

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](#)

[Configurer](#)

[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 : configuration du demandeur NAM du client sécurisé pour l'authentification des utilisateurs PEAP \(MS-CHAPv2\)](#)
- [5. Scénario 2 : configuration du demandeur NAM du client sécurisé pour l'authentification simultanée des utilisateurs et des machines EAP-FAST](#)
- [6. Scénario 3 : configuration du demandeur NAM du client sécurisé pour l'authentification du certificat utilisateur EAP TLS](#)
- [7. Configurez ISR 1100 et ISE pour autoriser les authentifications en fonction du scénario 1 PEAP MSCHAPv2](#)

[Vérifier](#)

[Dépannage](#)

[Problème : le profil NAM n'est pas utilisé par le client sécurisé.](#)

[Problème 2 : les journaux doivent être collectés pour une analyse plus approfondie.](#)

- [1. Activer la journalisation étendue NAM](#)
- [2. Reproduisez la question.](#)
- [3. Collectez 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 de ce qu'est 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
- Logiciel Cisco IOS® XE C117, 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 un ordinateur d'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.

À propos de 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 pour être à résidence unique, ce qui permet d'établir 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 nécessaires ; le demandeur qui peut effectuer dot1x, l'authentificateur également connu sous le nom de NAS/NAD qui sert de proxy encapsulant le trafic dot1x à l'intérieur de RADIUS, et le serveur d'authentification.

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

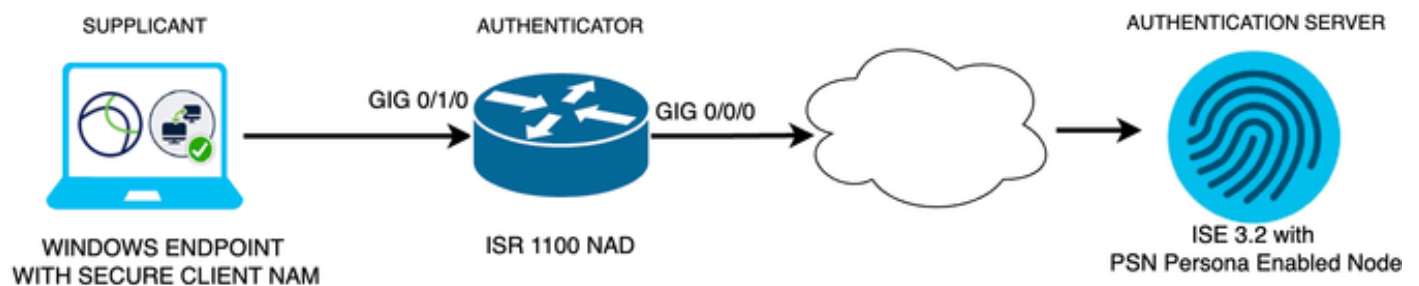


Diagramme du réseau

Configurations

1. Téléchargez et installez Secure Client NAM (Network Access Manager).
2. Téléchargez et installez l'éditeur de profil NAM Secure Client.
3. Configurations générales par défaut
4. Scénario 1 : configuration du 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 : configuration du demandeur NAM du client sécurisé pour EAP-TLS
7. Scénario 3, partie 2 : configuration de la démonstration NAD et ISE

1. Téléchargez et installez Secure Client NAM (Network Access Manager)

[Téléchargement de logiciels Cisco](#)

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.


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

Il existe plusieurs façons de déployer le client sécurisé sur les périphériques Windows : depuis


SCCM, depuis le moteur de service d'identité et depuis la tête de réseau VPN. Cependant, dans cet article, la méthode d'installation utilisée est la méthode de pré-déploiement.

Sur la page, recherchez le fichier Package de déploiement de tête de réseau Cisco Secure Client (Windows).

Cisco Secure Client Pre-Deployment 06-Feb-2024 108.30 MB  















Package (Windows) - includes individual MSI files 

[cisco-secure-client-win-5.1.2.42-predeploy-k9.zip](#)

[Advisories](#) 

Fichier zip Msi

Une fois téléchargé et extrait, cliquez sur Setup.

 Profiles	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-dart-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nam-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-posture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 setup	4/4/2024 7:16 PM

Fichiers client sécurisés

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, veuillez à installer le module VPN.

Select the Cisco Secure Client 5.1.2.42 modules you wish to install:

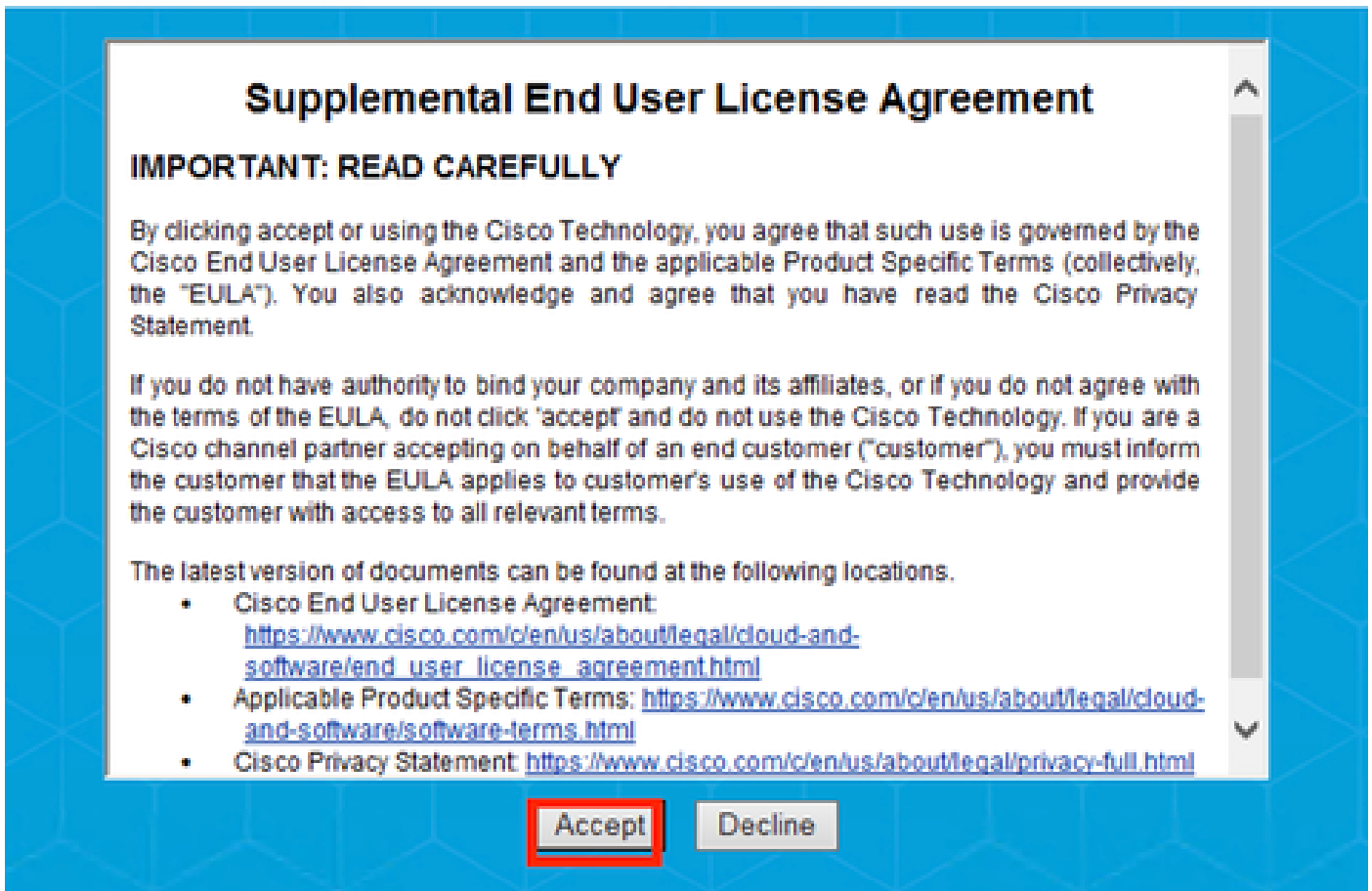
- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- ThousandEyes
- Zero Trust Access
- Select All
- Diagnostic And Reporting Tool
- Lock Down Component Services

