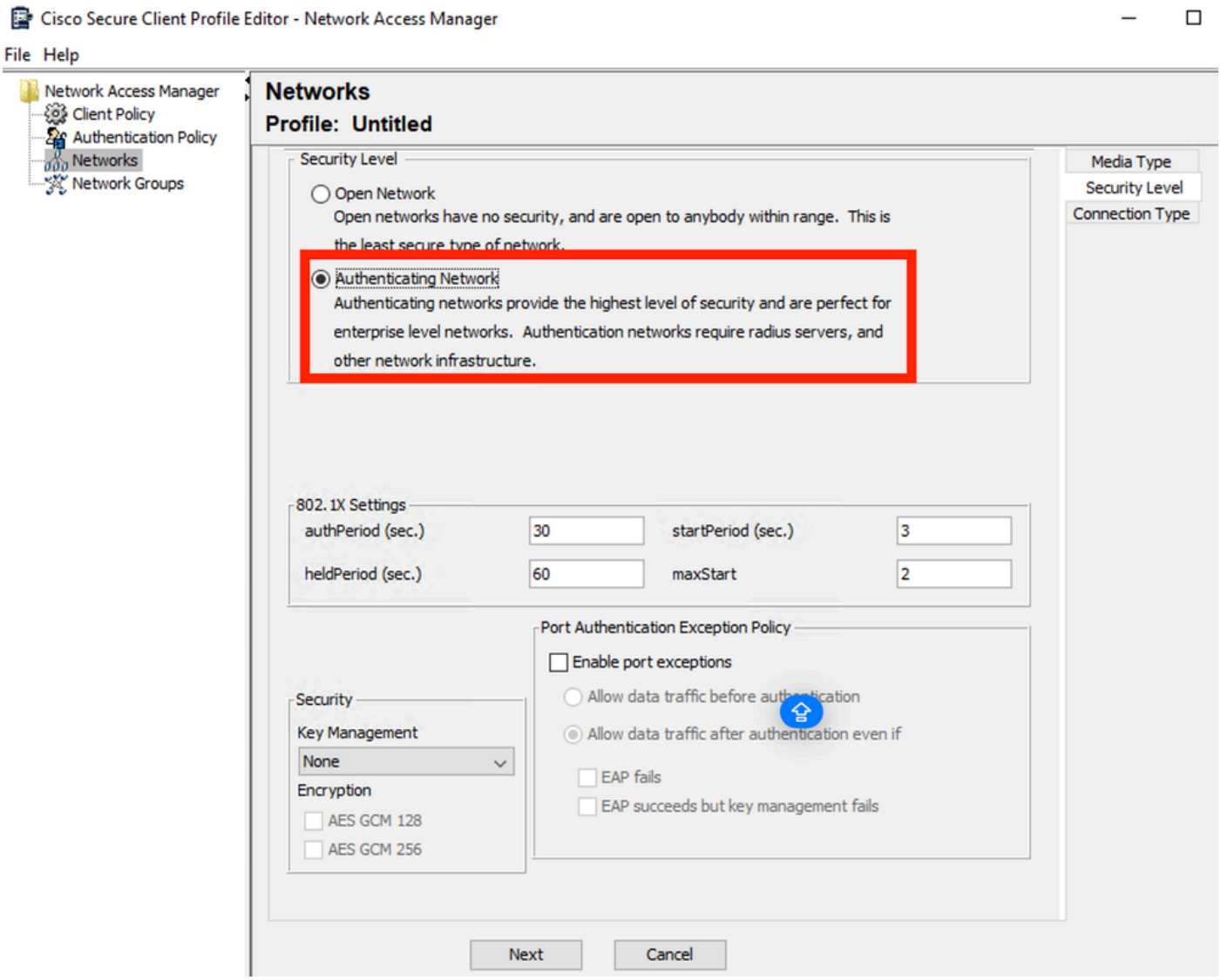
4. Sélectionnez Global pour Appartenance au groupe. Sélectionnez Média réseau filaire.



Section Type de support

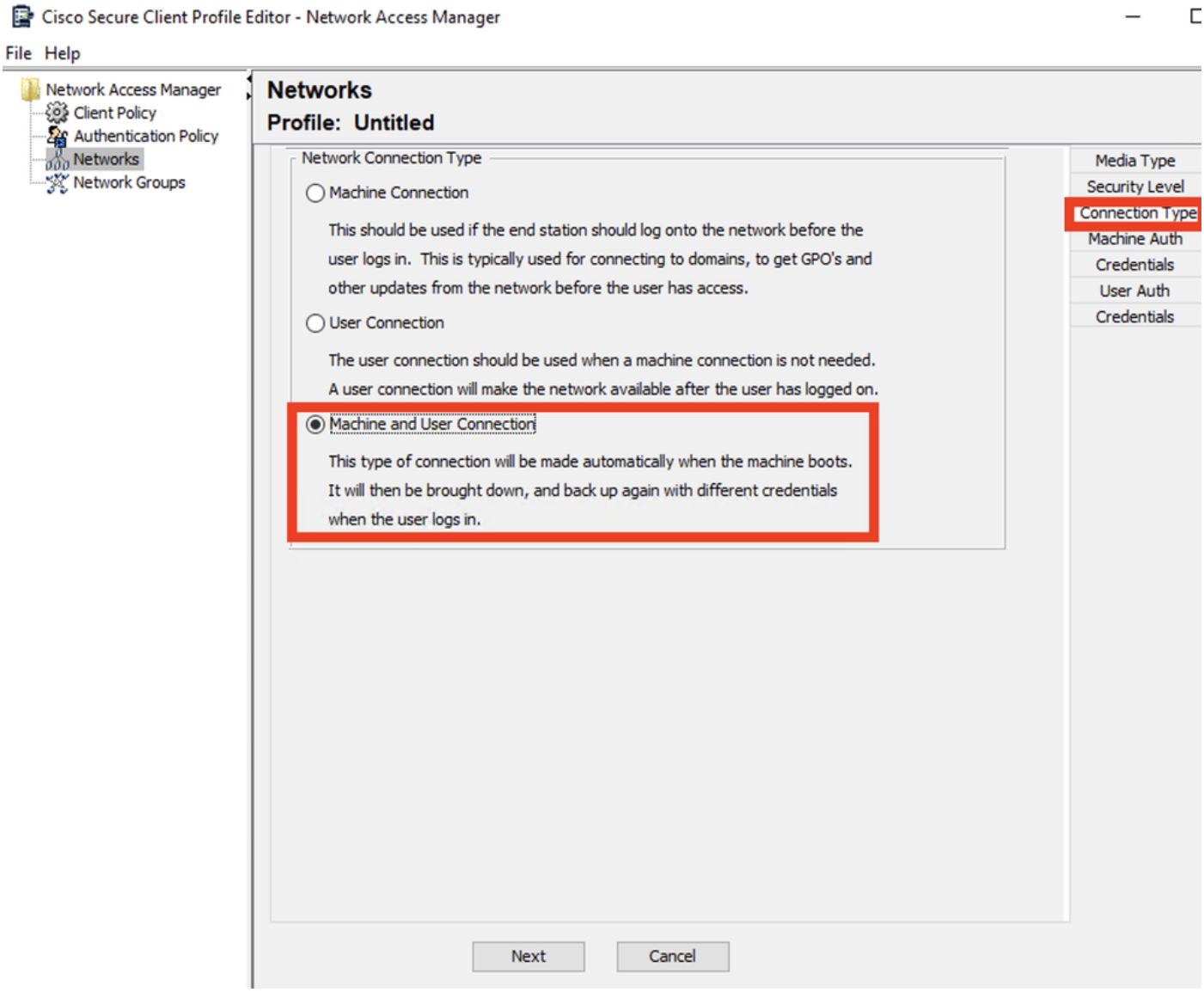
5. Cliquez sur Suivant.

6. Sélectionnez Authenticating Network et ne modifiez pas les valeurs par défaut pour les autres options de cette section.



Section Éditeur de profil de niveau de sécurité

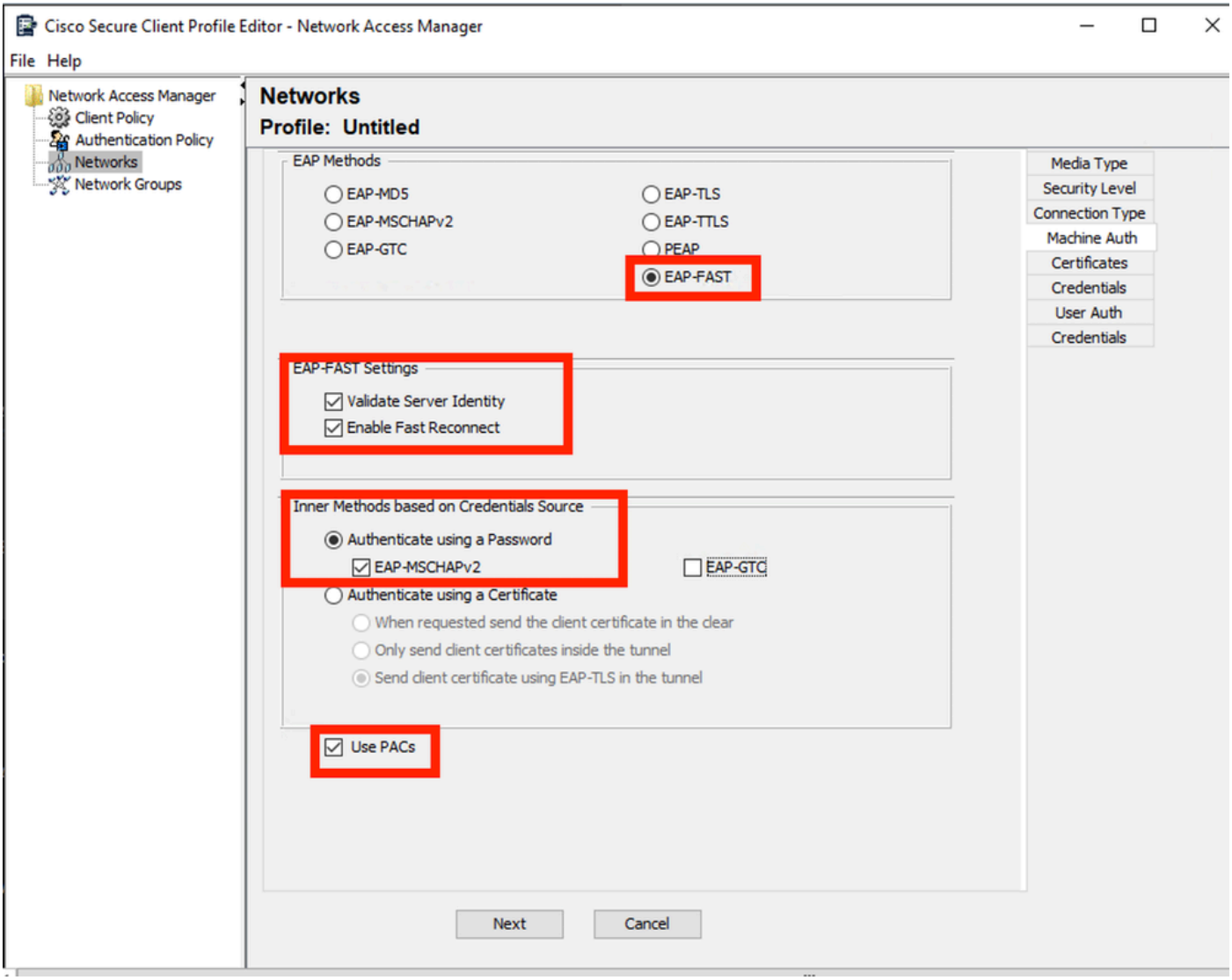
7. Cliquez sur Suivant pour passer à la section Type de connexion.



Section Type de connexion

8. Configurez l'authentification de l'utilisateur et de la machine simultanément en sélectionnant la troisième option.

9. Cliquez sur Suivant.



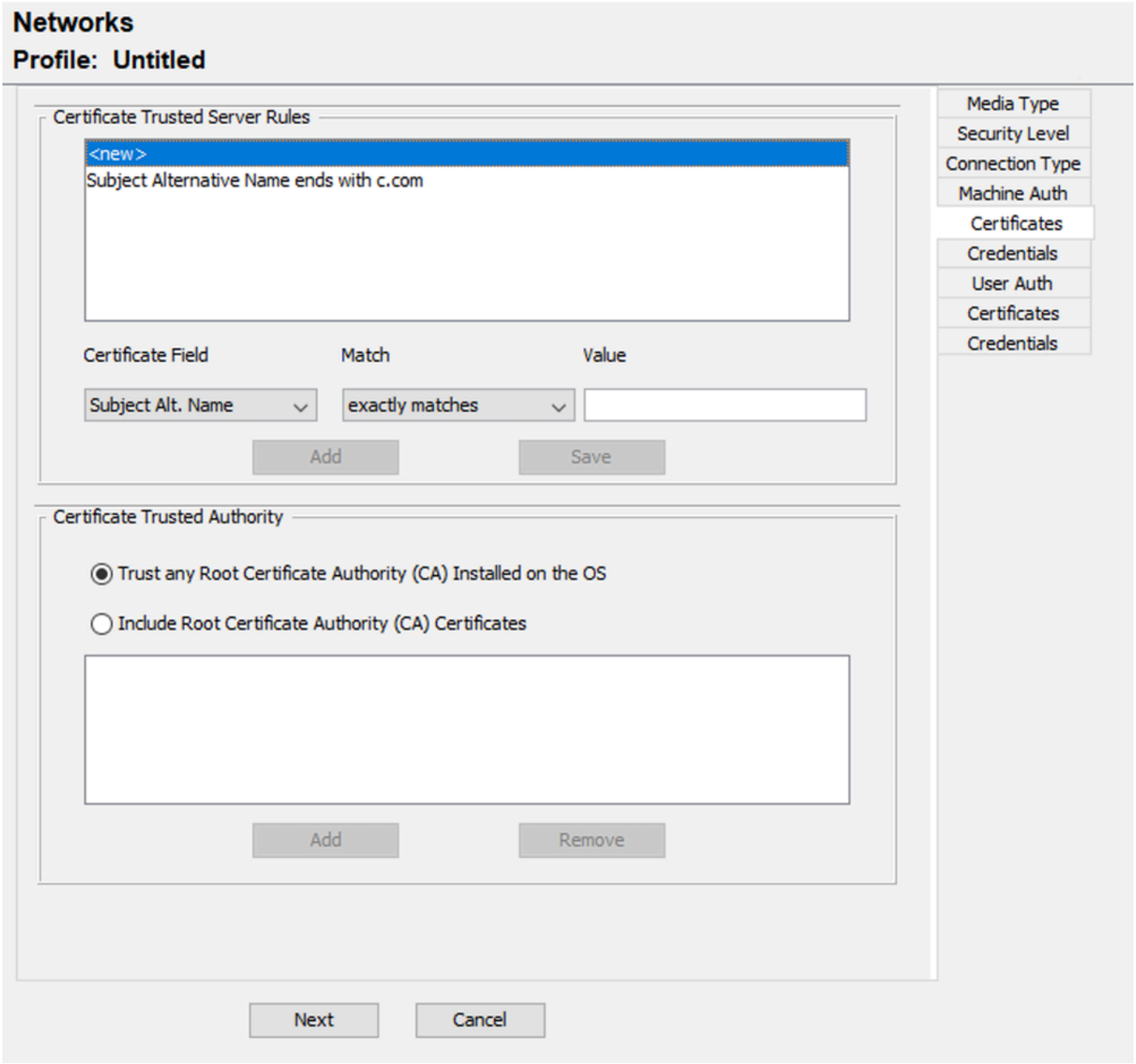
Section Authentification machine

10. Dans la section Auth machine, sélectionnez EAP-FAST comme méthode EAP. Ne modifiez pas les valeurs par défaut des paramètres EAP FAST.

11. Pour la section Méthodes internes basées sur la source des informations d'identification, sélectionnez Authentifier à l'aide d'un mot de passe et EAP-MSCHAPv2 comme méthode. Sélectionnez ensuite l'option Utiliser PACs.

12. Cliquez sur Next.

13. Dans la section Certificates, les règles de serveur de confiance de certificat, la règle est un nom commun se termine par c.com. Cette section fait référence au certificat que le serveur utilise pendant le flux PEAP EAP. Si Identity Service Engine (ISE) est utilisé dans votre environnement, le nom commun du certificat EAP du noeud du serveur de stratégie peut être utilisé.

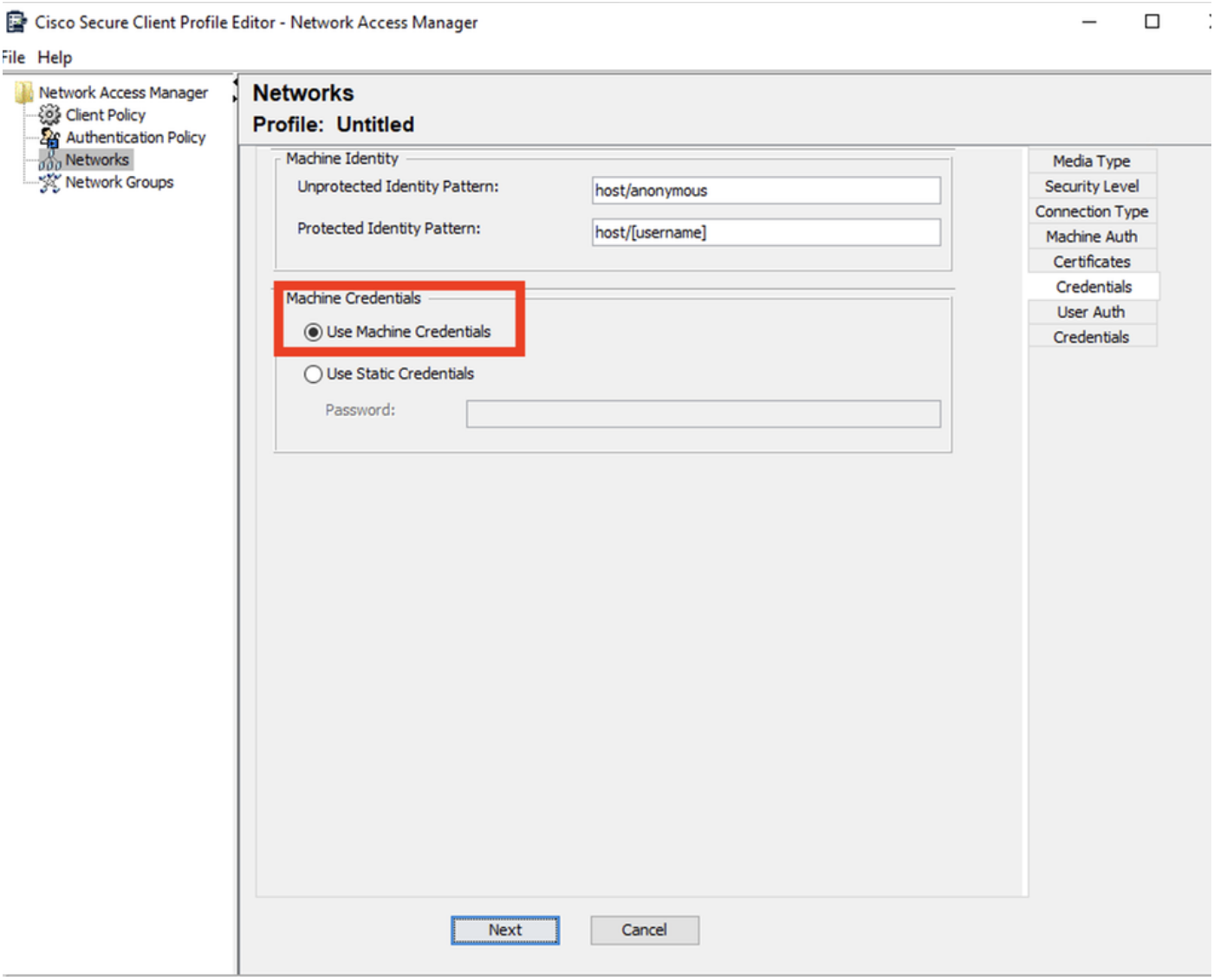


Section Autorisation du certificat du serveur d'authentification machine

14. Deux options peuvent être sélectionnées dans l'autorité de confiance du certificat. Dans ce scénario, au lieu d'ajouter un certificat CA spécifique qui a signé le certificat RADIUS EAP, utilisez l'option, Trust Any Root Certificate Authority (CA) Installed on the OS.