Install Selected

Sélecteur d'installation

Cliquez sur Instal Selected.

Acceptez le CLUF.



Fenêtre CLUF

Un redémarrage est nécessaire après l'installation de NAM.

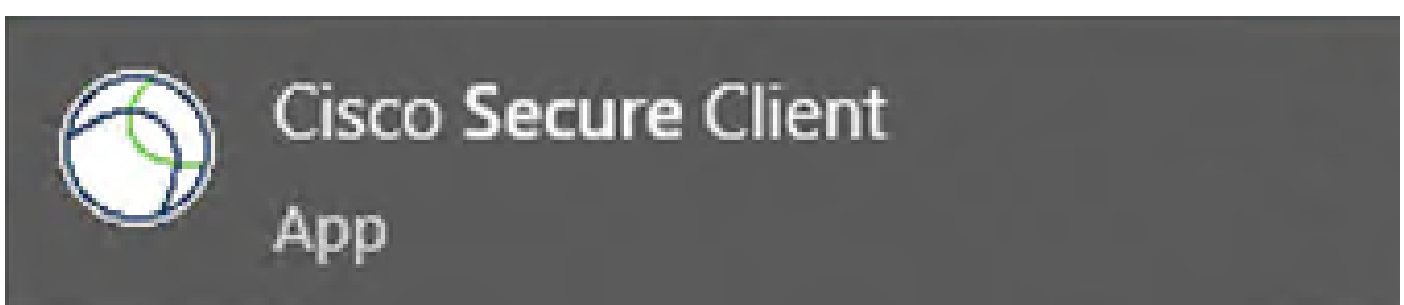
Cisco Secure Client Install Selector

You must reboot your system for the installed changes to take effect.

OK

Fenêtre Conditions de redémarrage

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

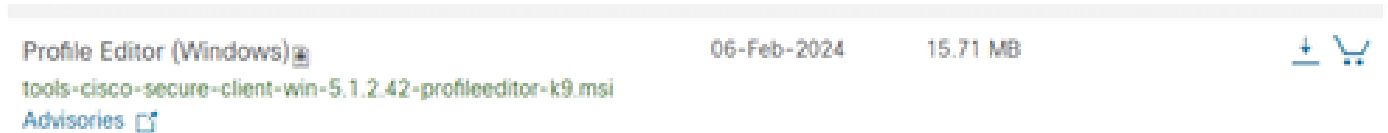


2. Téléchargez et installez Secure Client NAM Profile Editor.

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

L'option Éditeur de profil est disponible à partir de la même page où Secure Client est téléchargé.

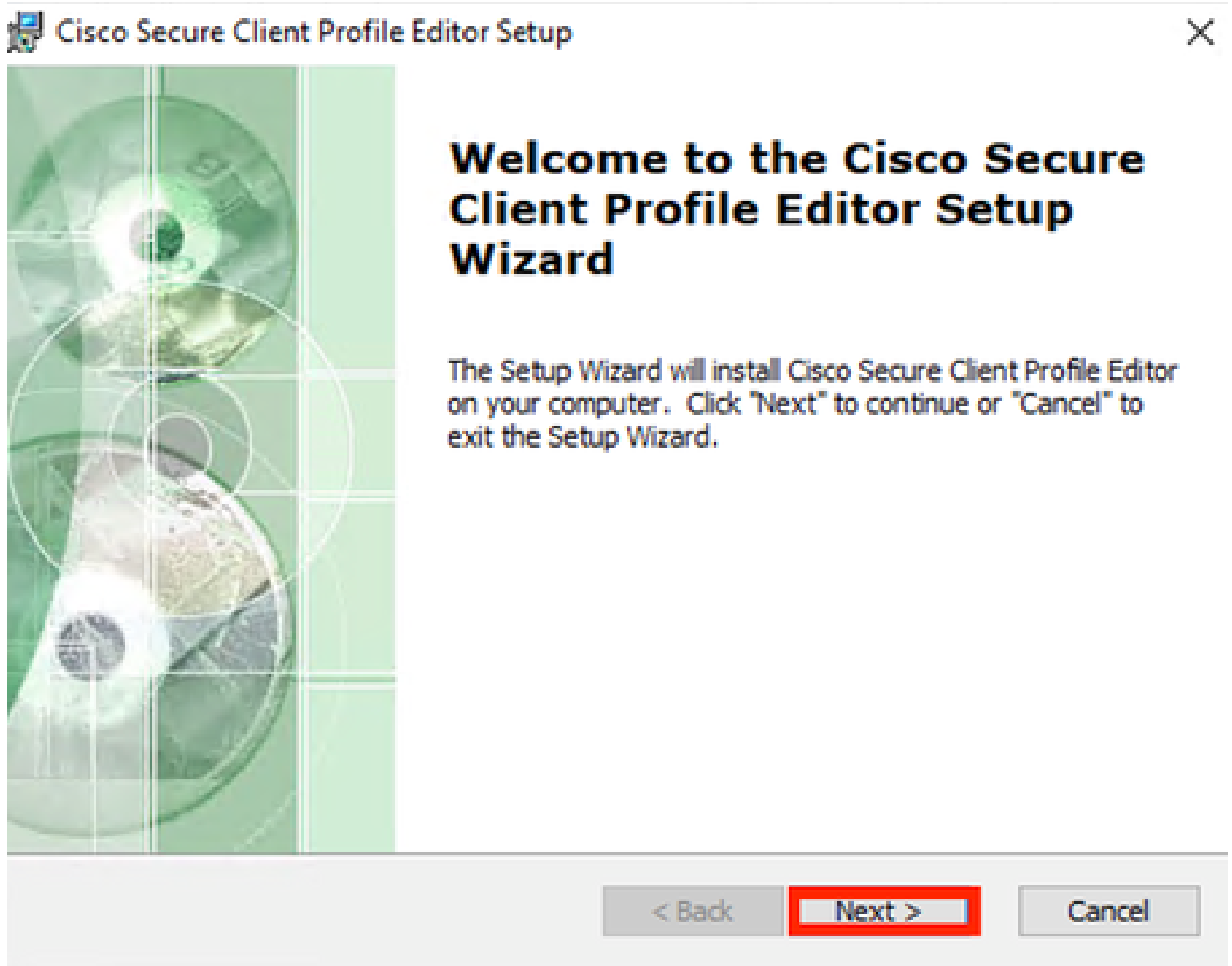
Cet exemple utilise l'option avec la version 5.1.2.42.



Éditeur de profil

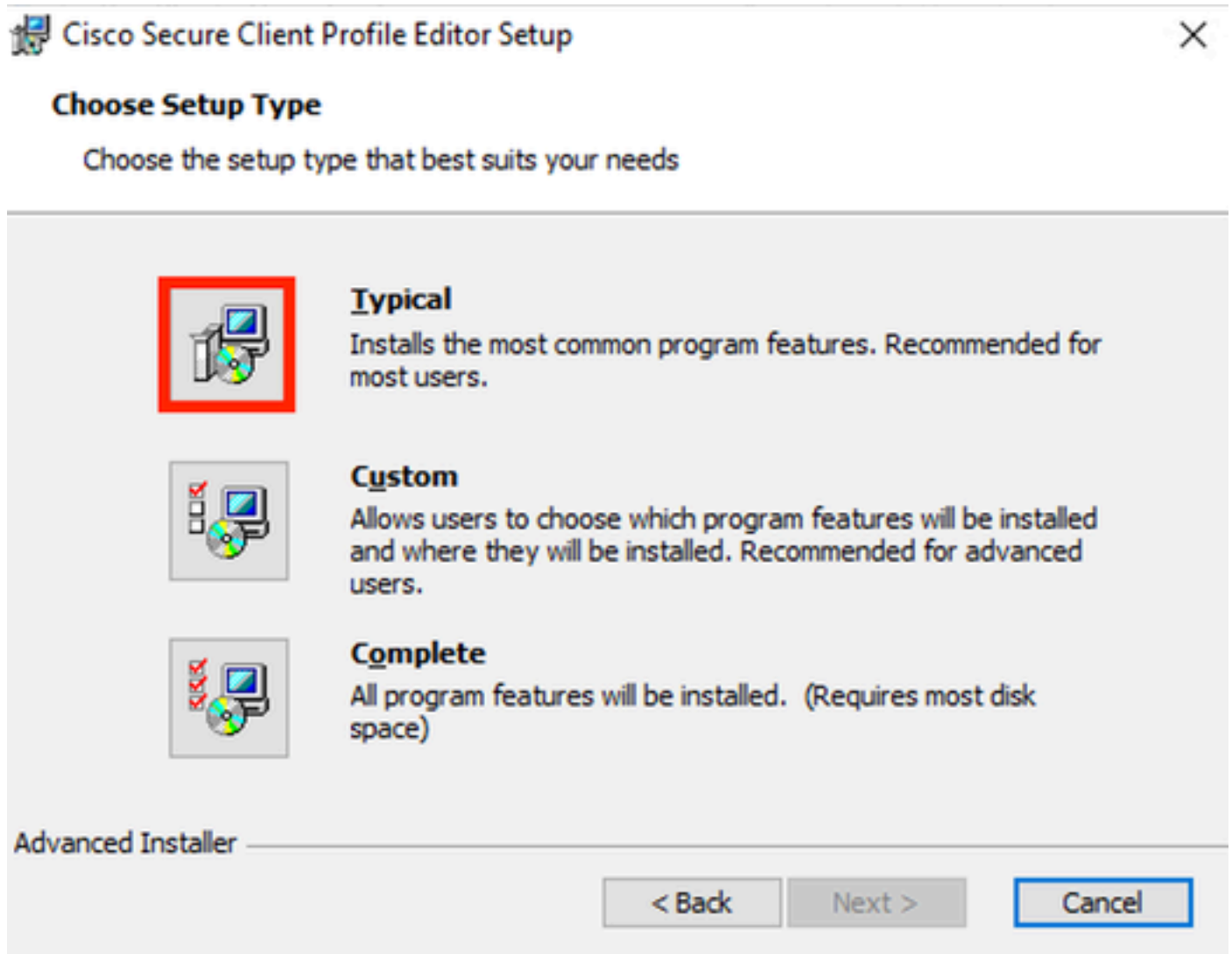
Une fois le téléchargement terminé, poursuivez l'installation.

Exécutez le fichier msi.