15. Avec cette option, Windows approuve tout certificat EAP signé par un certificat inclus dans le programme Gérer les certificats utilisateur (Utilisateur actuel > Autorités de certification racines de confiance > Certificats).

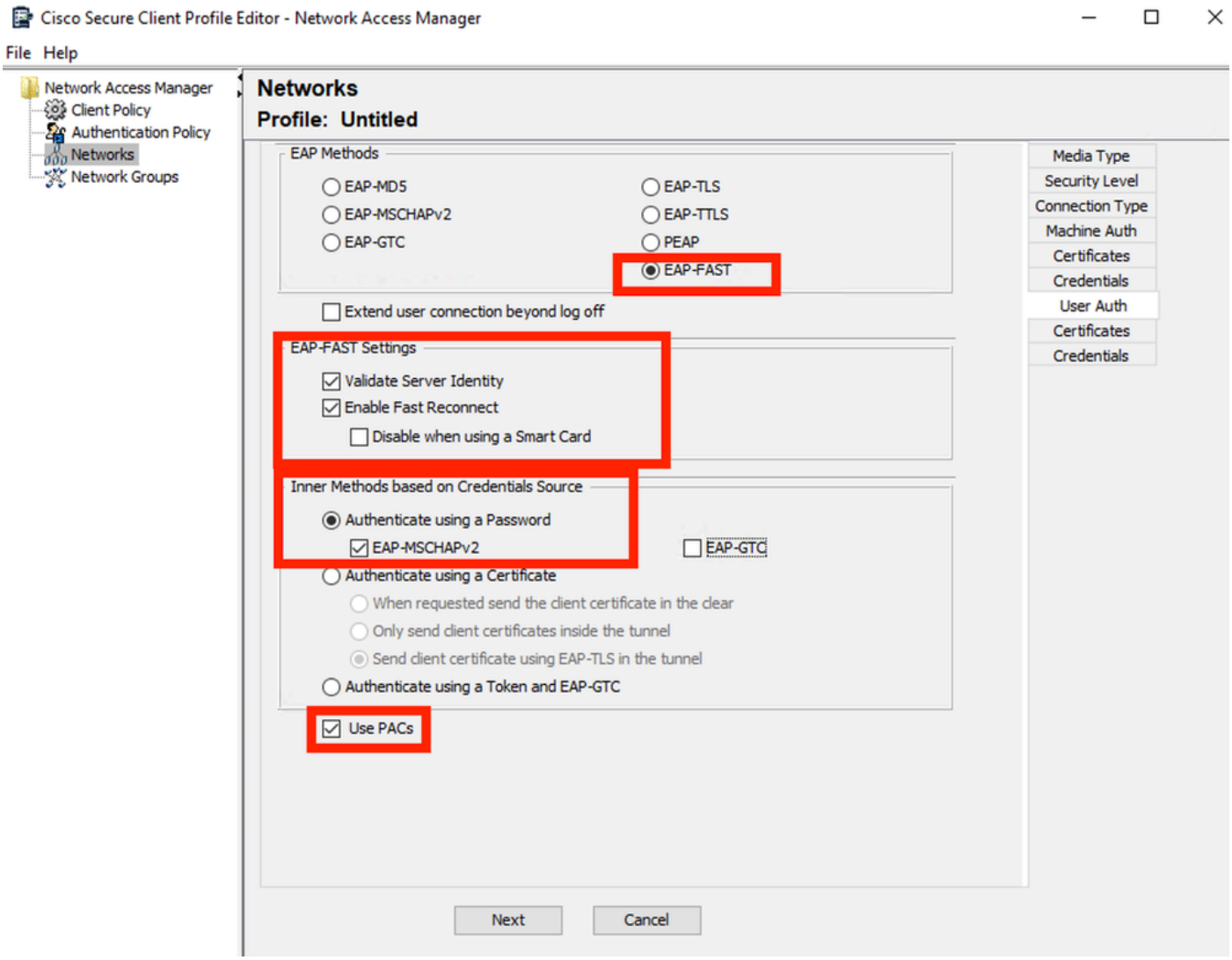
16. Cliquez sur Next.



Section Authentifications d'authentification machine

17. Sélectionnez Utiliser les informations d'identification de la machine dans la section Informations d'identification de la machine.

18. Cliquez sur Next.



Section Authentification utilisateur

19. Pour User Auth, sélectionnez EAP-FAST comme méthode EAP.

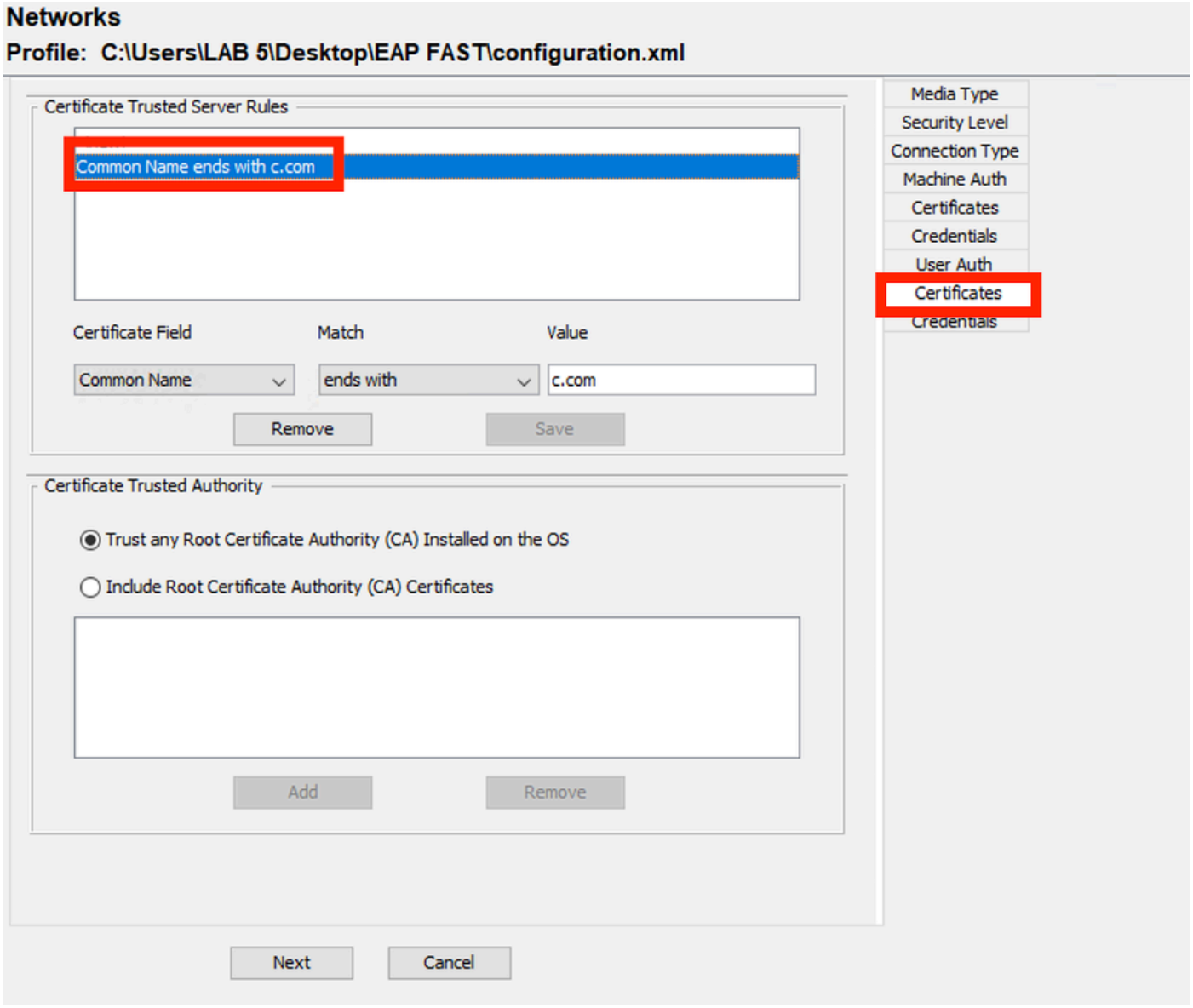
20. Ne modifiez pas les valeurs par défaut dans la section des paramètres EAP-FAST.

21. Pour la section Méthode interne basée sur la source des informations d'identification, sélectionnez Authentifier à l'aide d'un mot de passe et EAP-MSCHAPv2 comme méthode.

22. Sélectionnez Utiliser PAC.

23. Cliquez sur Suivant.

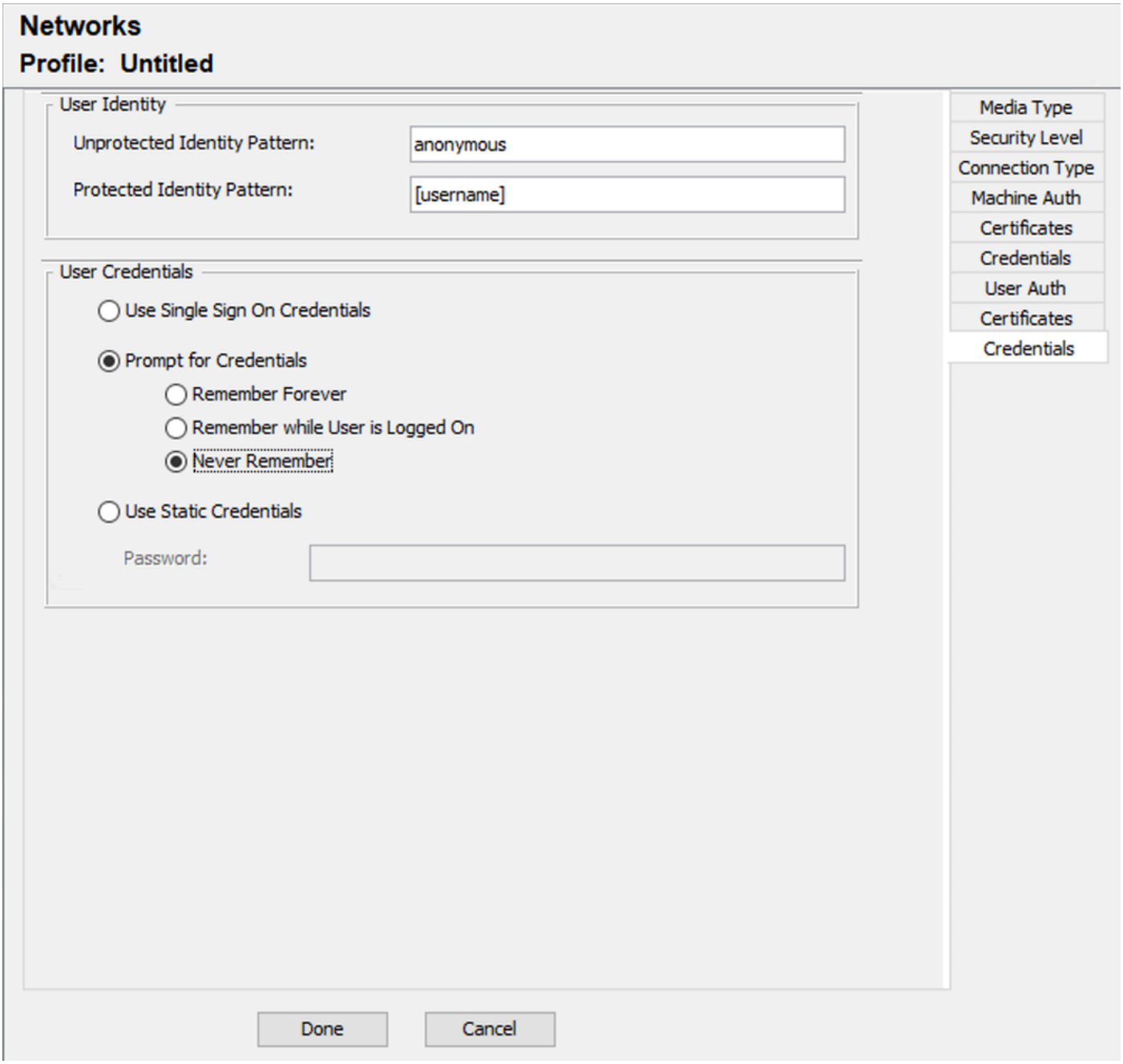
24. Dans la section Certificates, Règles de serveur de confiance de certificat, la règle est common Name se termine par c.com. Ces configurations sont destinées au certificat que le serveur utilise pendant le flux PEAP EAP. Si ISE est utilisé dans votre environnement, le nom commun du certificat EAP du noeud du serveur de stratégie peut être utilisé.



Section Autorisation du certificat du serveur d'authentification utilisateur

25. Deux options peuvent être sélectionnées dans l'autorité de confiance du certificat. Dans ce scénario, au lieu d'ajouter un certificat CA spécifique qui a signé le certificat RADIUS EAP, l'option Trust Any Root Certificate Authority (CA) Installed on the OS est utilisée.

26. Cliquez sur Next.



Identifiants d'authentification utilisateur

27. Dans la section Informations d'identification, seule la section Informations d'identification utilisateur est modifiée.

28. L'option Demander les informations d'identification > Ne jamais se souvenir est sélectionnée. Ainsi, dans chaque authentification, l'utilisateur qui s'authentifie doit entrer ses informations d'identification.

29. Cliquez sur le bouton Terminé.

30. Sélectionnez Fichier > Enregistrer sous et enregistrez le profil Secure Client Network Access Manager sous le nom configuration.xml.

31. Pour créer le Gestionnaire d'accès réseau du client sécurisé, utilisez le profil que vous venez de créer et remplacez le fichier configuration.xml dans le répertoire suivant par le nouveau :

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

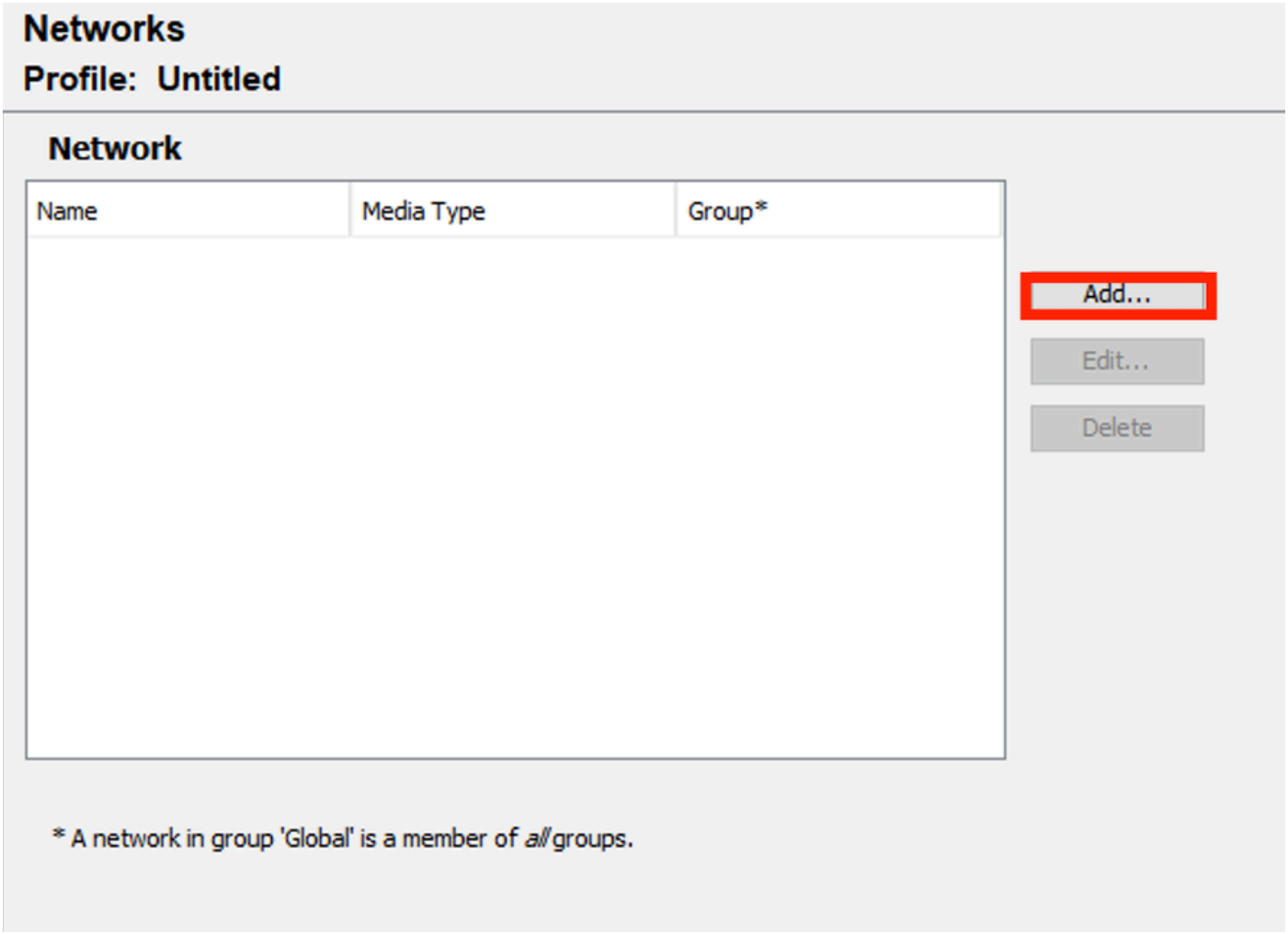
---

Remarque : Le fichier doit être nommé configuration.xml, sinon il ne fonctionne pas.