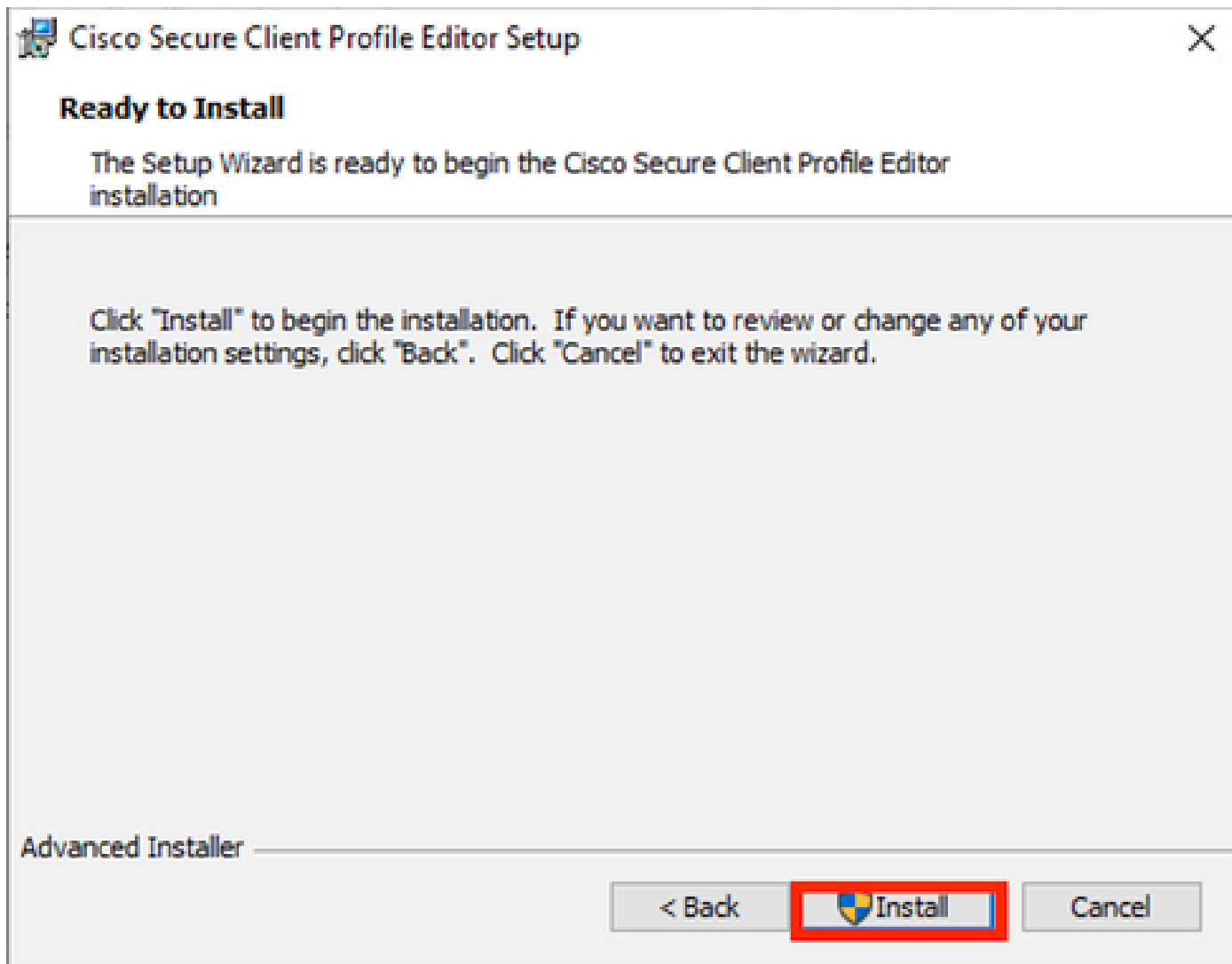


Fenêtre Configuration de Profile Editor

Utilisez l'option Typical setup.



Configuration de Profile Editor



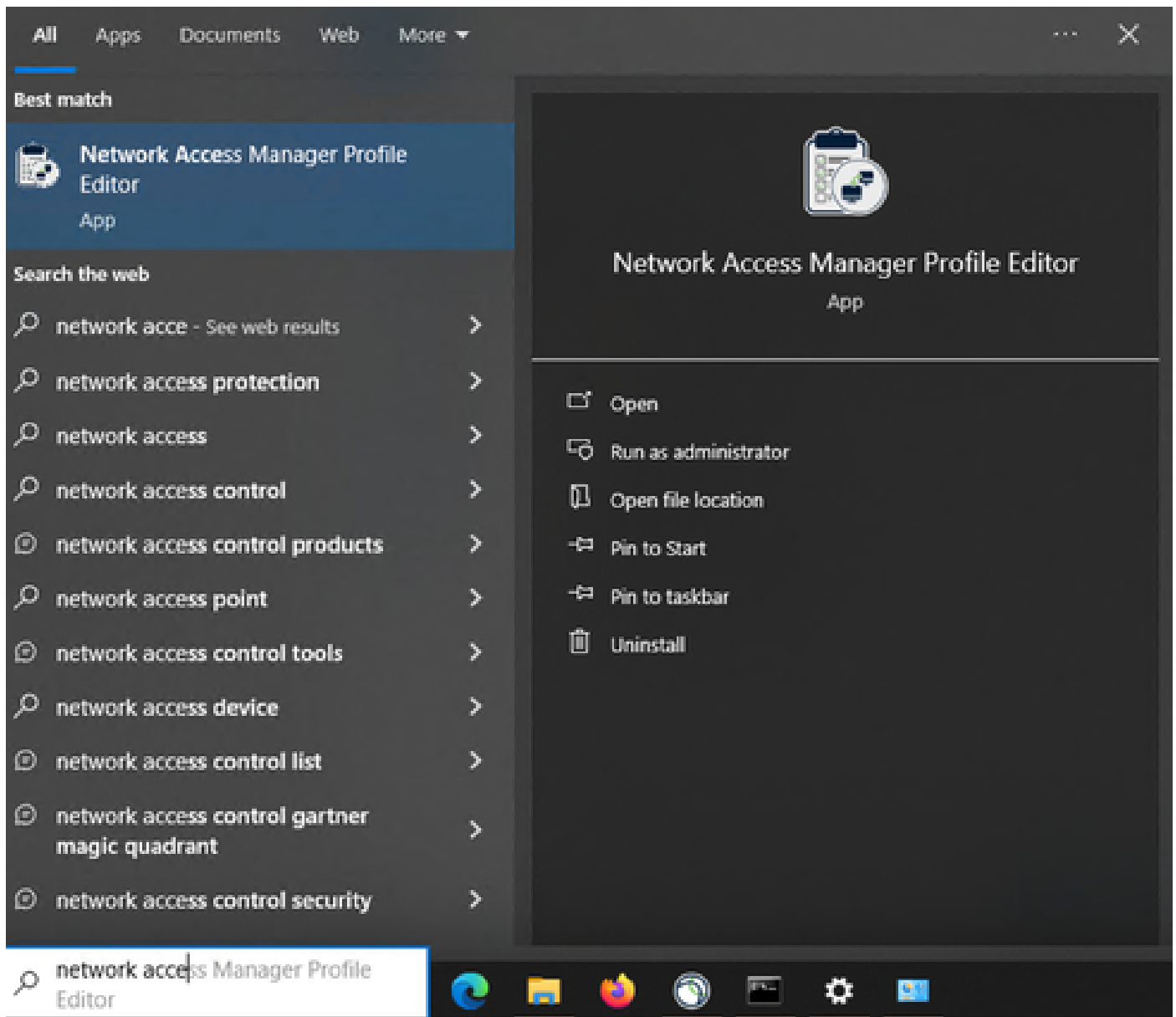
Fenêtre d'installation

Cliquez sur Finish (Terminer).



Fin de la configuration de Profile Editor

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

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

3. Configurations générales par défaut

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

- Stratégie client
- Stratégie d'authentification
- Groupes réseau

Network Access Manager

- Client Policy
- Authentication Policy
- Networks
- Network Groups

Client Policy

Profile: Untitled

Connection Settings

Default Connection Timeout (sec.)

Connection Attempt:

Before user logon

Time to wait before allowing user to logon (sec.)

After user logon

Media

Manage Wi-Fi (wireless) Media

- Enable validation of WPA/WPA2/WPA3 handshake
- Enable Randomized MAC Address

Default Association Timeout (sec.)

Manage Wired (802.3) Media

Manage Mobile Broadband (3G) Media

- Enable Data Roaming

End-user Control

Allow end-user to:

- Disable Client
- Display user groups
- Specify a script or application to run when connected
- Auto-connect

Select machine connection type

Enable by default

Administrative Status

Service Operation: Enable Disable

FIPS Mode: Enable Disable

Captive Portal Detection: Enable Disable

Stratégie du client Éditeur de profil NAM

- Network Access Manager
 - Client Policy
 - Authentication Policy**
 - Networks
 - Network Groups

Authentication Policy

Profile: Untitled

Allow Association Modes

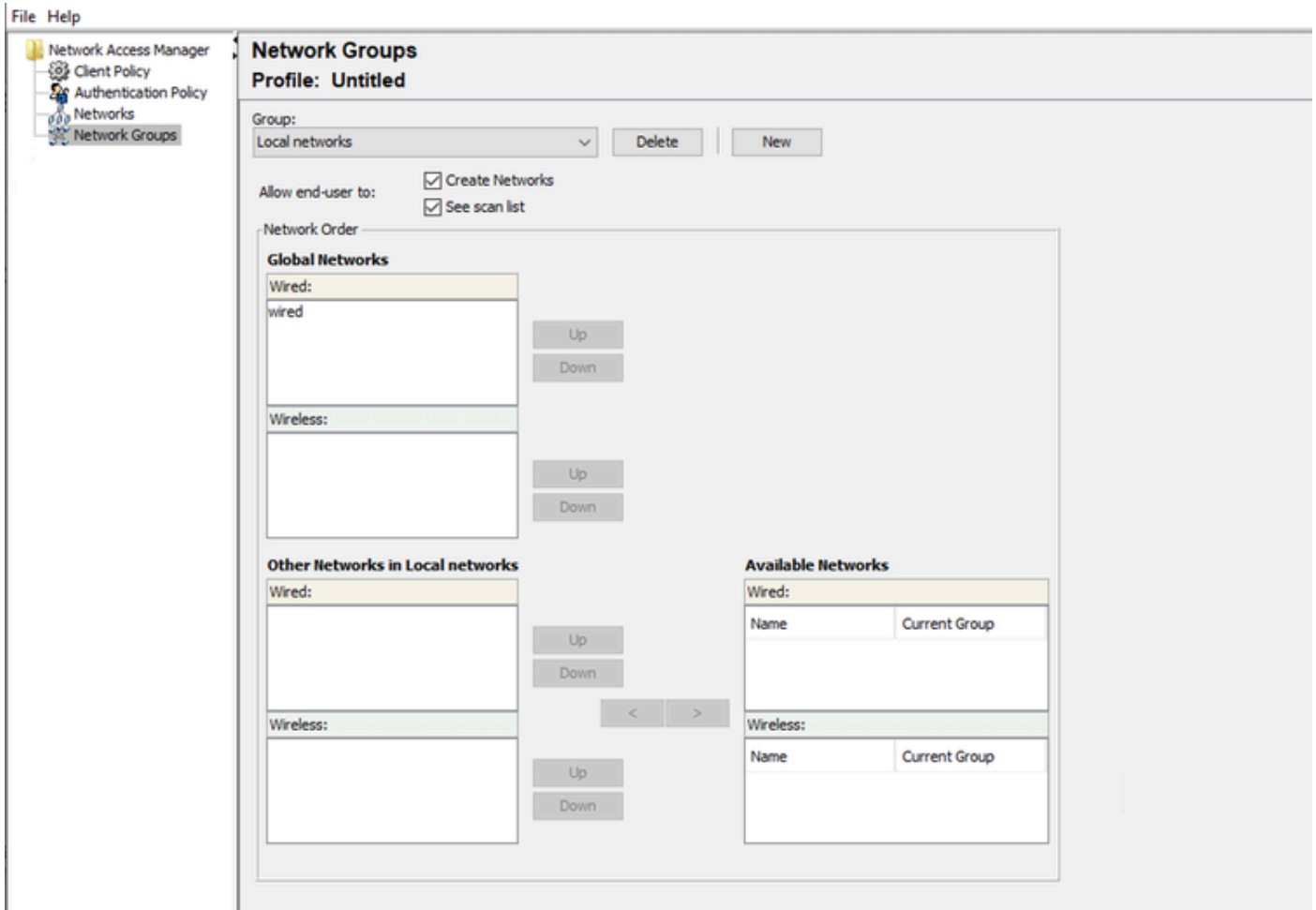
- Select All (Personal)
 - Open (no encryption)
 - Open (Static WEP)
 - Shared (WEP)
 - WPA Personal TKIP
 - WPA Personal AES
 - WPA2 Personal TKIP
 - WPA2 Personal AES
 - WPA3 Open (OWE)
 - WPA3 Personal AES (SAE)
- Select All (Enterprise)
 - Open (Dynamic (802.1X) WEP)
 - WPA Enterprise TKIP
 - WPA Enterprise AES
 - WPA2 Enterprise TKIP
 - WPA2 Enterprise AES
 - CKM Enterprise TKIP
 - CKM Enterprise AES
 - WPA3 Enterprise AES

Allowed Authentication Modes

- Select All Outer
 - EAP-FAST
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS
 - EAP-TLS
 - EAP-TTLS
 - EAP-MD5
 - EAP-MSCHAPv2
 - PAP (legacy)
 - CHAP (legacy)
 - MSCHAP (legacy)
 - MSCHAPv2 (legacy)
 - LEAP
 - PEAP
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS

Allowed Wired Security

- Select All
 - Open (no encryption)
 - 802.1x only
 - 802.1x with MacSec
 - AES-GCM-128
 - AES-GCM-256



Onglet Groupes de réseaux

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

Accédez à la section Réseaux.