Scénario 3 : Configurer le demandeur NAM du client sécurisé pour l'authentification du certificat utilisateur EAP TLS

1. Ouvrez l'Éditeur de profil NAM et accédez à la section Réseaux.

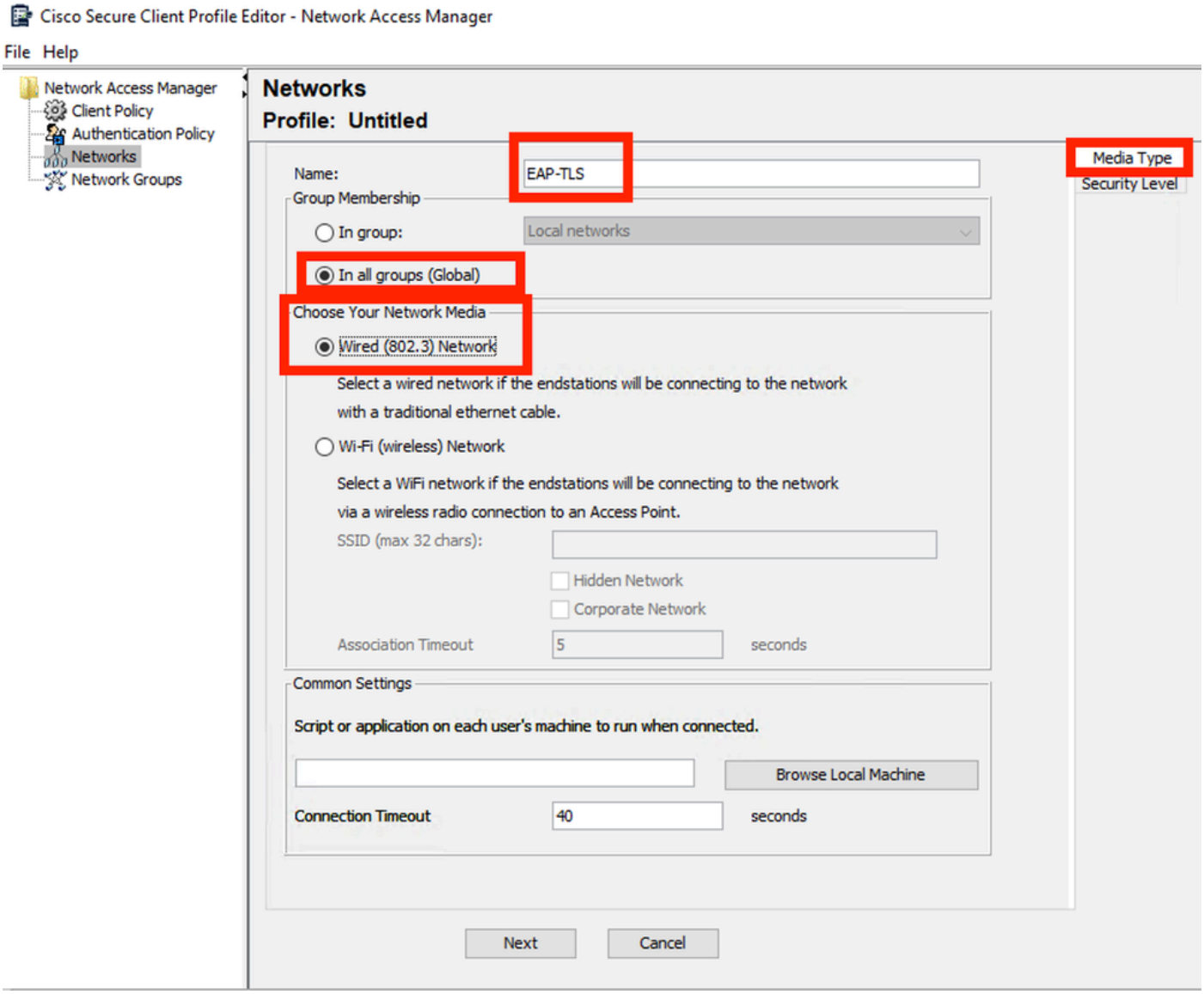
2. Cliquez sur Ajouter.



Section Création de réseau

3. Nommez le profil réseau, dans ce cas, le nom est le protocole EAP.

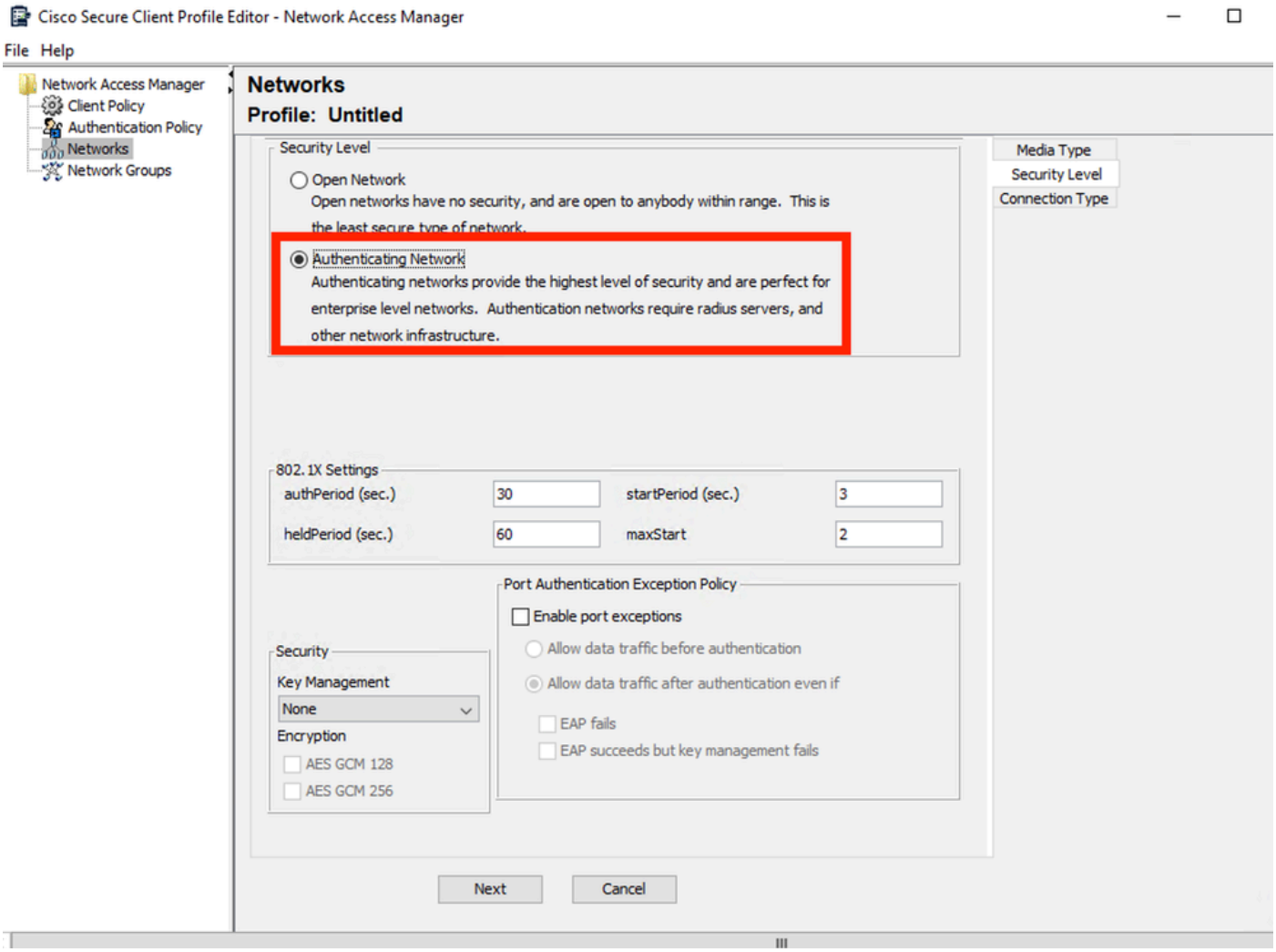
4. Sélectionnez Global pour Appartenance au groupe. Et Les Supports Réseau Filaires.



Section Type de support

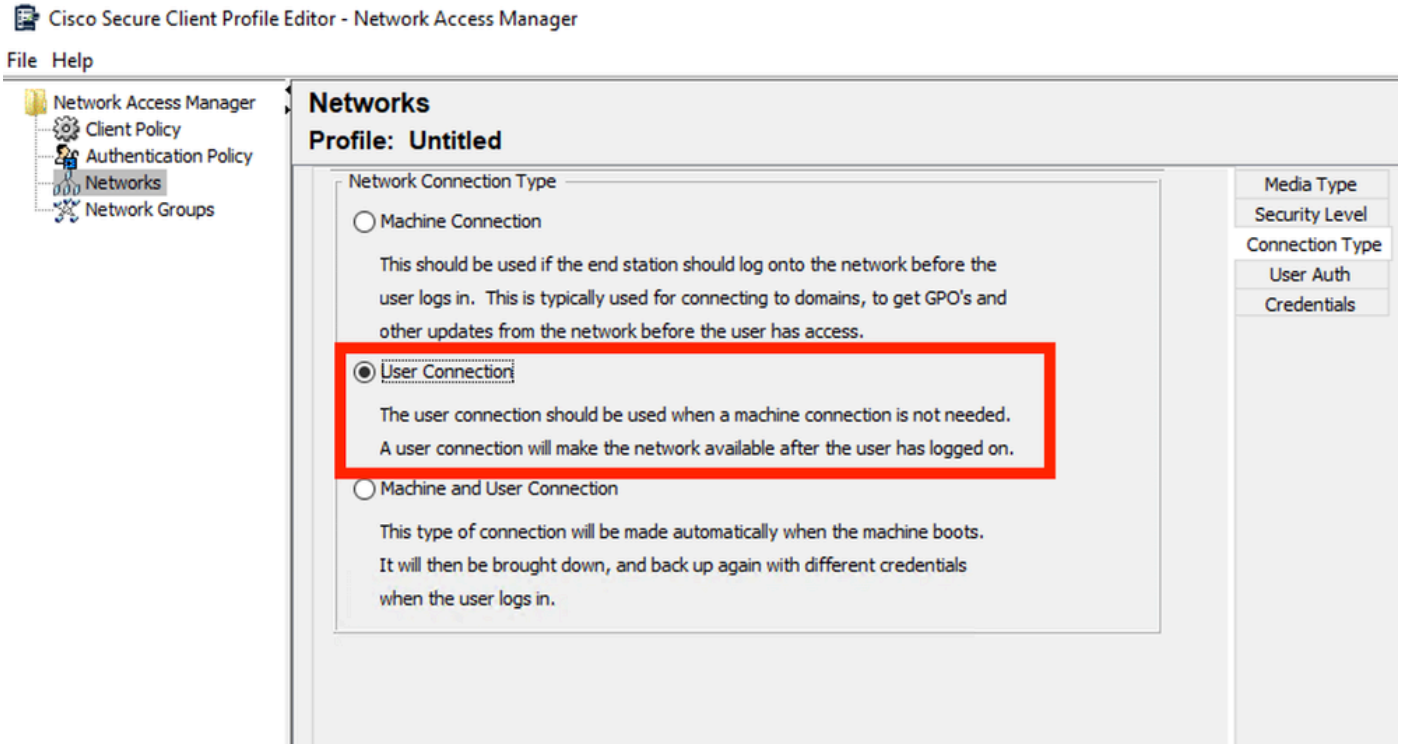
5. Cliquez sur Suivant.

6. Sélectionnez Authenticating Network et ne modifiez pas les valeurs par défaut pour les autres options de la section Security Level.



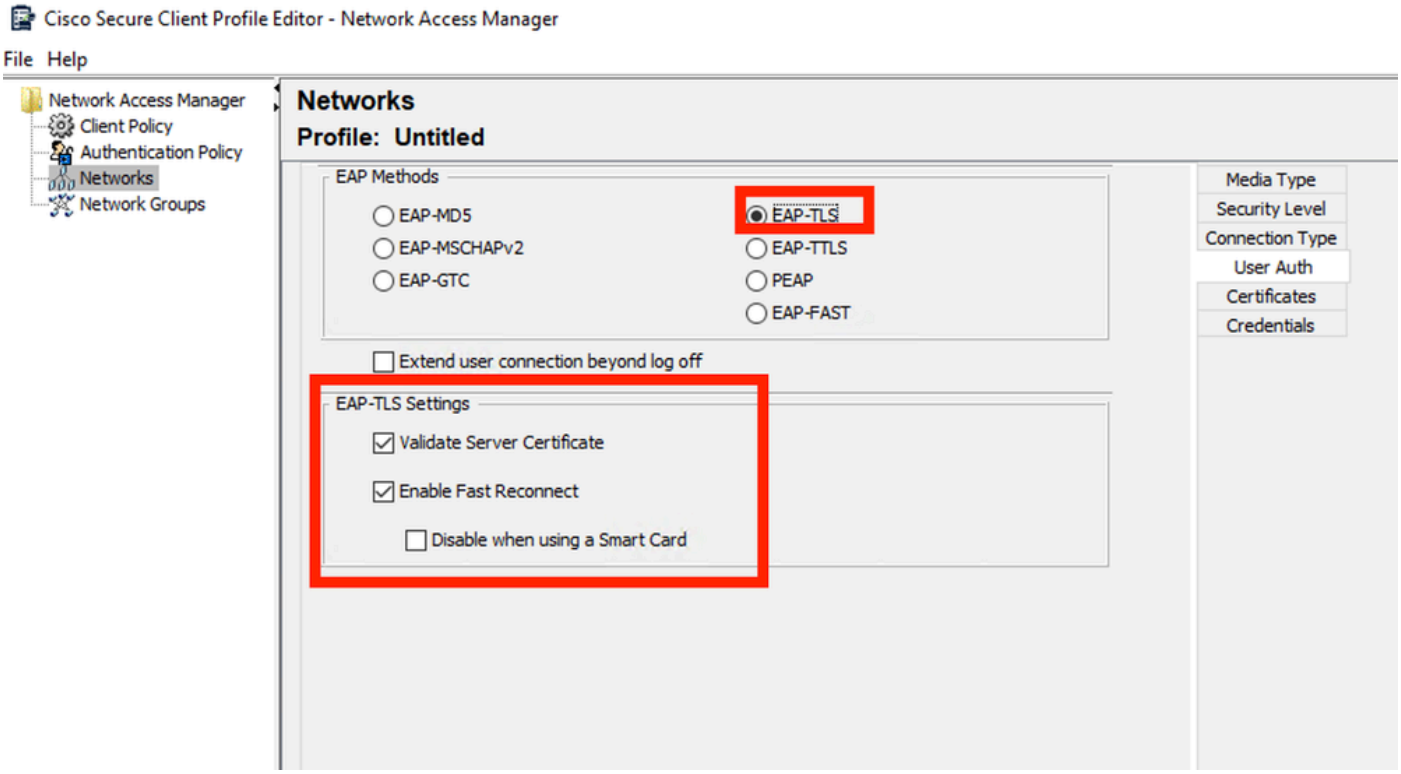
Niveau de sécurité

7. Ce scénario concerne l'authentification des utilisateurs à l'aide d'un certificat. Pour cette raison, l'option User Connection est utilisée.



Type de connexion

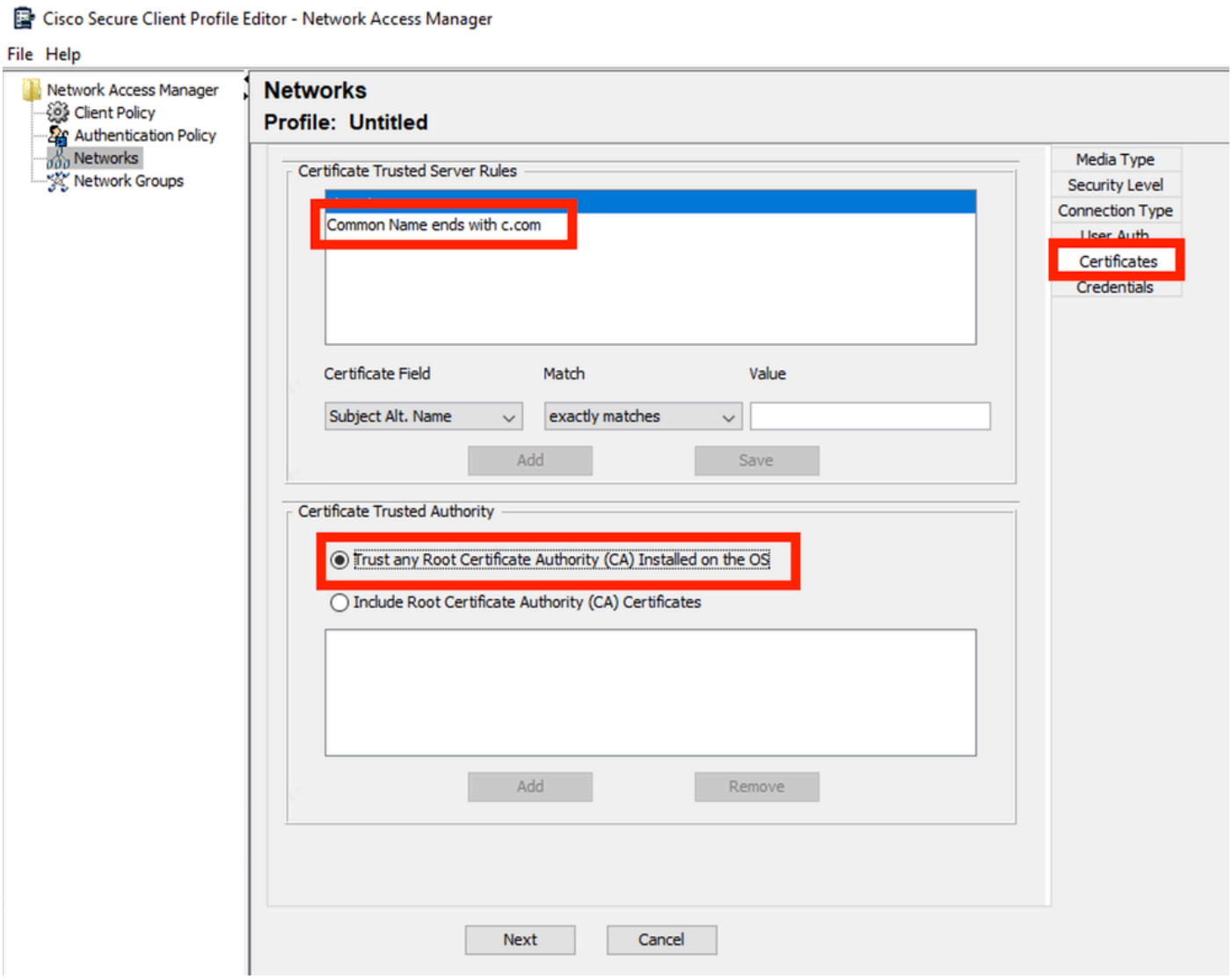
8. Configurez EAP-TLS comme méthode EAP et ne modifiez pas les valeurs par défaut dans la section Paramètres EAP-TLS.



Section User Auth

9. Pour la section Certificats, créez une règle qui correspond au certificat EAP-TLS AAA. Si vous utilisez ISE, recherchez cette règle dans la section Administration > Système > Certificats.