Le profil réseau par défaut peut être supprimé.

Cliquez sur Add.

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Création de profils réseau

Nommez le profil réseau.

Sélectionnez Global pour Appartenance au groupe. Sélectionnez Wired Network media.

Networks

Profile: Untitled

Name:	<input type="text" value="PEAP MSCHAPv2"/>	Media Type
Group Membership	<input type="radio"/> In group: <input type="text" value="Local networks"/>	Security Level
	<input checked="" type="radio"/> In all groups (Global)	
Choose Your Network Media	<input checked="" type="radio"/> Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.	
	<input type="radio"/> Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): <input type="text"/> <input type="checkbox"/> Hidden Network <input type="checkbox"/> Corporate Network Association Timeout: <input type="text" value="5"/> seconds	
Common Settings	Script or application on each user's machine to run when connected. <input type="text"/> <input type="button" value="Browse Local Machine"/> Connection Timeout: <input type="text" value="40"/> seconds	
<input type="button" value="Next"/> <input type="button" value="Cancel"/>		

Section Network Profile Media Type

Cliquez sur Next (Suivant).

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

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

Media Type
Security Level
Connection Type

802.1X Settings

authPeriod (sec.) 30 startPeriod (sec.) 3
heldPeriod (sec.) 60 maxStart 2

Security

Key Management
None

Encryption

AES GCM 128
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

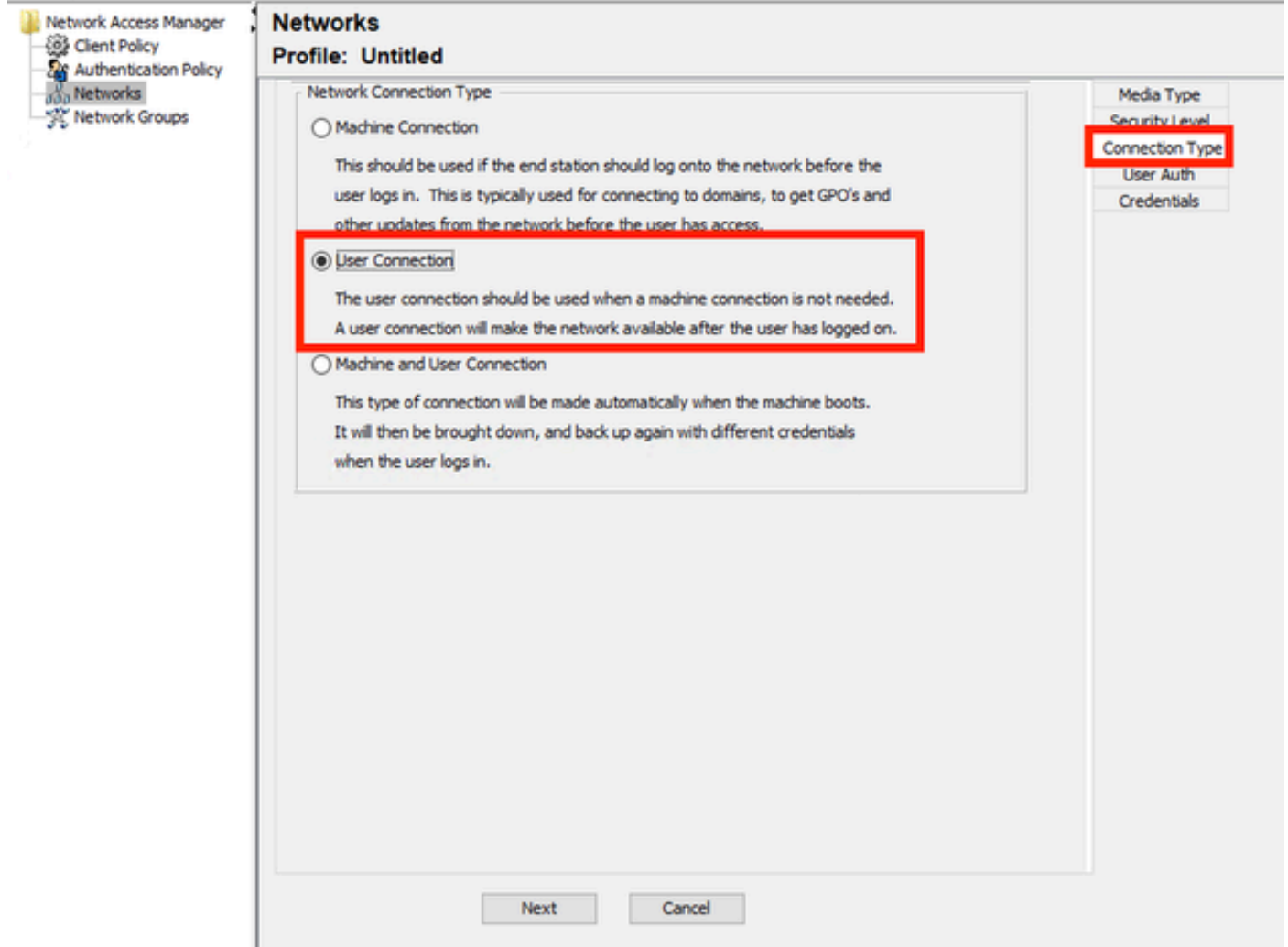
Allow data traffic before authentication
 Allow data traffic after authentication even if

EAP fails
 EAP succeeds but key management fails

Next Cancel

Niveau de sécurité du profil réseau

Cliquez sur Next pour passer à la section Connection Type.



Type de connexion de profil réseau

Sélectionnez le type de connexion Connexion utilisateur.

Cliquez sur Next pour continuer avec la section User Auth qui est maintenant disponible.

Sélectionnez PEAP comme méthode EAP générale.

Networks
Profile: Untitled

EAP Methods

- EAP-MD5
- EAP-MSCHAPv2
- EAP-GTC
- EAP-TLS
- EAP-TTLS
- PEAP
- EAP-FAST

Extend user connection beyond log off

EAP-PEAP Settings

- Validate Server Identity
- Enable Fast Reconnect
- Disable when using a Smart Card

Inner Methods based on Credentials Source

- Authenticate using a Password
 - EAP-MSCHAPv2
 - EAP-GTC
- EAP-TLS, using a Certificate
- Authenticate using a Token and EAP-GTC

Media Type
Security Level
Connection Type
User Auth
Certificates
Credentials

Next Cancel

Authentification utilisateur profil réseau

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

Passez à la section Méthodes internes basées sur la source des informations d'identification.

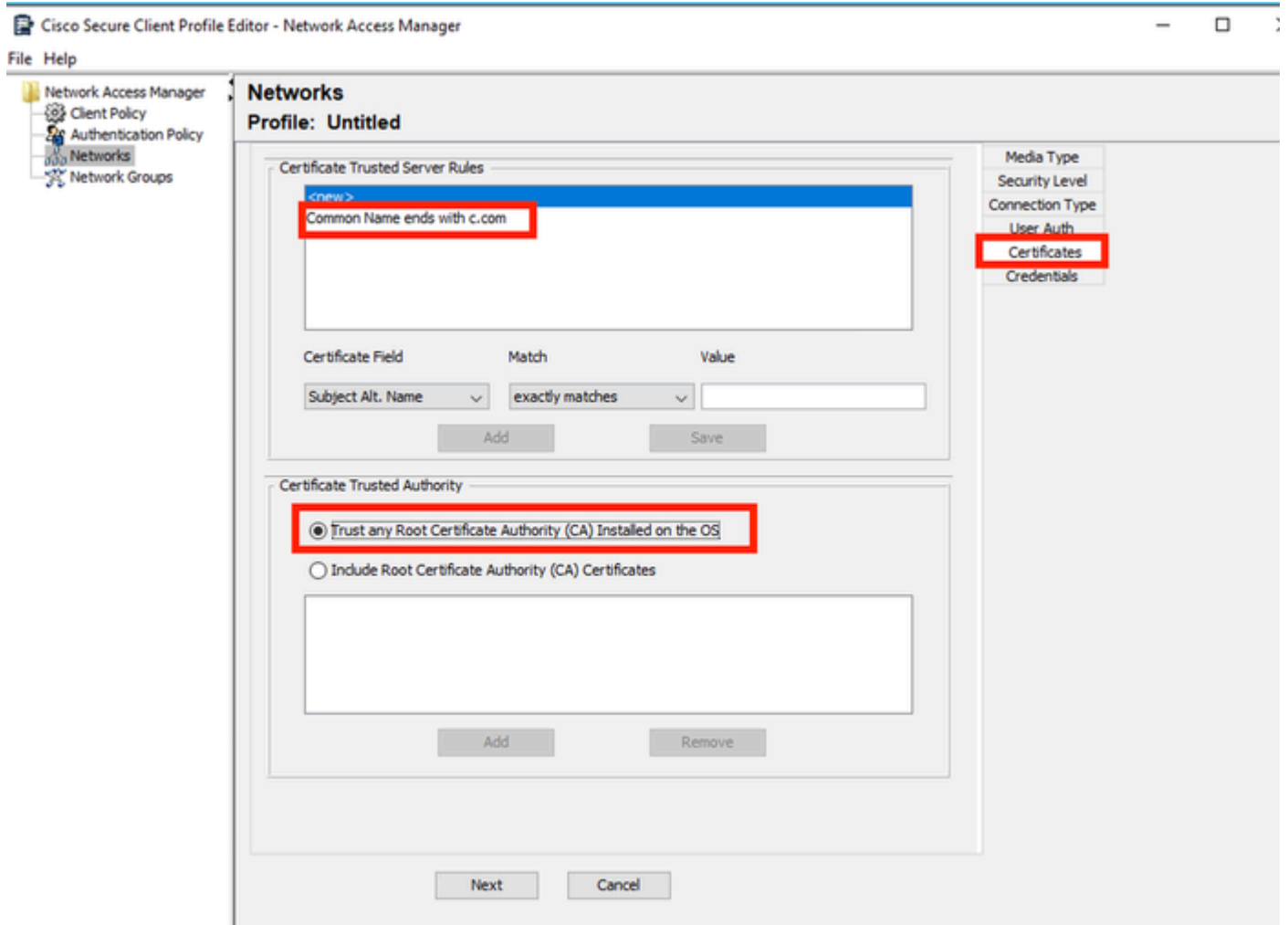
Parmi les multiples méthodes internes qui existent pour EAP PEAP, sélectionnez Authenticate using a Password et sélectionnez EAP-MSCHAPv2.

Cliquez sur Next pour passer à la section Certificate.



Remarque : la section Certificate s'affiche car l'option Validate Server Identity in EAP-PEAP Settings est sélectionnée. Pour EAP PEAP, il effectue l'encapsulation à l'aide du certificat du serveur.

Dans la section Certificates, dans 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 Identity Service Engine (ISE) est utilisé dans votre environnement, vous pouvez utiliser le nom commun du certificat EAP du noeud de serveur de stratégie.