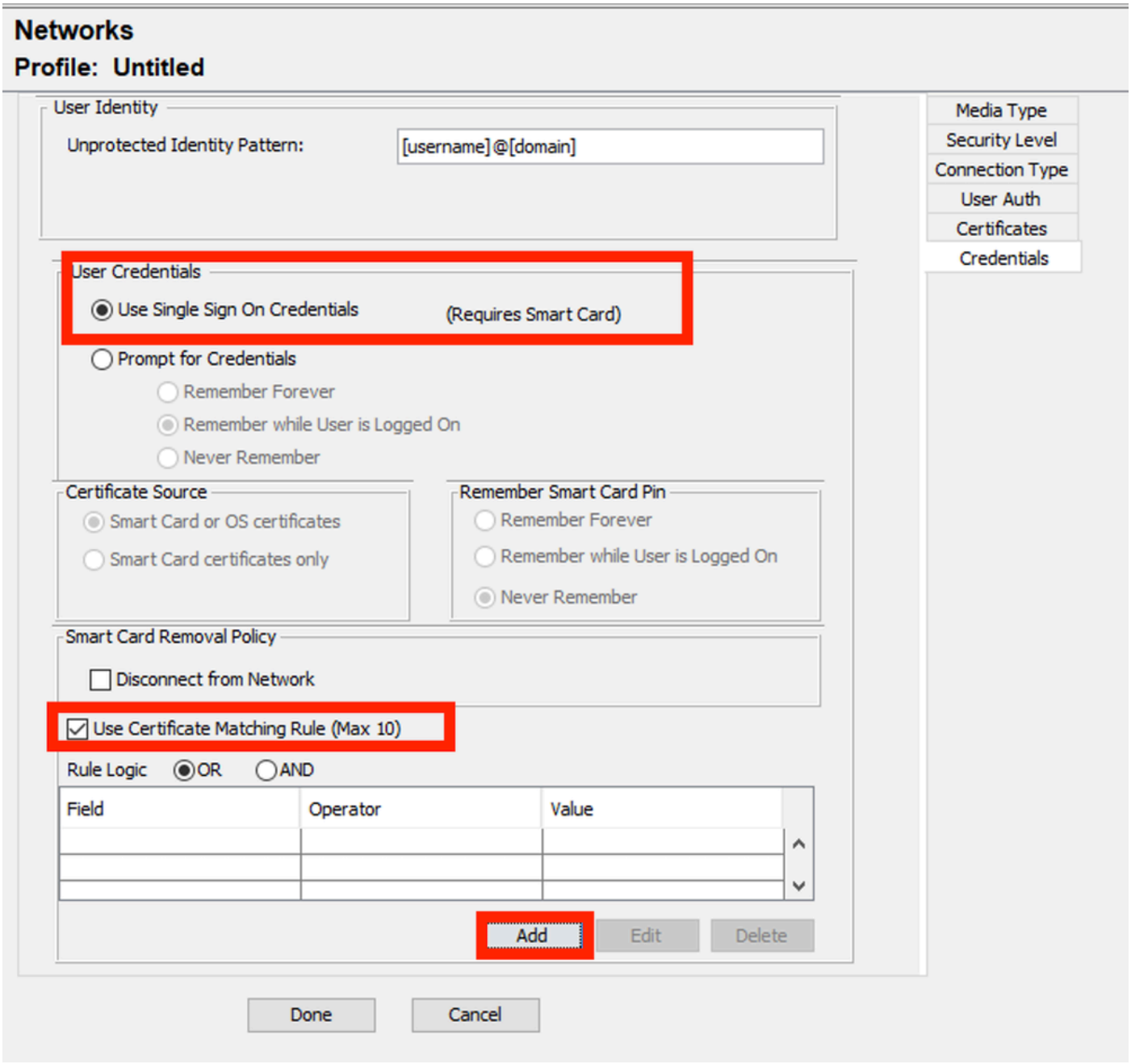
10. Dans la section Autorité de certification approuvée, sélectionnez Approuver toute autorité de certification racine installée sur le système d'exploitation.



Paramètres d'approbation des certificats du serveur d'authentification utilisateur

11. Cliquez sur Next.

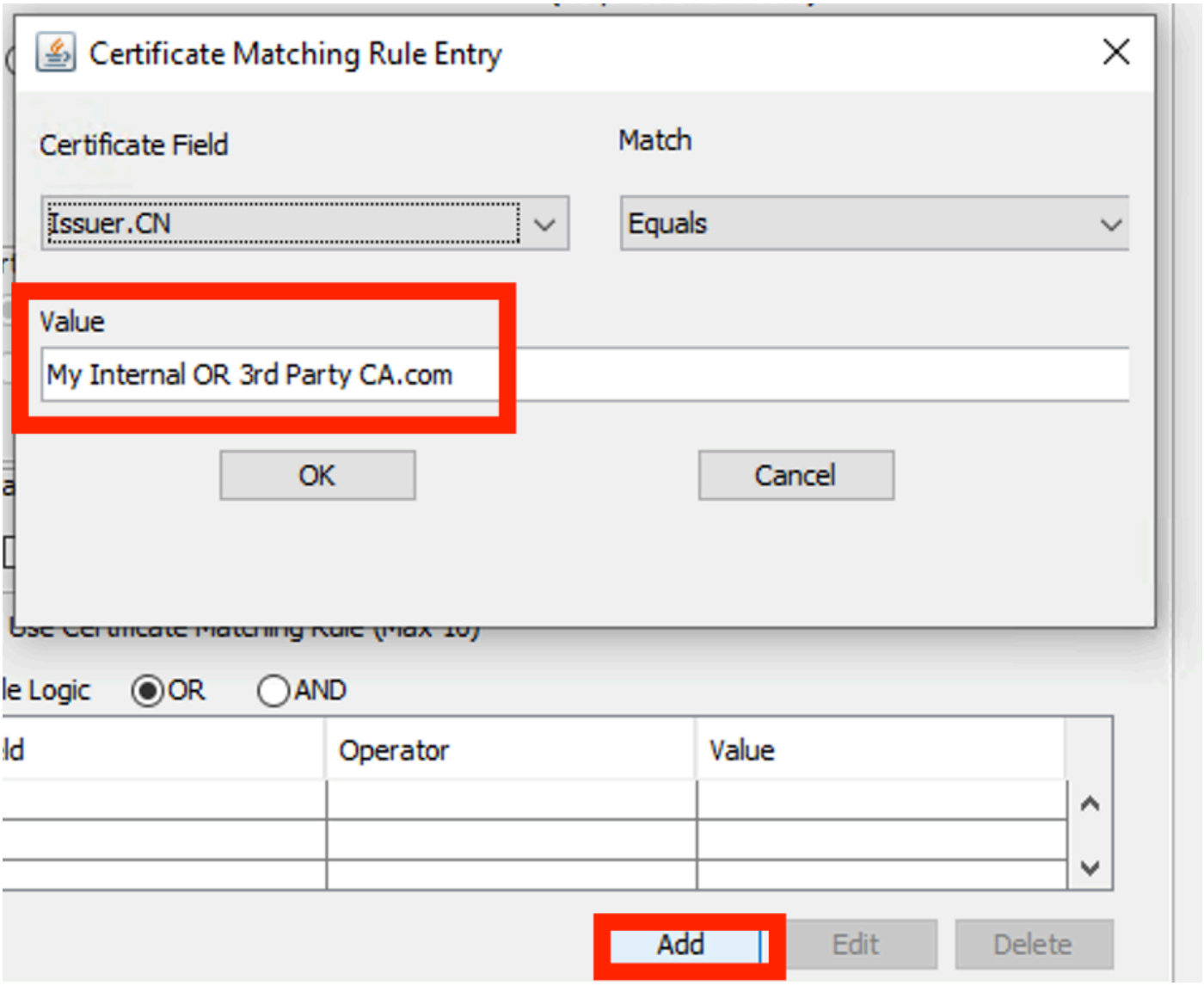
12, Pour la section User Credentials, ne modifiez pas les valeurs par défaut dans la première section.



Section User Auth Credentials

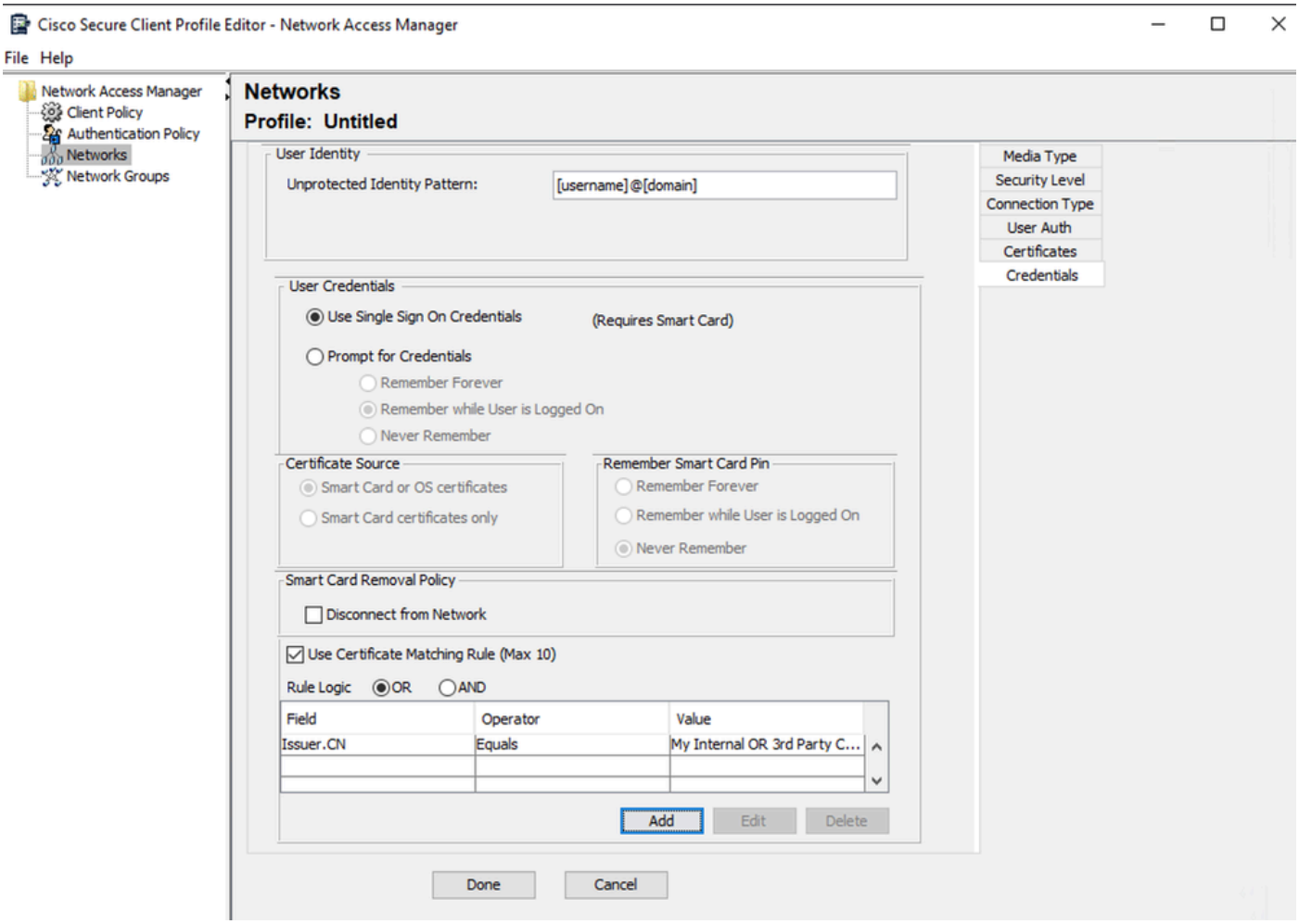
13. Il est important de configurer une règle qui correspond au certificat d'identité que l'utilisateur envoie pendant le processus TLS EAP. Pour ce faire, cochez la case en regard de Utiliser la règle de correspondance de certificat (10 max).

14. Cliquez sur Ajouter.



Fenêtre Règle de correspondance de certificat

15. Remplacez la valeur de la chaîne My Internal OR 3rd Party CA.com par le CN du certificat utilisateur.



Section User Auth Certificate Credentials

16. Cliquez sur Done pour terminer la configuration.

17. Sélectionnez Fichier > Enregistrer sous pour enregistrer le profil Secure Client Network Access Manager sous le nom configuration.xml.

18. Pour ajouter le Gestionnaire d'accès réseau du client sécurisé, utilisez le profil que vous venez de créer et remplacez le fichier configuration.xml dans le répertoire suivant par le nouveau :

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

---

Remarque : Le fichier doit être nommé configuration.xml, sinon il ne fonctionne pas.

Configurer ISR 1100 et ISE pour autoriser les authentifications en fonction du scénario 1 PEAP MSCHAPv2

1. Configuration du routeur ISR 1100

2. Cette section couvre la configuration de base que NAD doit avoir pour assurer les fonctions dot1x comme prévu.



Remarque : Pour les déploiements ISE multinoeuds, pointez vers n'importe quel noeud sur lequel le profil Noeud de serveur de stratégie est activé. Vous pouvez le vérifier en accédant à l'ISE dans l'onglet Administration > System > Deployment.

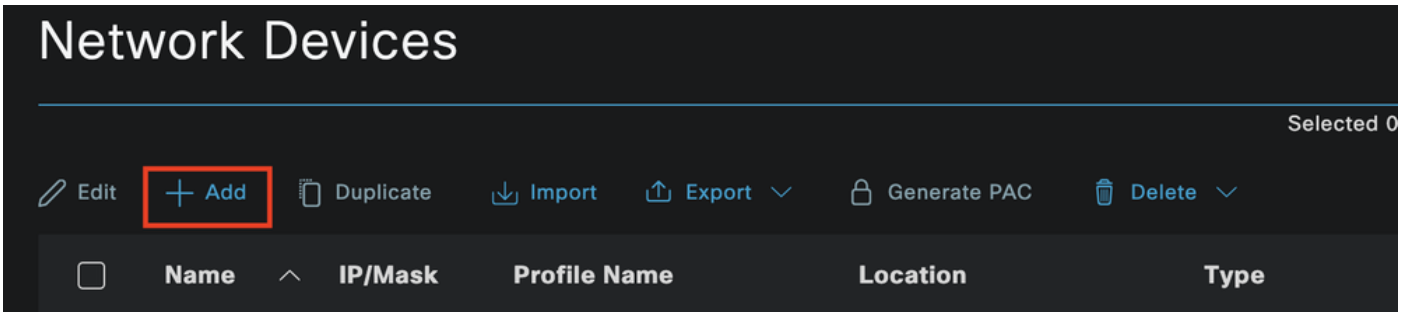
```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
 key <Your shared secret>
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

3. Configurez Identity Service Engine 3.2.

4. Configurez le périphérique réseau.

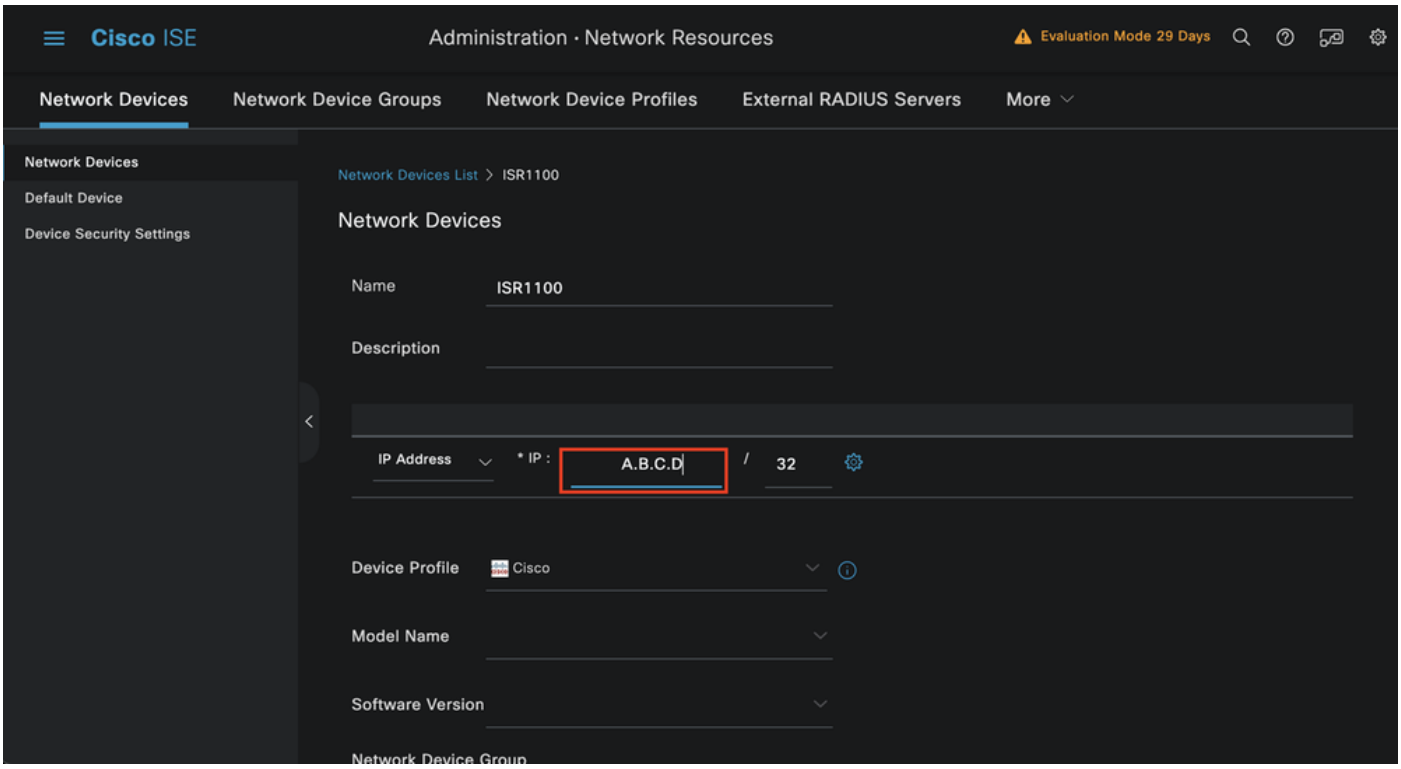
5. Ajoutez le NAD ISR à l'Administration ISE > Ressources réseau > Périphériques réseau.

6. Cliquez sur Ajouter.



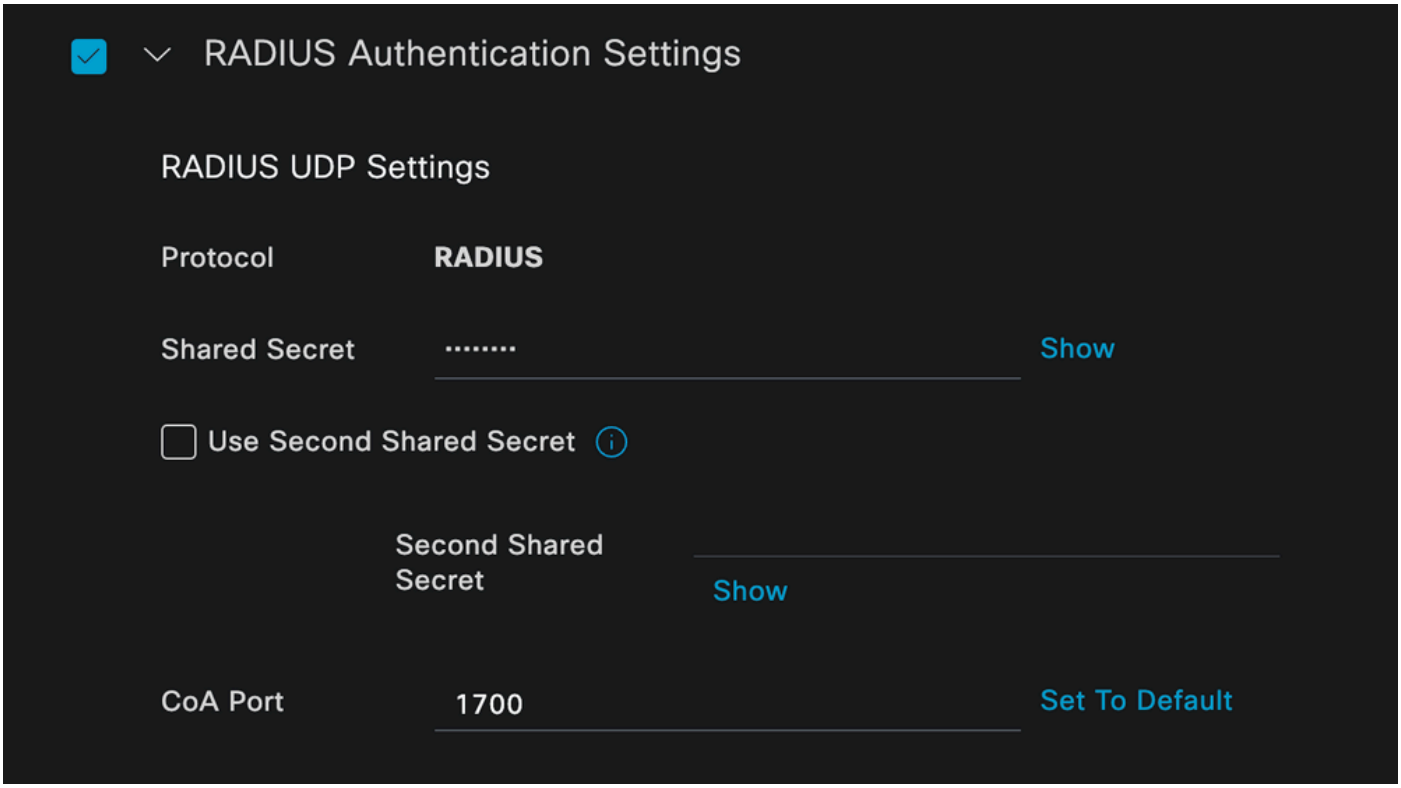
Section Network Device

7. Attribuez un nom au NAD que vous créez. Ajoutez l'adresse IP du périphérique réseau.



Création de périphériques réseau

8. Au bas de la même page, ajoutez le même secret partagé utilisé dans la configuration de votre périphérique réseau.



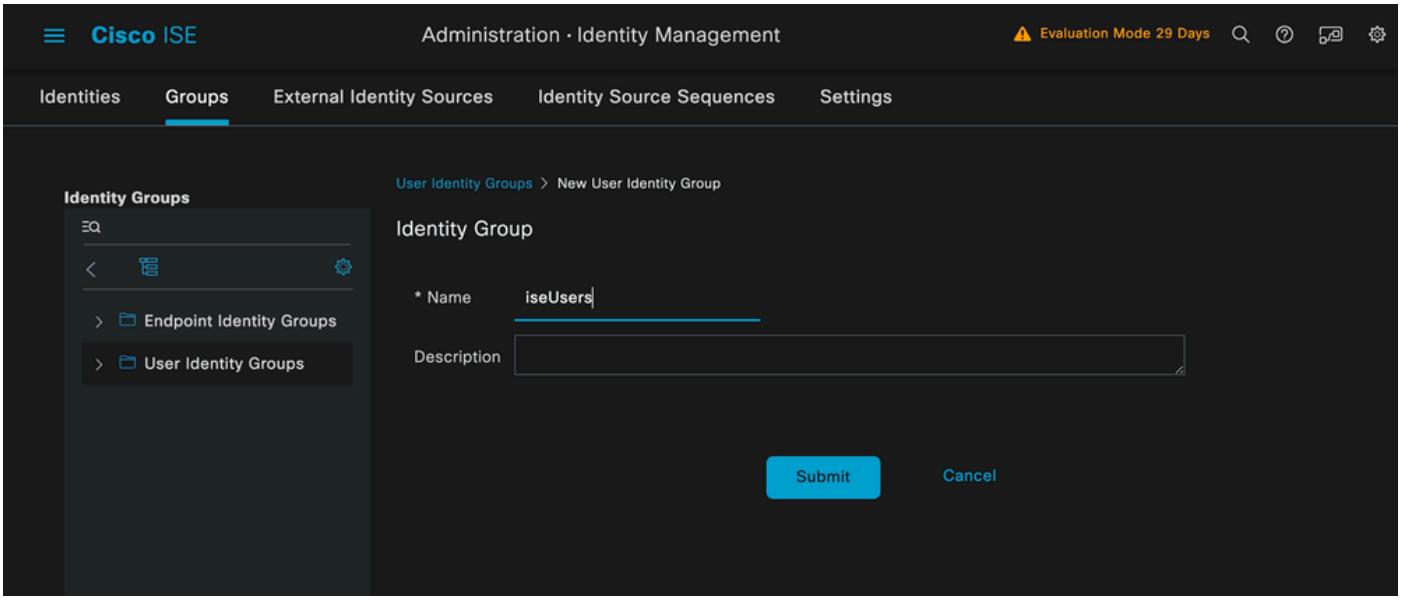
Paramètres du rayon du périphérique réseau

8. Enregistrez les modifications.

9. Configurez l'identité utilisée pour authentifier le point de terminaison.

10. L'authentification locale ISE est utilisée et l'authentification externe ISE n'est pas expliquée dans cet article.

11. Accédez à l'onglet Administration > Identity Management > Groups et créez le groupe dont fait partie votre utilisateur. Le groupe d'identité créé pour cet exemple est iseUsers.

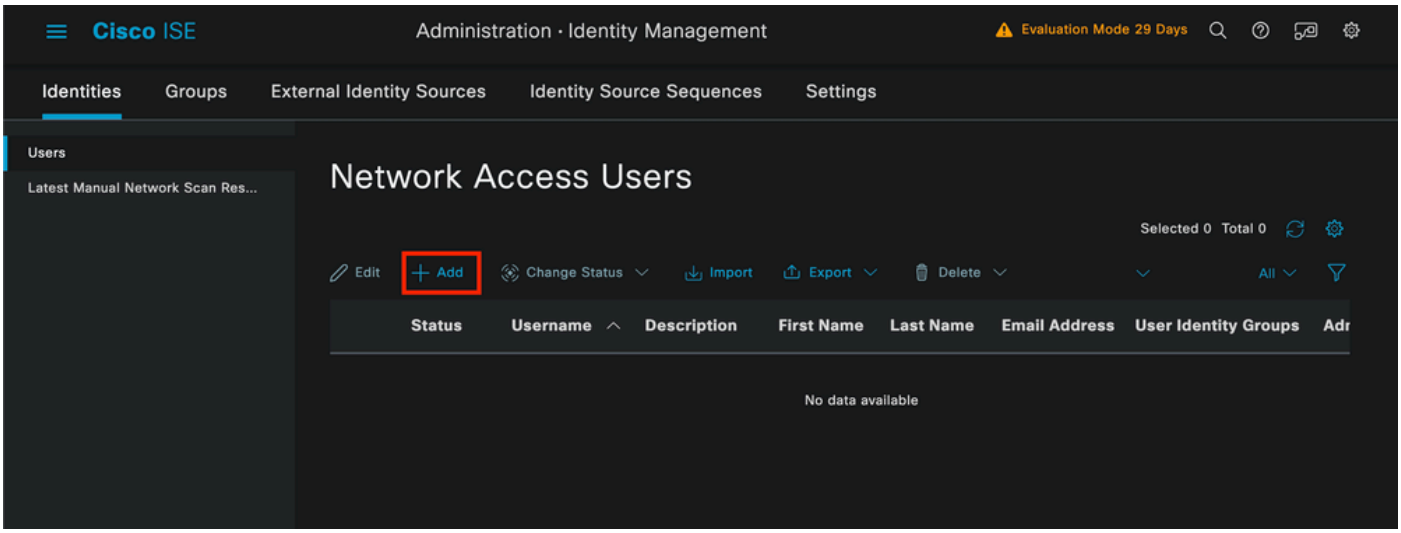


Création de groupe d'identités

12. Cliquez sur Soumettre.

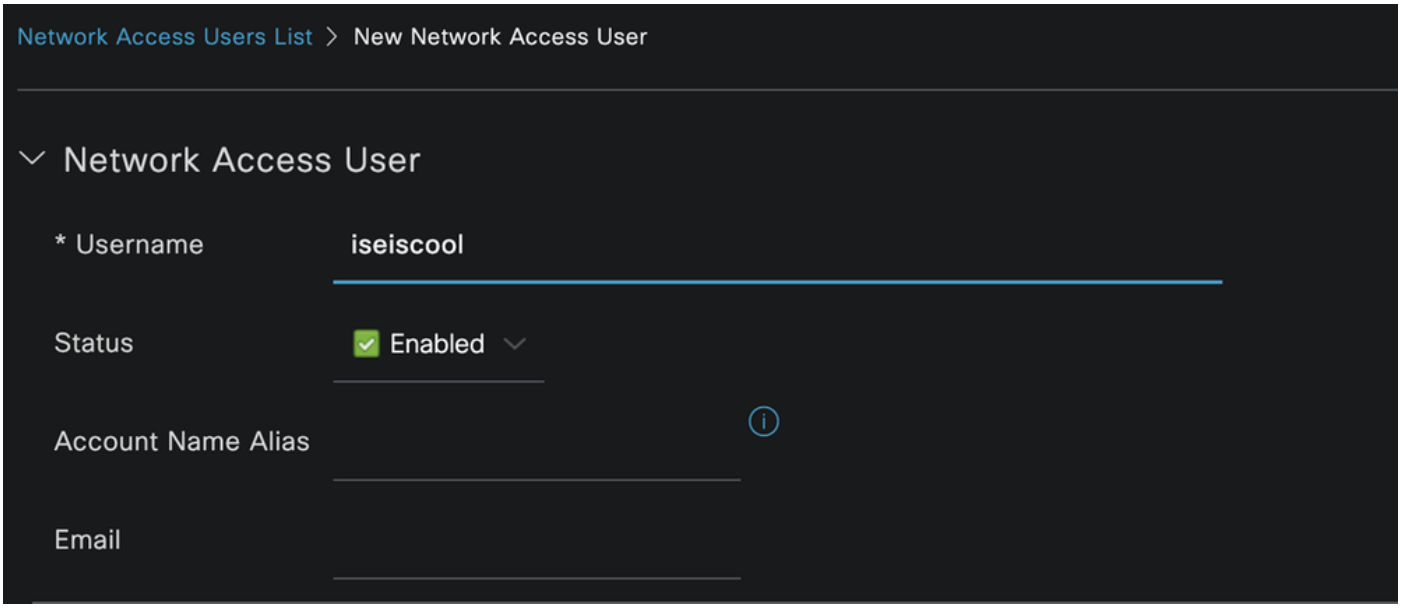
13. Accédez à l'onglet Administration > Gestion des identités > Identité.

14. Cliquez sur Ajouter.



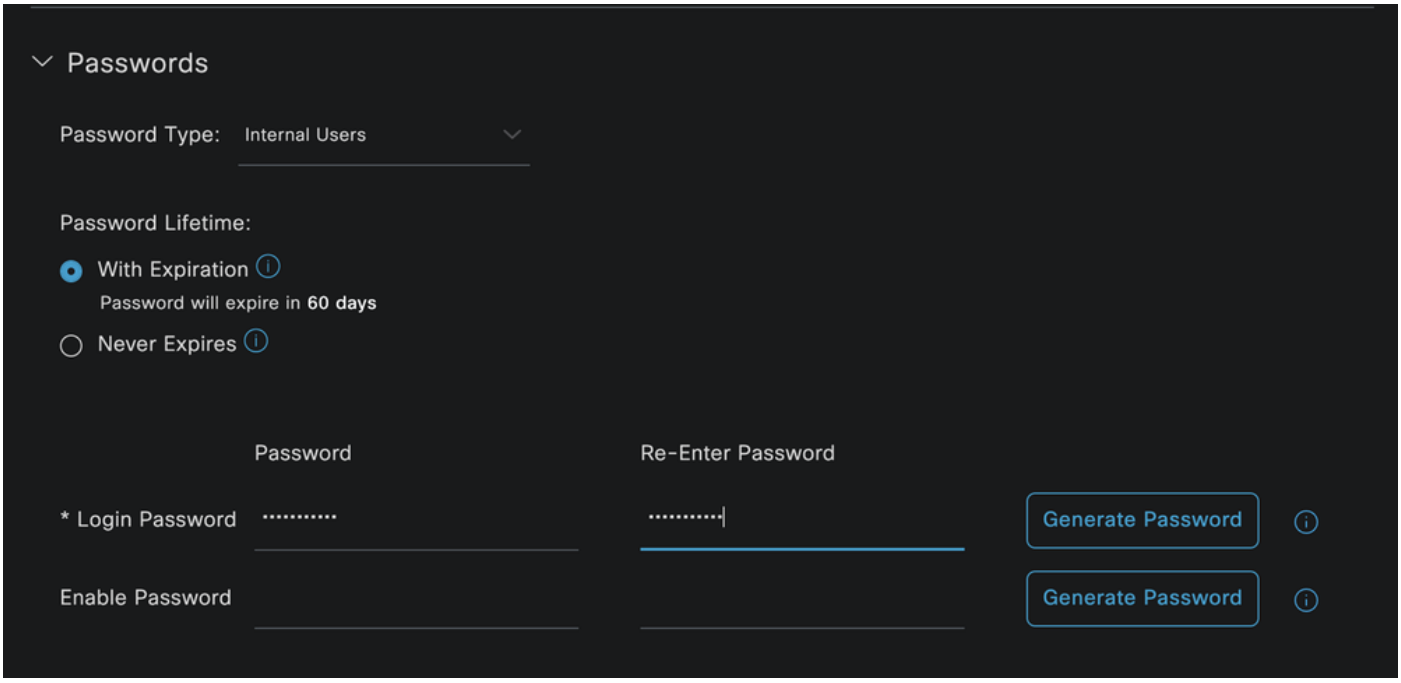
Section Utilisateurs d'accès réseau

15. Dans les champs obligatoires. commencez par le nom de l'utilisateur. Le nom d'utilisateur iseiscool est utilisé dans cet exemple.



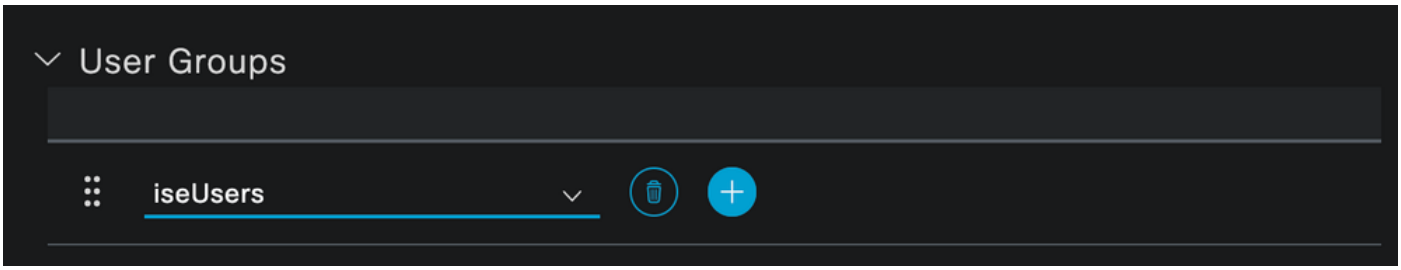
Création d'utilisateurs d'accès réseau

16. Attribuez un mot de passe à l'utilisateur. Dans cet exemple, VainillaISE97 est utilisé.



Section Mot de passe de création utilisateur

17. Affectez l'utilisateur au groupe iseUsers.



Attribution de groupe d'utilisateurs

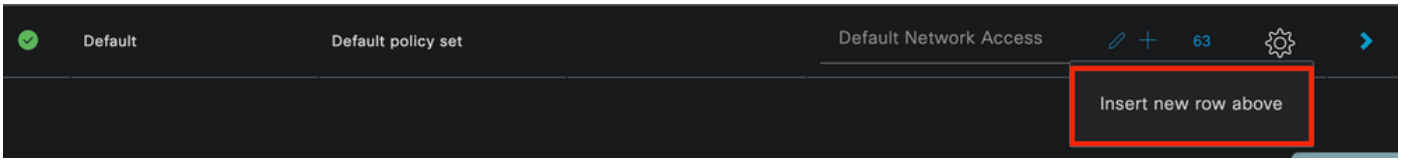
18. Configurez l'ensemble de stratégies.

19. Accédez à ISE Menu > Policy > Policy Sets.

20. Le jeu de stratégies par défaut peut être utilisé. Cependant, un réseau appelé câblé est créé pour cet exemple.

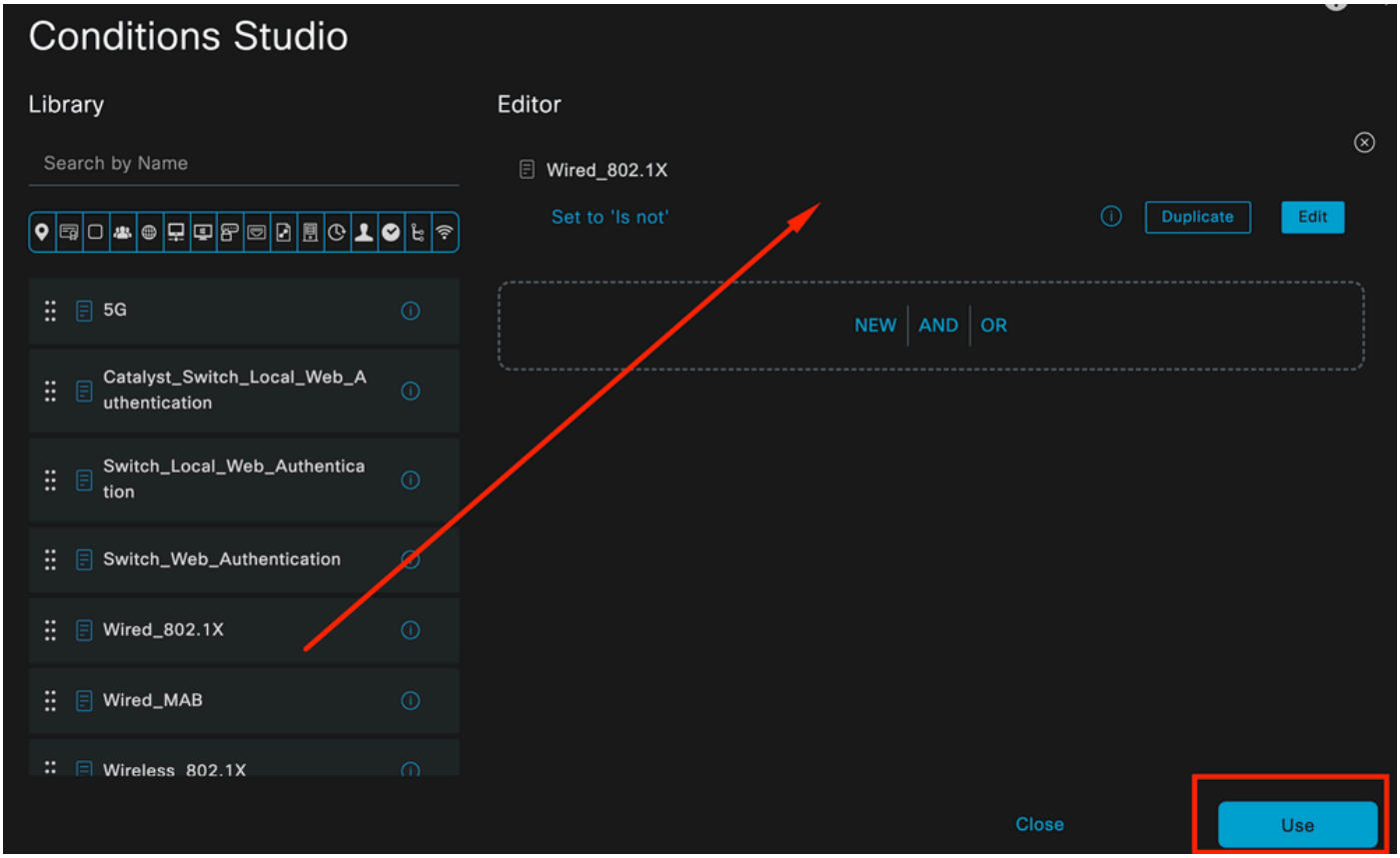
Remarque : La classification et la différenciation des ensembles de stratégies facilitent le dépannage,

Si l'icône d'ajout ou de plus "+" n'est pas visible, vous pouvez cliquer sur l'icône d'engrenage de n'importe quel jeu de stratégies, puis sélectionner Insérer une nouvelle ligne au-dessus.



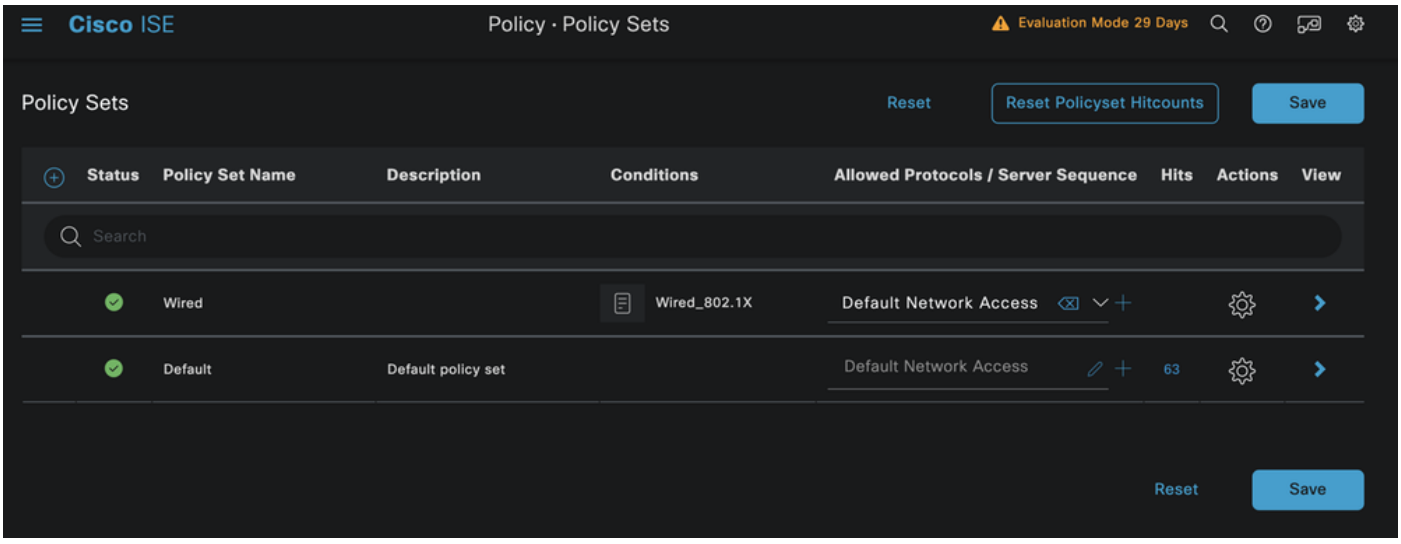
Options des icônes engrenage

21. La condition utilisée est Wired 8021x, faites-la glisser. puis cliquez sur Utiliser.



Studio de condition de stratégie d'authentification

22. Sélectionnez Accès réseau par défaut dans la section Protocoles autorisés.

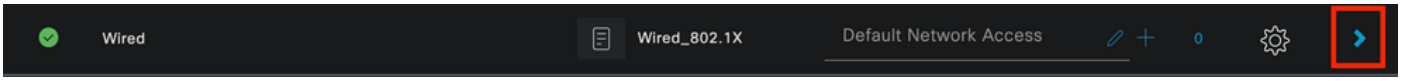


Vue générale Jeux de stratégies

23. Cliquez sur Enregistrer.

Configuration des stratégies d'authentification et d'autorisation

1. Cliquez sur l'icône >.



Ensemble de stratégies câblées

2. Développez la section Stratégie d'authentification.

3. Cliquez sur l'icône "+".



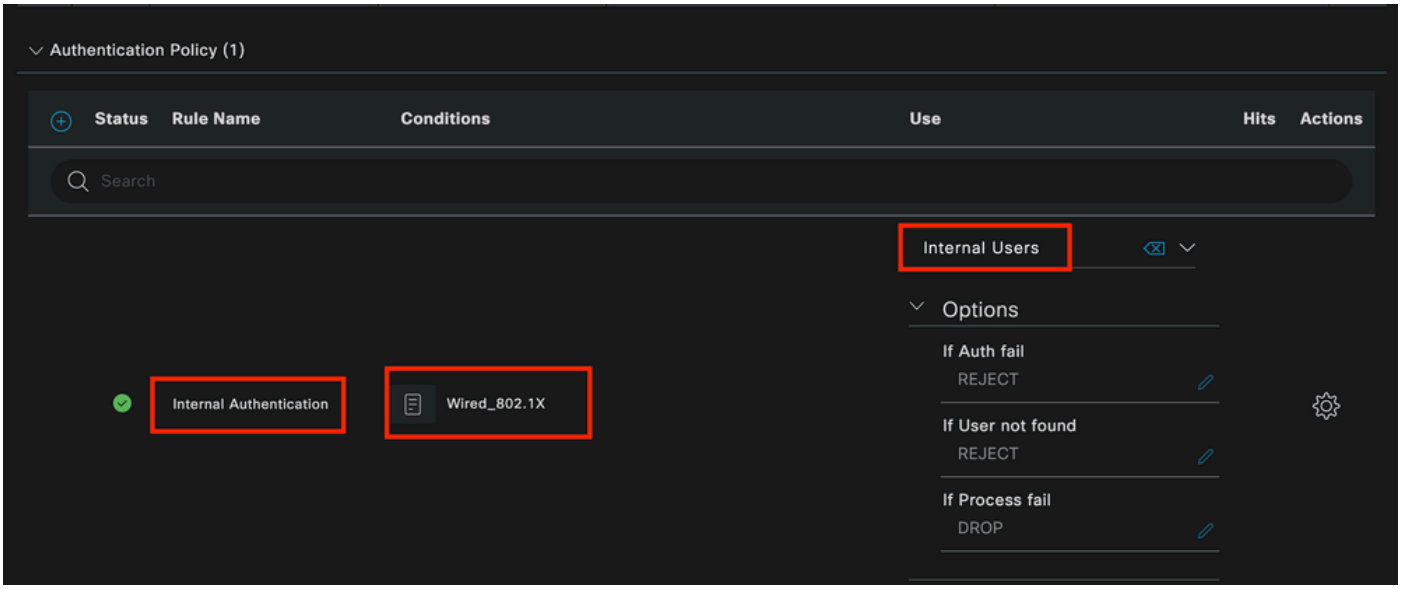
Stratégie d'authentification

4. Attribuez un nom à la stratégie d'authentification ; l'authentification interne est utilisée dans cet exemple.

5. Cliquez sur l'icône "+" dans la colonne des conditions pour cette nouvelle stratégie d'authentification.

6. La condition préconfigurée Wired Dot1x est utilisée.

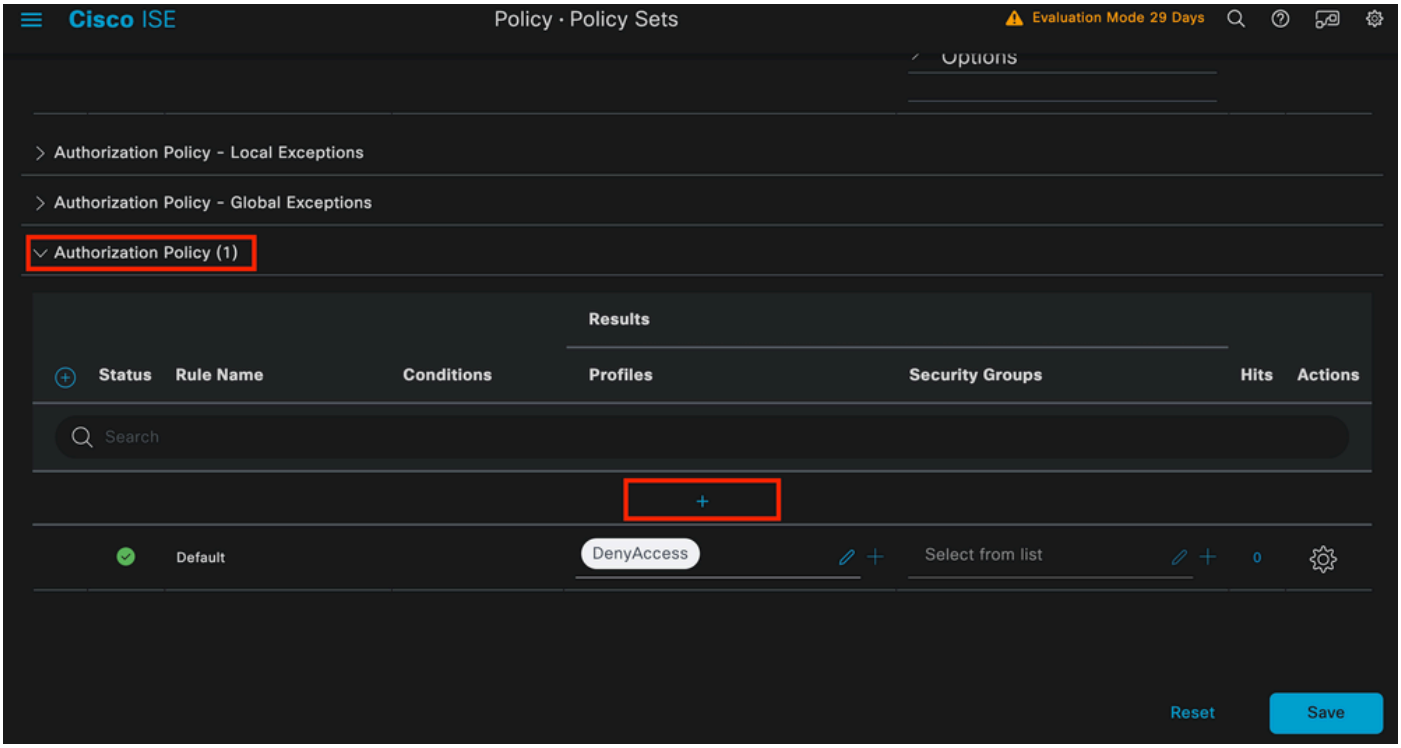
7. Dans la colonne Utiliser, sélectionnez Utilisateurs internes.



Stratégie d'authentification

Politique d'autorisation

1. La section Politique d'autorisation se trouve au bas de la page. Développez-le et cliquez sur l'icône +.



Politique d'autorisation

2. Attribuez un nom à la stratégie d'autorisation récemment créée. Dans cet exemple de configuration, le nom Internal ISE Users est utilisé.

3. Pour créer une condition pour cette stratégie d'autorisation, cliquez sur l'icône "+" dans la

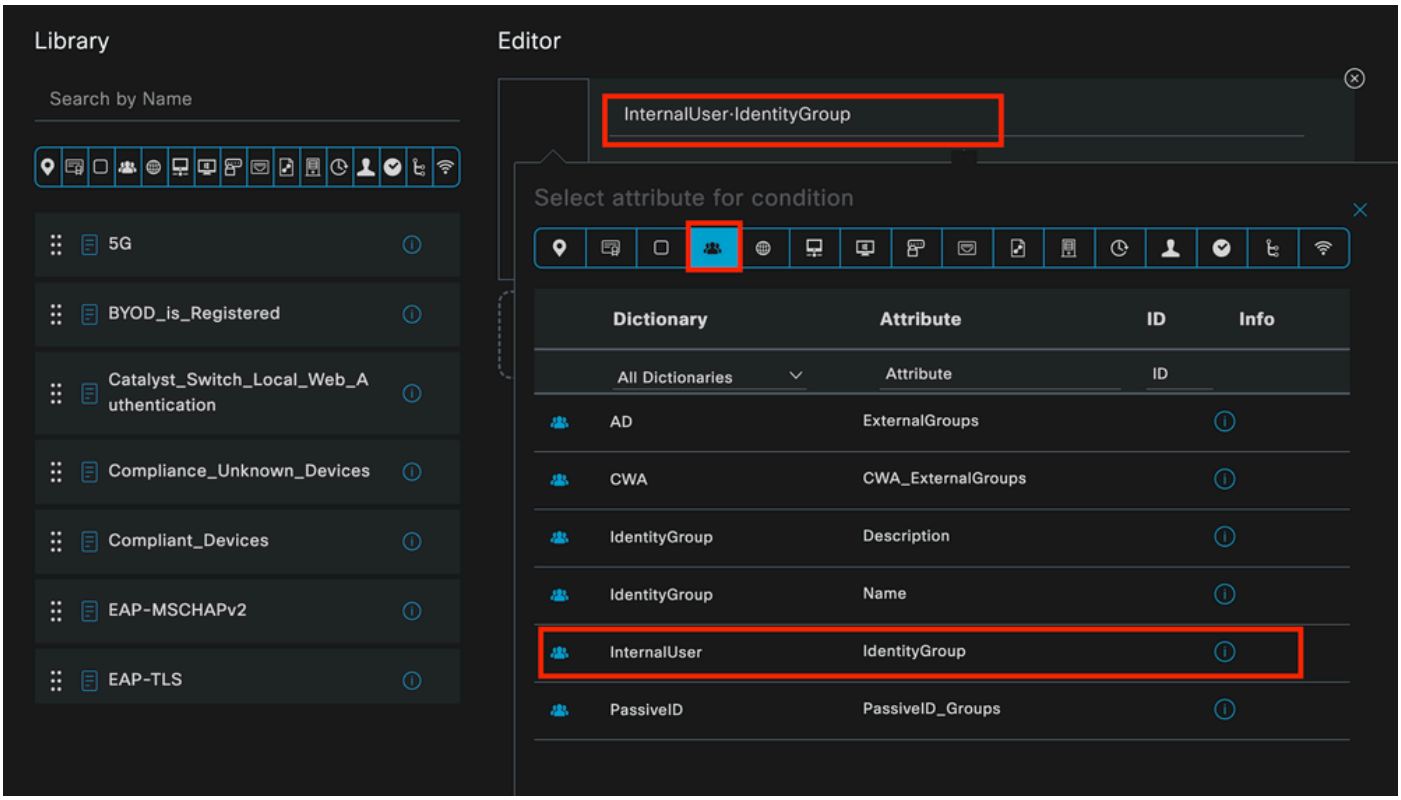
colonne Conditions.

4. Le groupe IseUsers est utilisé.

5. Cliquez sur la section Attribut.

6. Sélectionnez l'icône IdentityGroup.

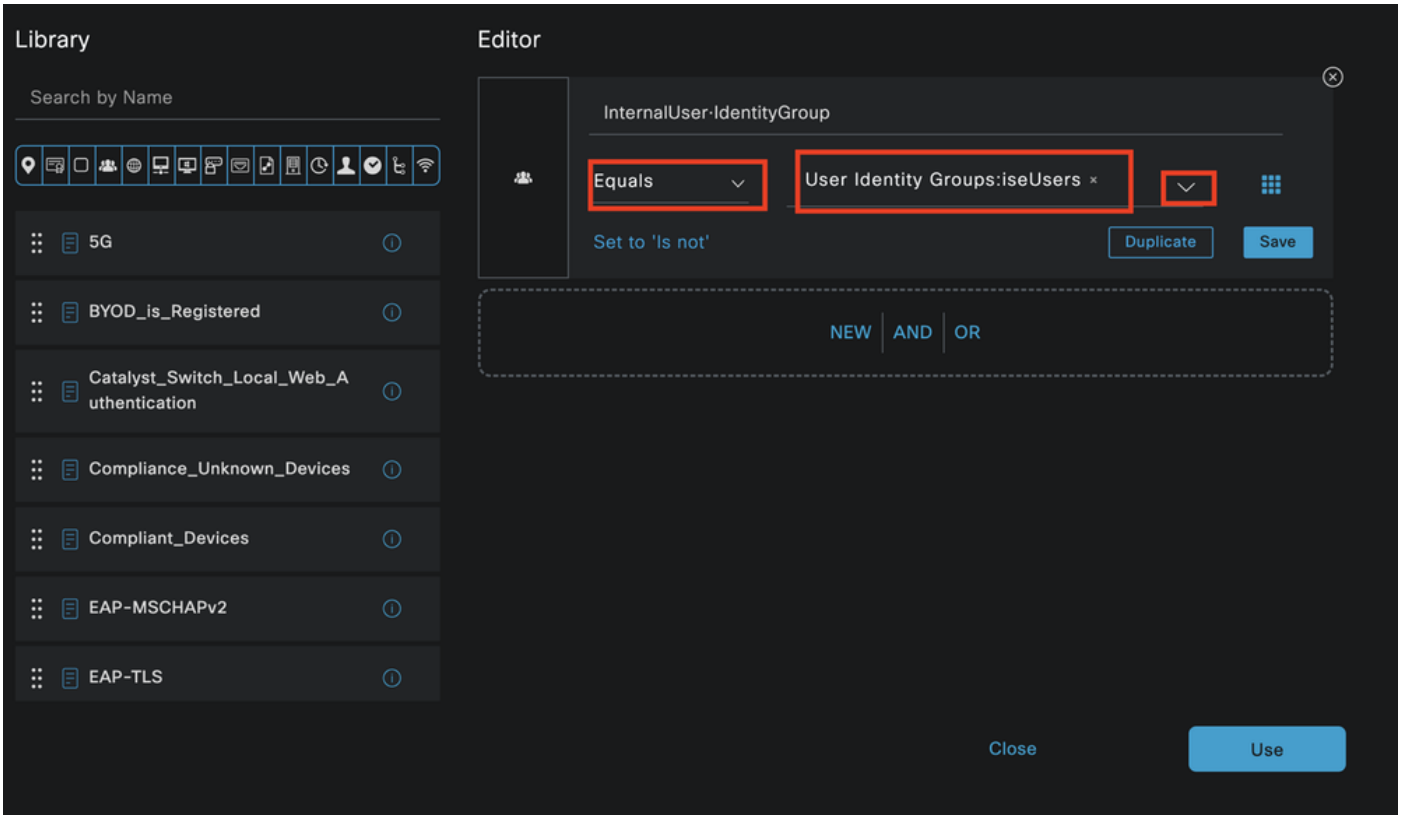
7. Dans le dictionnaire, sélectionnez le dictionnaire InternalUser fourni avec l'attribut IdentityGroup.



Création de condition

8. Dans le menu déroulant, sélectionnez l'opérateur Égale.

9. Dans le menu déroulant User Identity Groups, sélectionnez le groupe IseUsers.



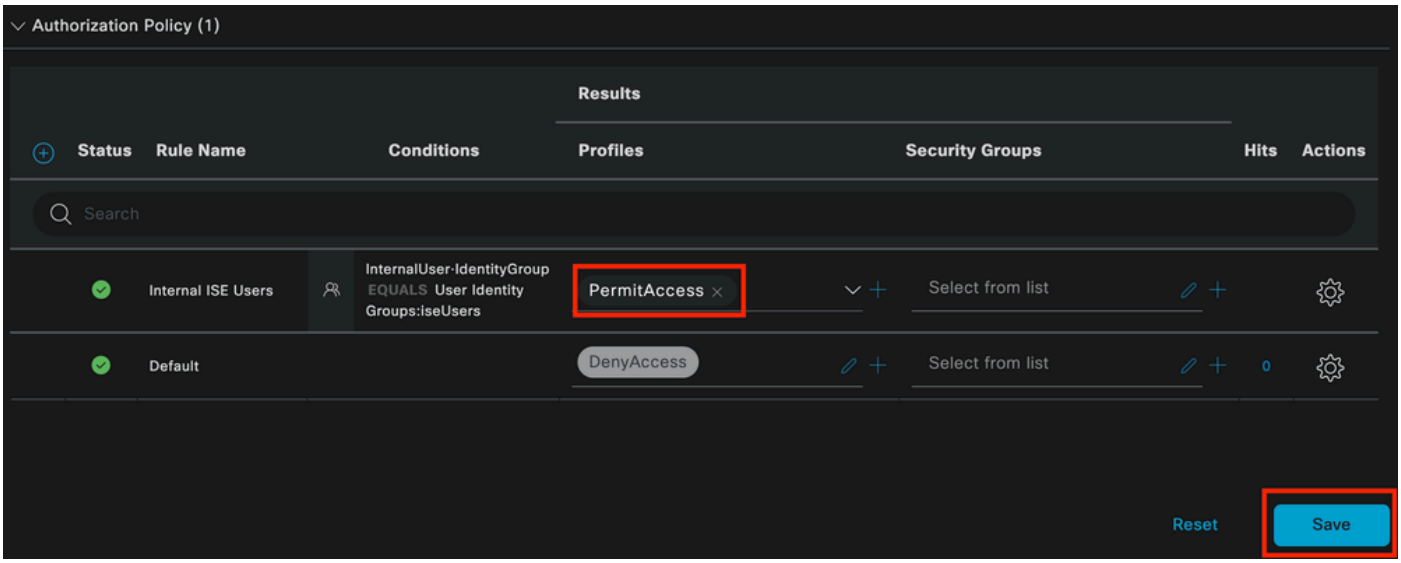
Création de condition

10. Cliquez sur Utiliser.

11. Ajoutez le profil d'autorisation de résultat.

12. Le profil préconfiguré Autoriser l'accès est utilisé.

Remarque : Les authentifications arrivant à l'ISE et atteignant le jeu de stratégies Wired Dot1x ne font pas partie des utilisateurs ISEUsers du groupe d'identité des utilisateurs. Appuyez sur la stratégie d'autorisation par défaut, ce qui entraîne DenyAccess.



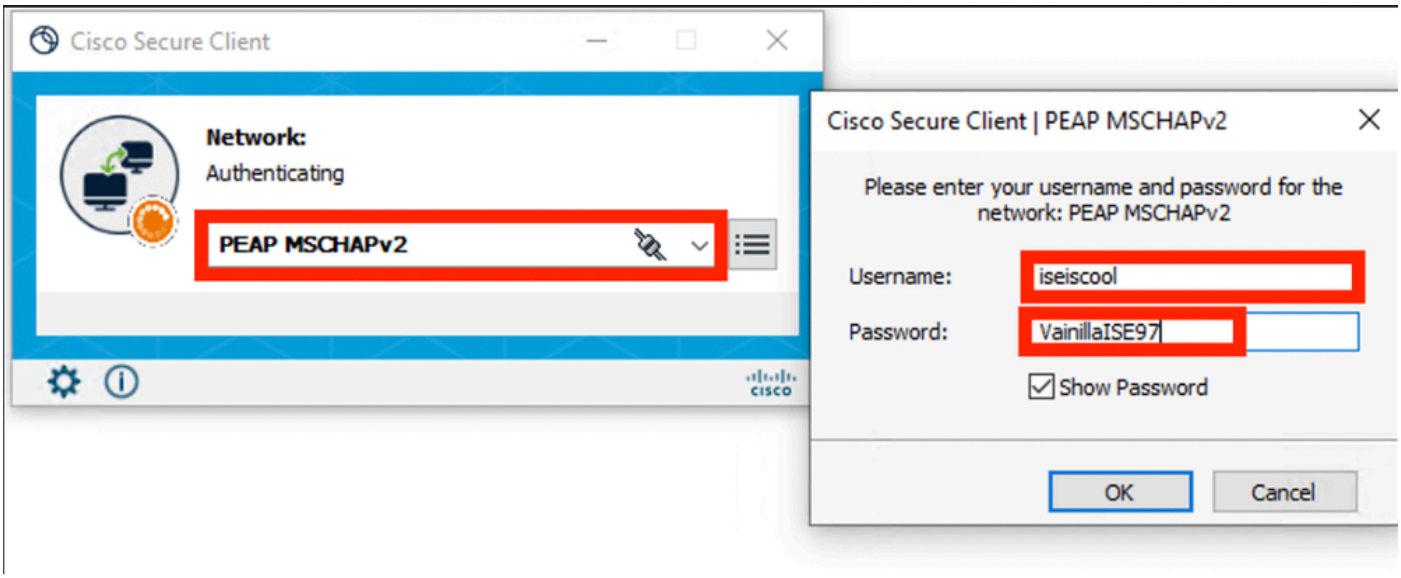
Politique d'autorisation

13. Cliquez sur Enregistrer.

Vérifier

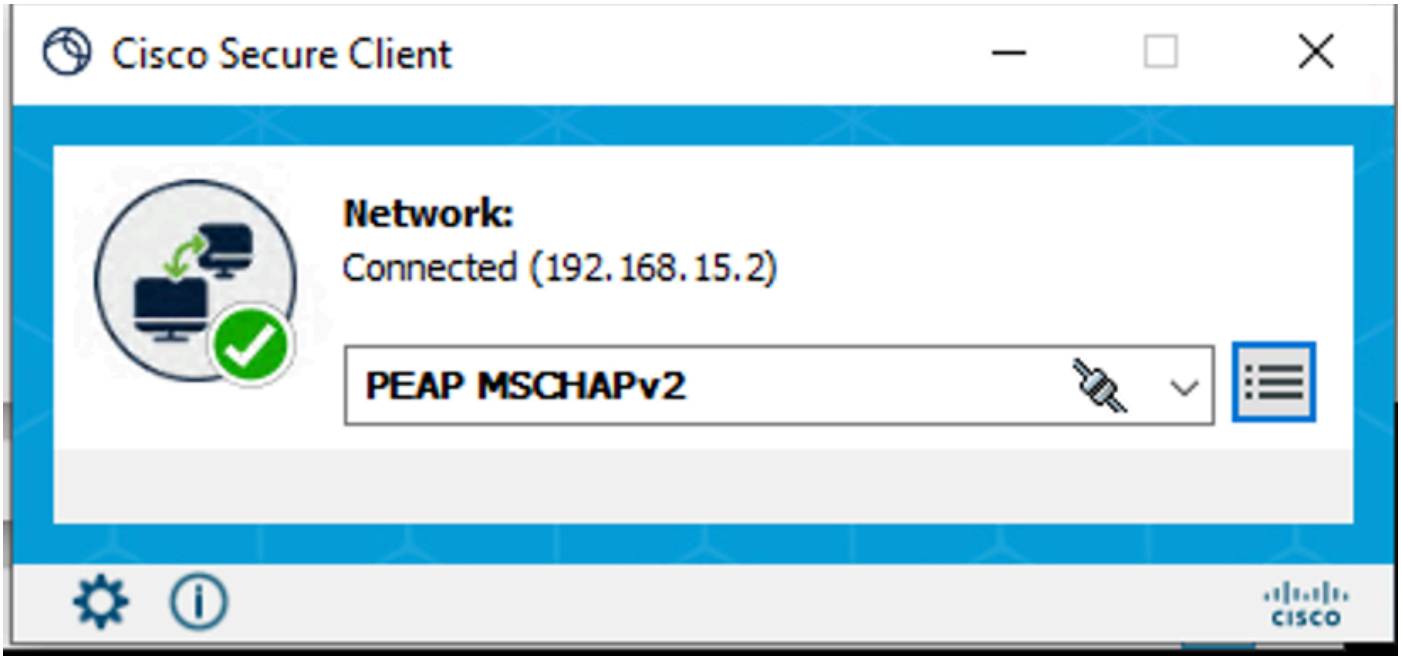
1. Une fois la configuration terminée, Secure Client demande les informations d'identification et spécifie l'utilisation du profil PEAP MSCHAPv2.

2. Les informations d'identification précédemment créées sont saisies.



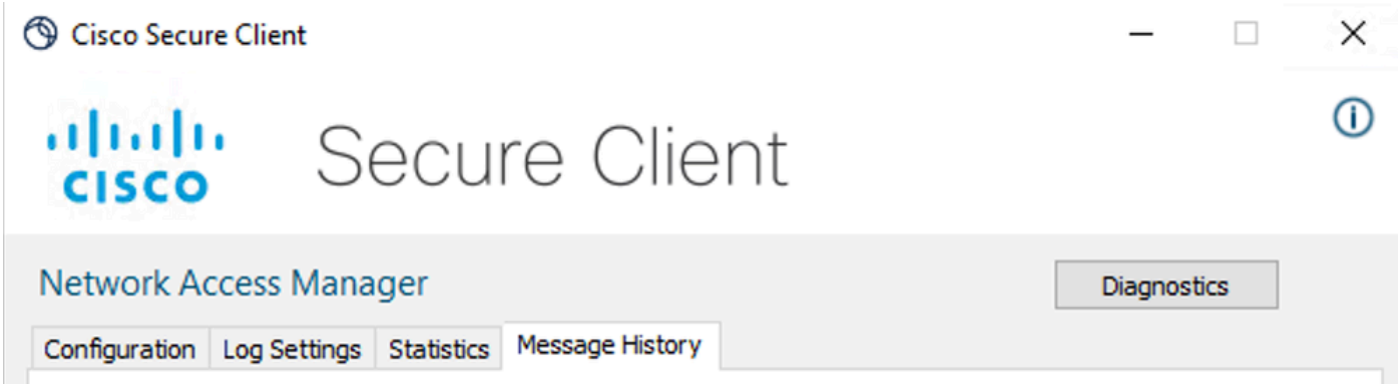
NAM du client sécurisé

3. Si le point d'extrémité s'authentifie correctement, NAM indique qu'il est connecté.

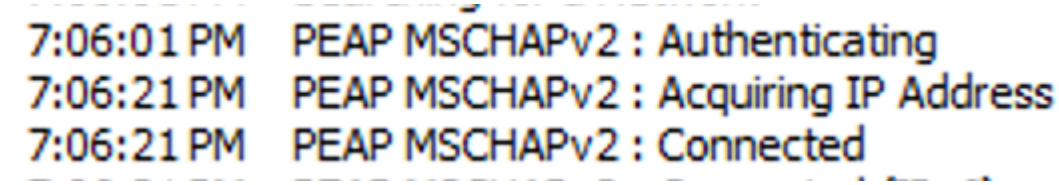


NAM du client sécurisé

4. En cliquant sur l'icône d'informations et en naviguant jusqu'à la section Historique des messages, les détails de chaque étape de NAM terminée s'affichent.



Historique des messages du client sécurisé



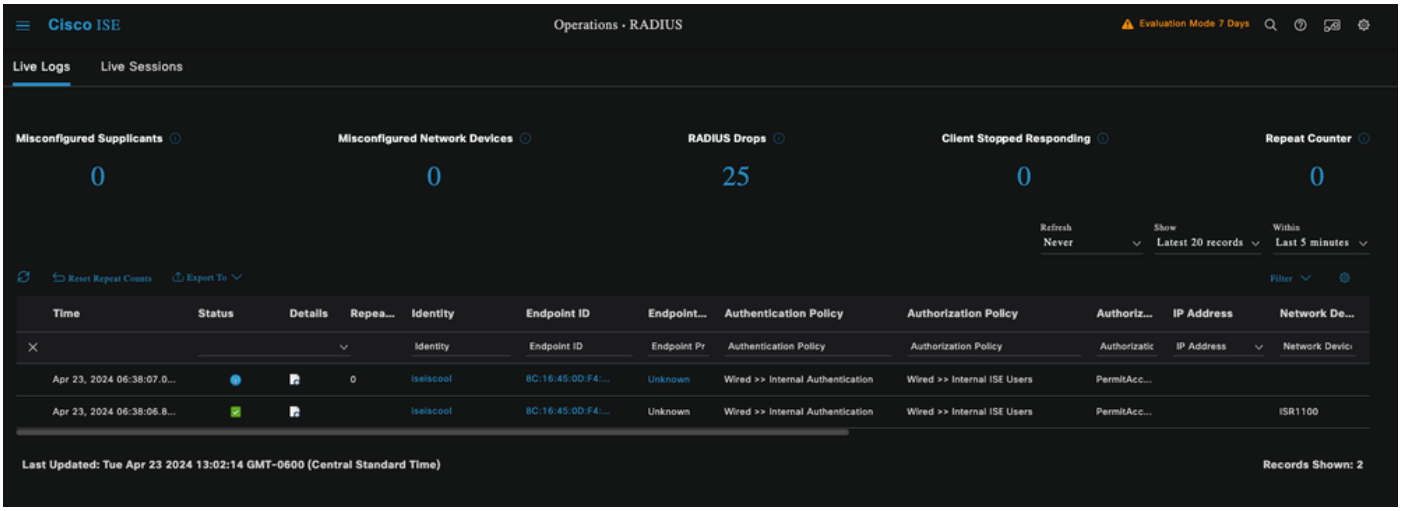
Historique des messages du client sécurisé

5. Dans ISE, accédez à Operations > Radius LiveLogs pour afficher les détails de l'authentification. Comme le montre l'image suivante, le nom d'utilisateur utilisé s'affiche.

D'autres détails sont disponibles tels que :

- Horodatage

- Adresse MAC :
- Jeu de stratégies utilisé
- Stratégie d'authentification
- Politique d'autorisation
- Autres informations pertinentes



Journaux en direct ISE RADIUS

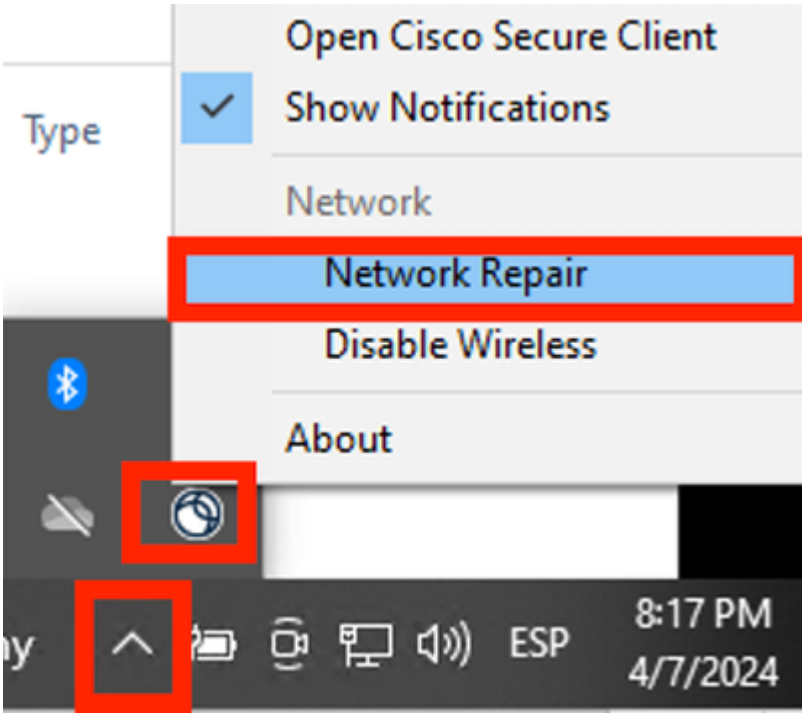
6. Dans cette vue, il affiche toutes les stratégies correctes sont affichées, et le résultat est un état d'authentification réussie. Ceci conclut que la configuration est correcte.

Dépannage

Problème 1 : Profil NAM non utilisé par le client sécurisé

1. Si le nouveau profil a été créé dans l'Éditeur de profil n'est pas utilisé par NAM, utilisez l'option Réparation du réseau du client sécurisé.

2. Vous pouvez trouver cette option en naviguant vers la barre Windows > Cliquer sur l'icône circumflex > Cliquez avec le bouton droit sur l'icône Secure Client > Cliquez sur Réparation du réseau.



Section Réparation du réseau

Problème 2 : Les journaux doivent être collectés pour une analyse plus approfondie

1. Activer la journalisation étendue NAM

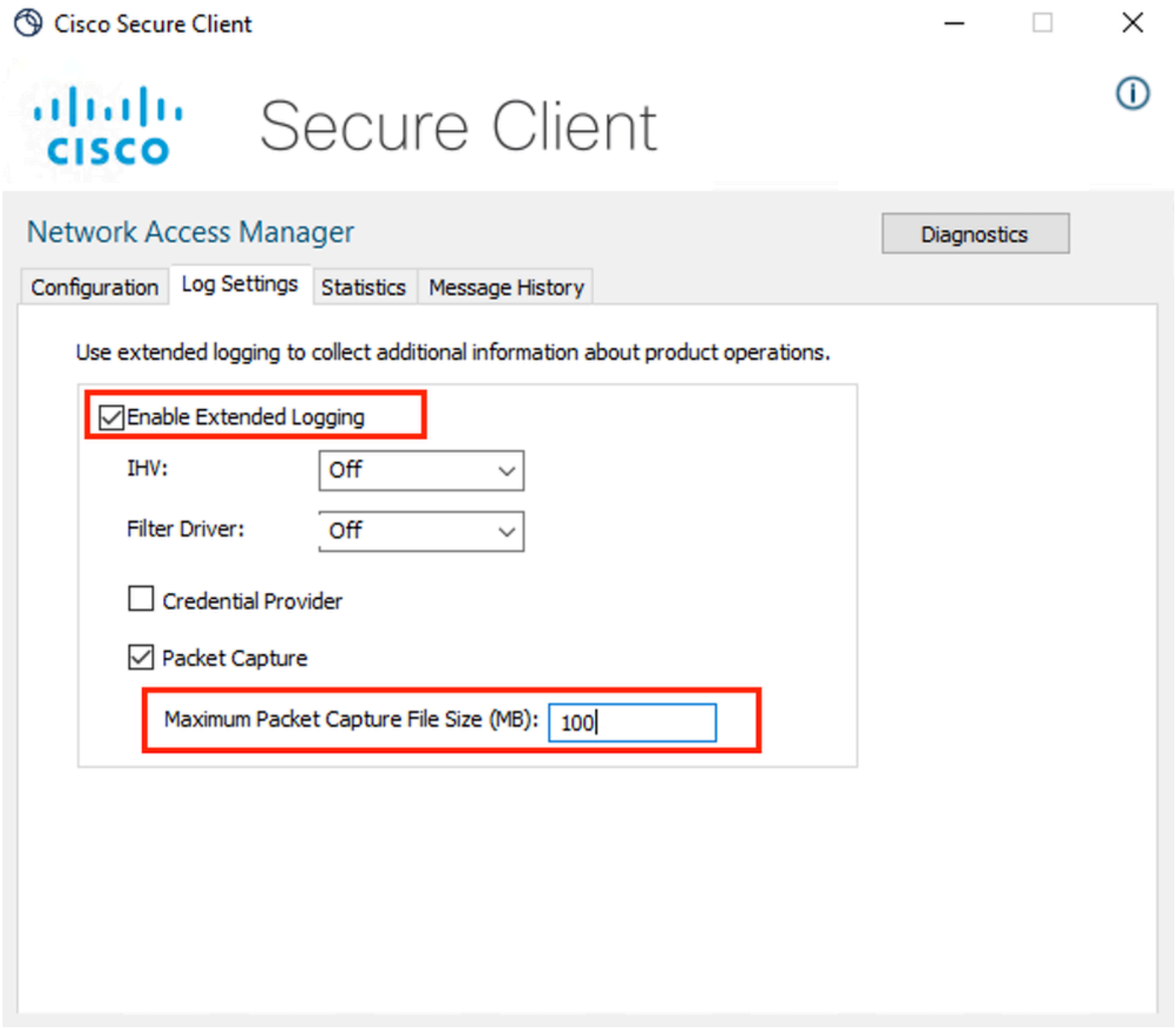
2. Ouvrez NAM et cliquez sur l'icône d'engrenage.



Interface NAM

3. Accédez à l'onglet Paramètres du journal. Cochez la case Enable Extended Logging.

4. Définissez la taille du fichier de capture de paquets sur 100 Mo.



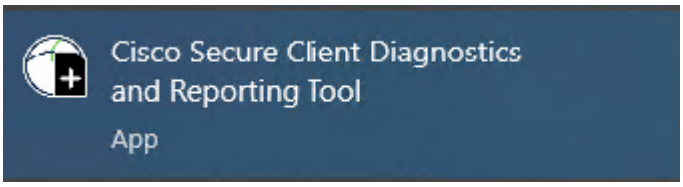
Paramètres du journal NAM du client sécurisé

Reproduisez le problème

5. Une fois la journalisation étendue activée, reproduisez le problème plusieurs fois pour vous assurer que les journaux sont générés et que le trafic est capturé.

Collecter l'offre groupée Secure Client DART

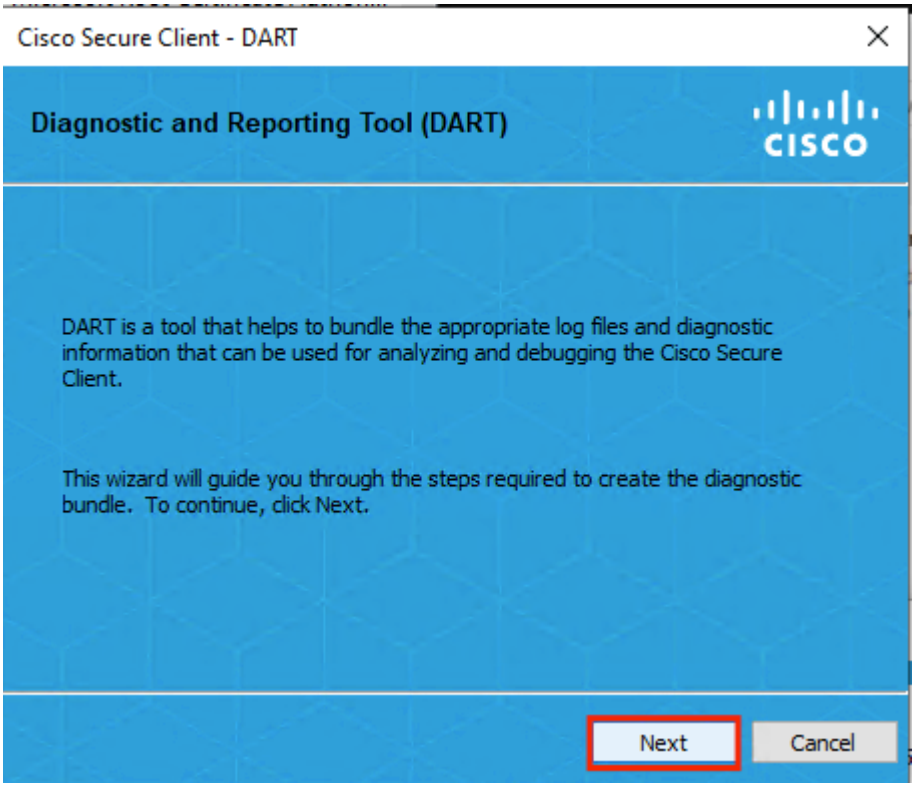
6. Dans Windows, accédez à la barre de recherche et tapez : Outil de diagnostic et de création de rapports Cisco Secure Client.



Module DART

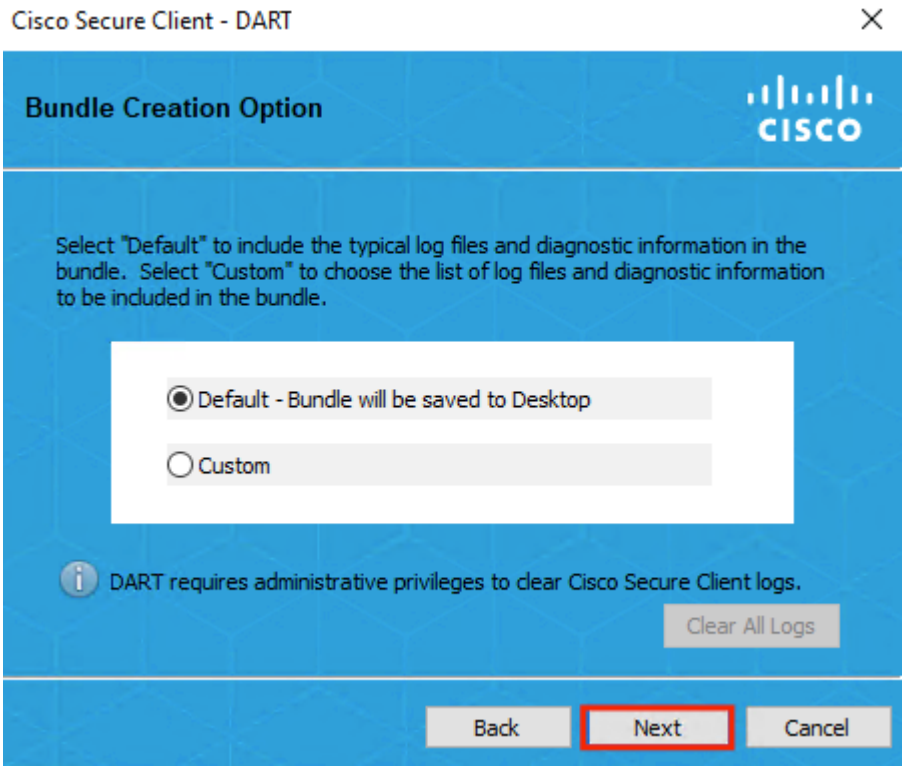
7. Au cours du processus d'installation, vous avez également installé ce module. Il s'agit d'un outil qui facilite les processus de dépannage en collectant des journaux et des informations de session dot1x pertinentes.

8. Cliquez sur Next dans la première fenêtre.



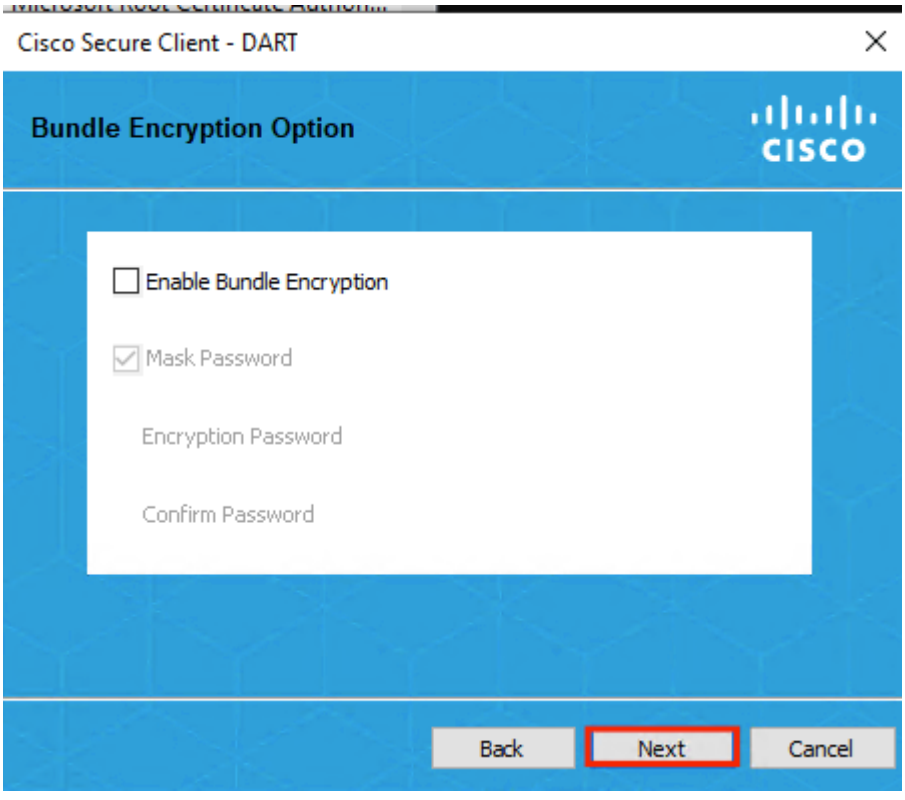
Module DART

9. Cliquez sur Next, ceci permet à l'ensemble de journal d'être enregistré sur le bureau.



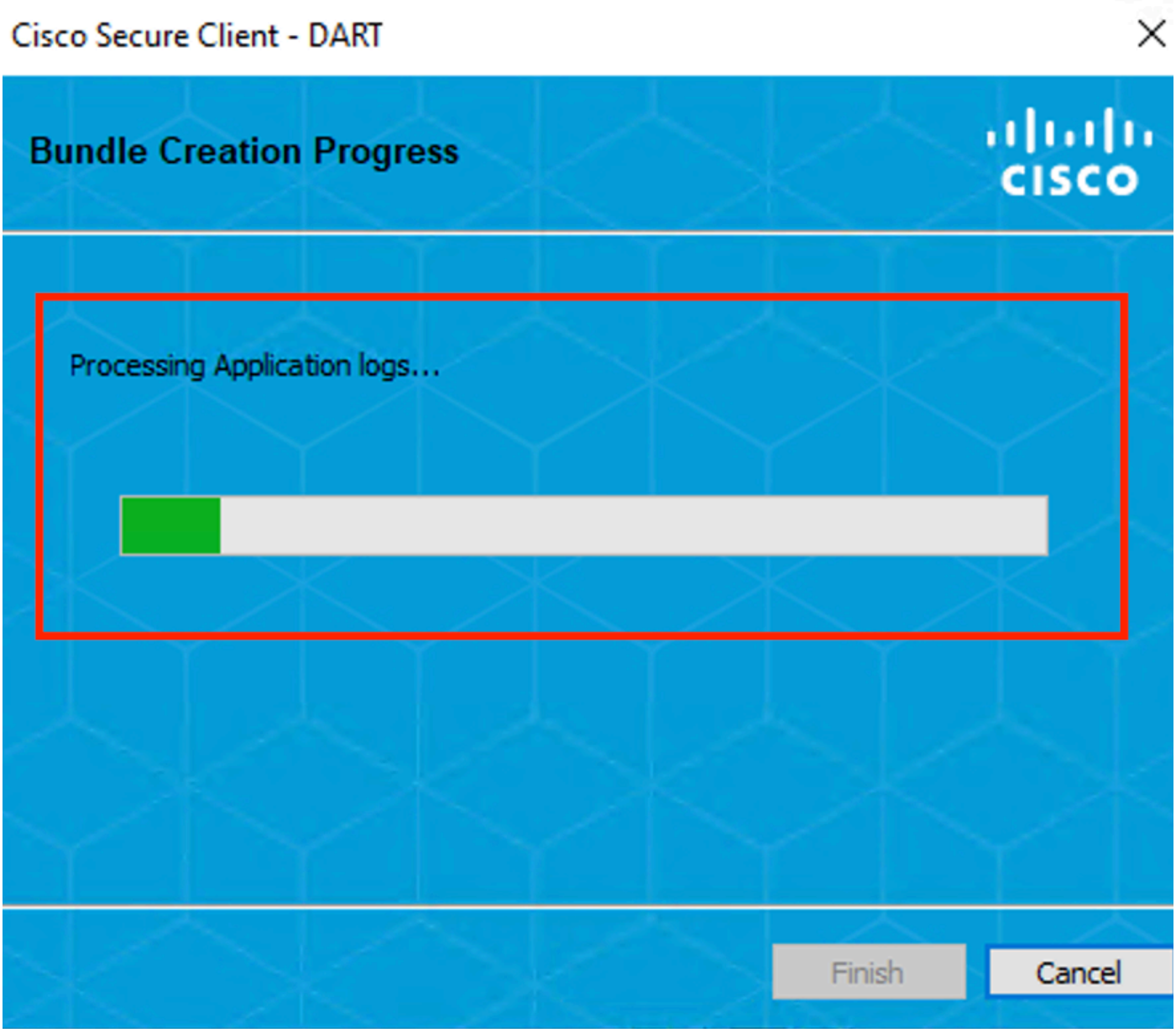
Module DART

10. Si nécessaire, cochez la case Enable Bundle Encryption.



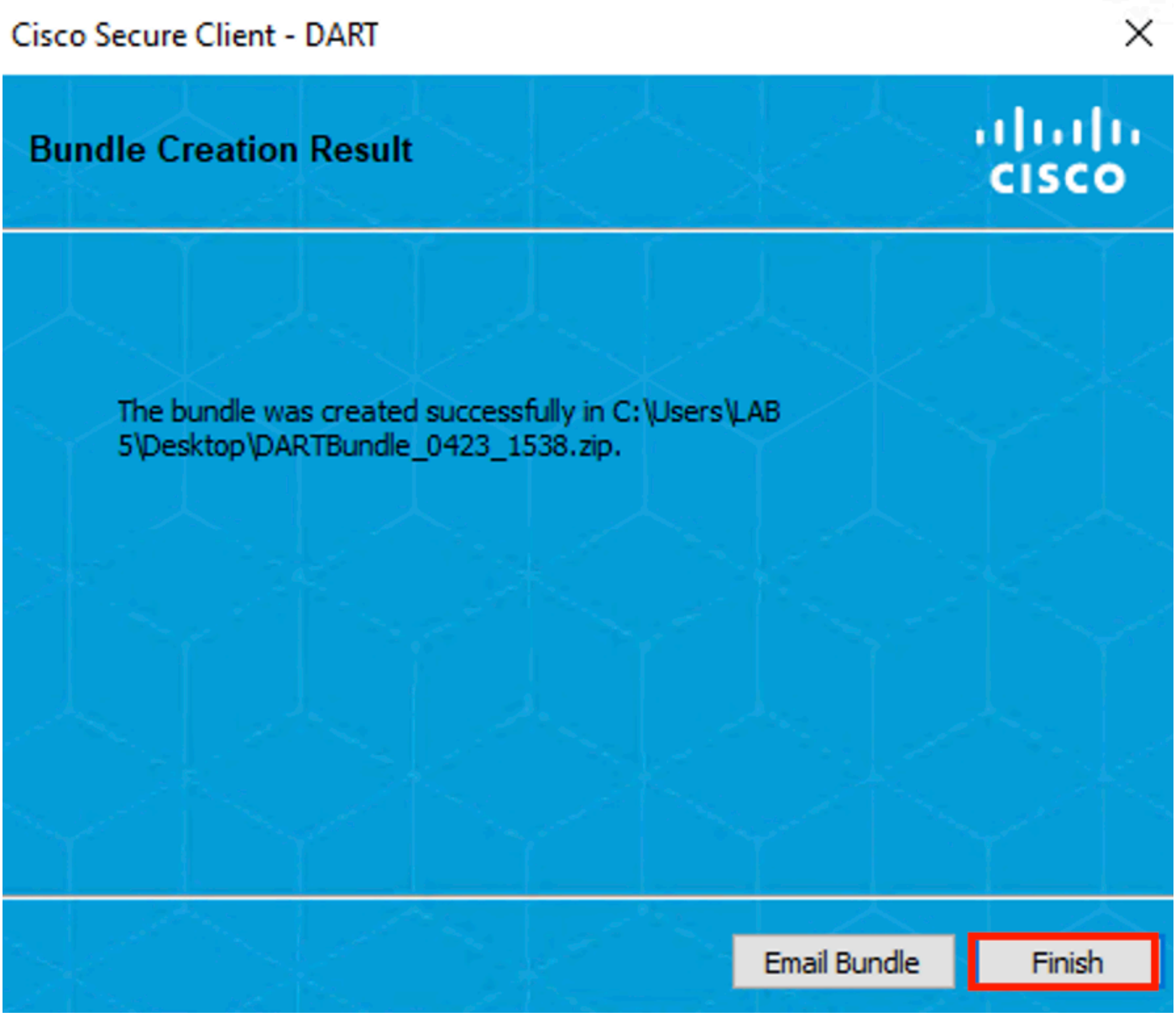
Module DART

11. La collection de journaux DART démarre.



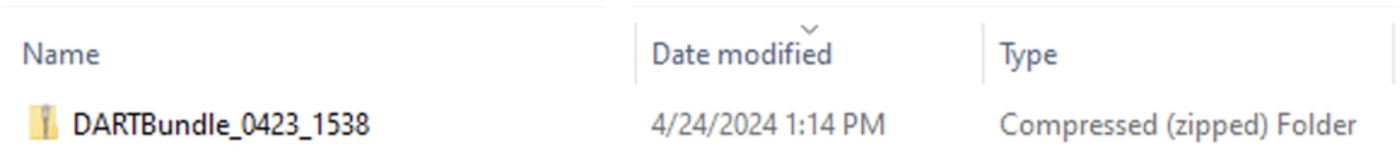
DART Log Collection

12. Cela peut prendre environ 10 minutes jusqu'à la fin du processus.



Résultat de la création du bundle DART

13. Le fichier de résultats DART se trouve dans le répertoire du bureau.



Fichier de résultats DART

Informations connexes

- Assistance technique de Cisco et téléchargements

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.