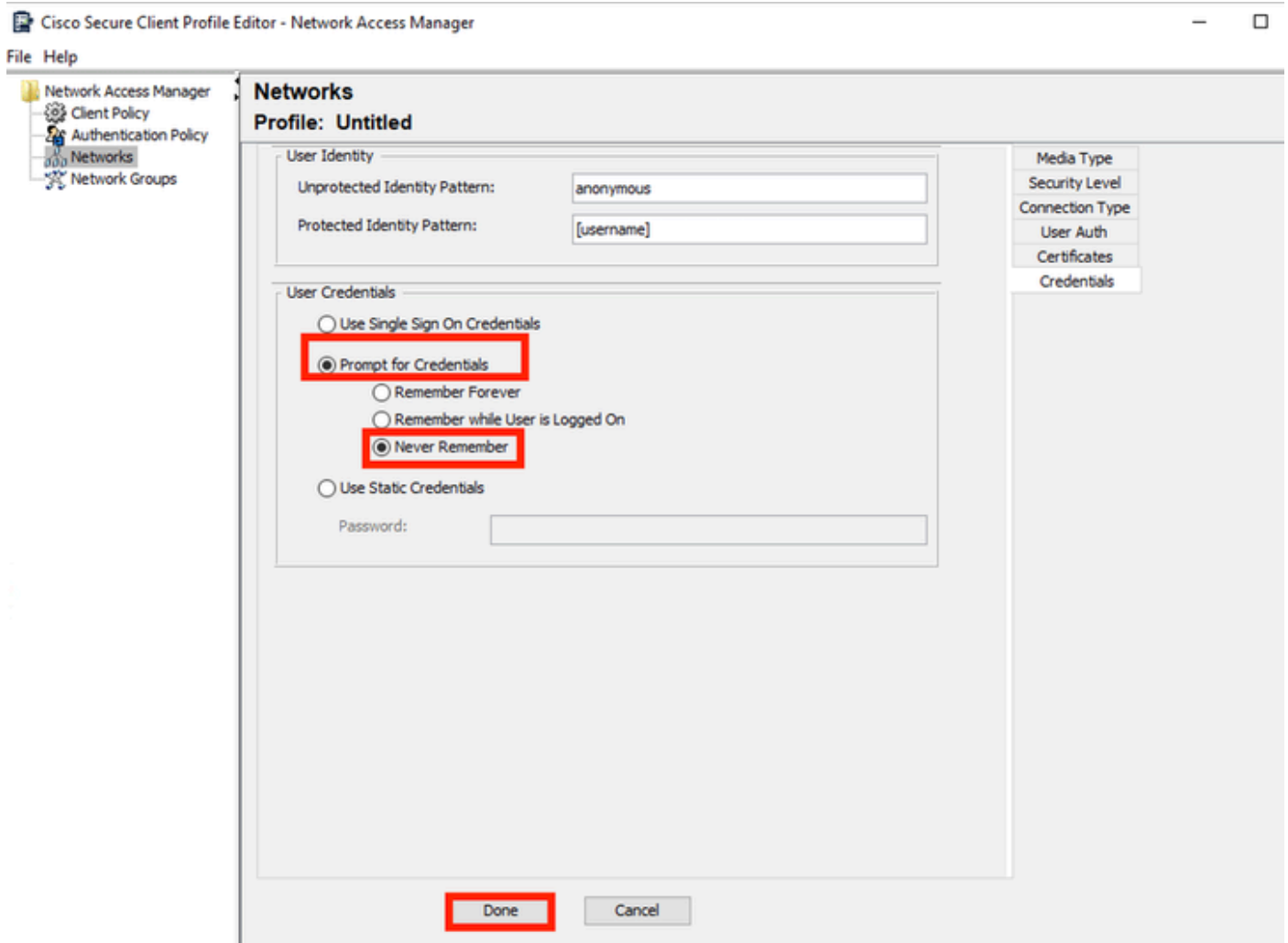


Section Certificat de profil réseau

Deux options peuvent être sélectionnées dans l'autorité de confiance du certificat. Pour 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.

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.

Cliquez sur Next (Suivant).



Section Network Profile Credentials

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

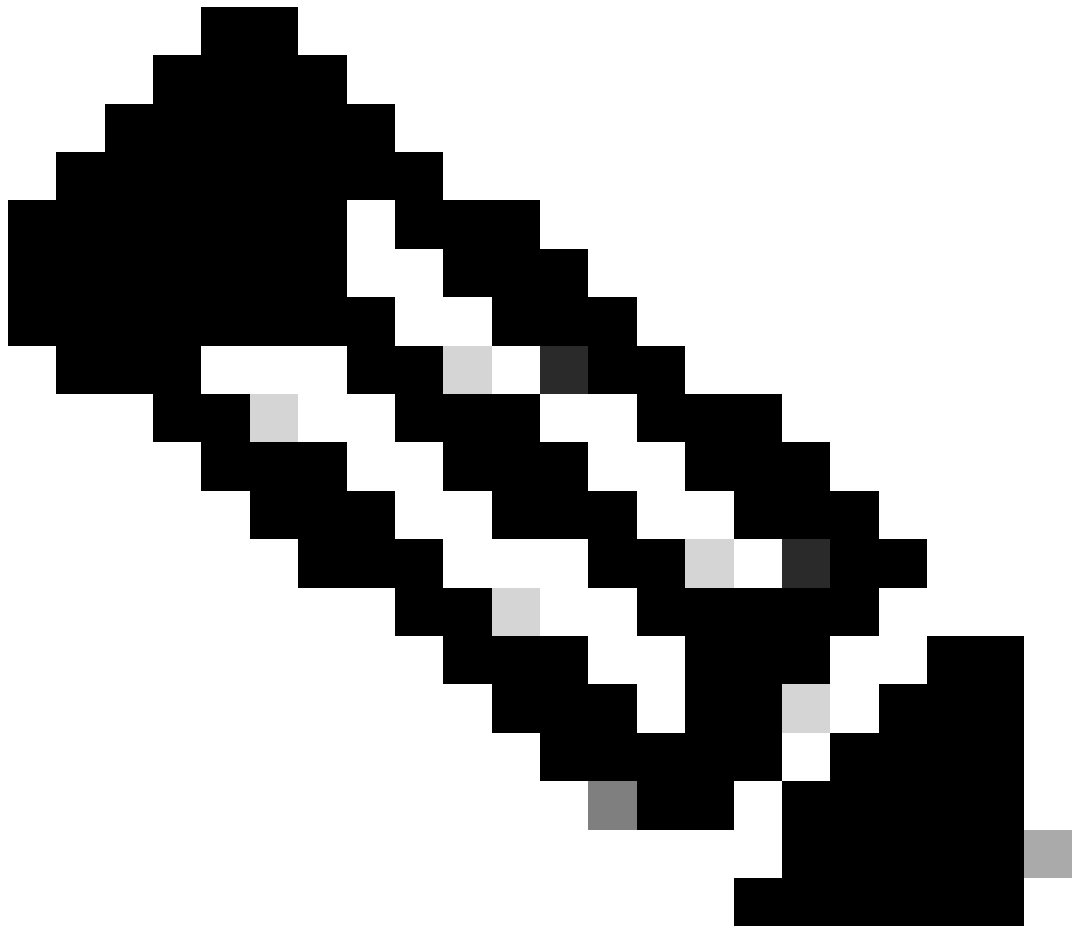
L'option Prompt for Credentials > Never Remember est sélectionnée, de sorte que dans chaque authentification, l'utilisateur qui effectue l'authentification doit entrer ses identifiants.

Cliquez sur Done.

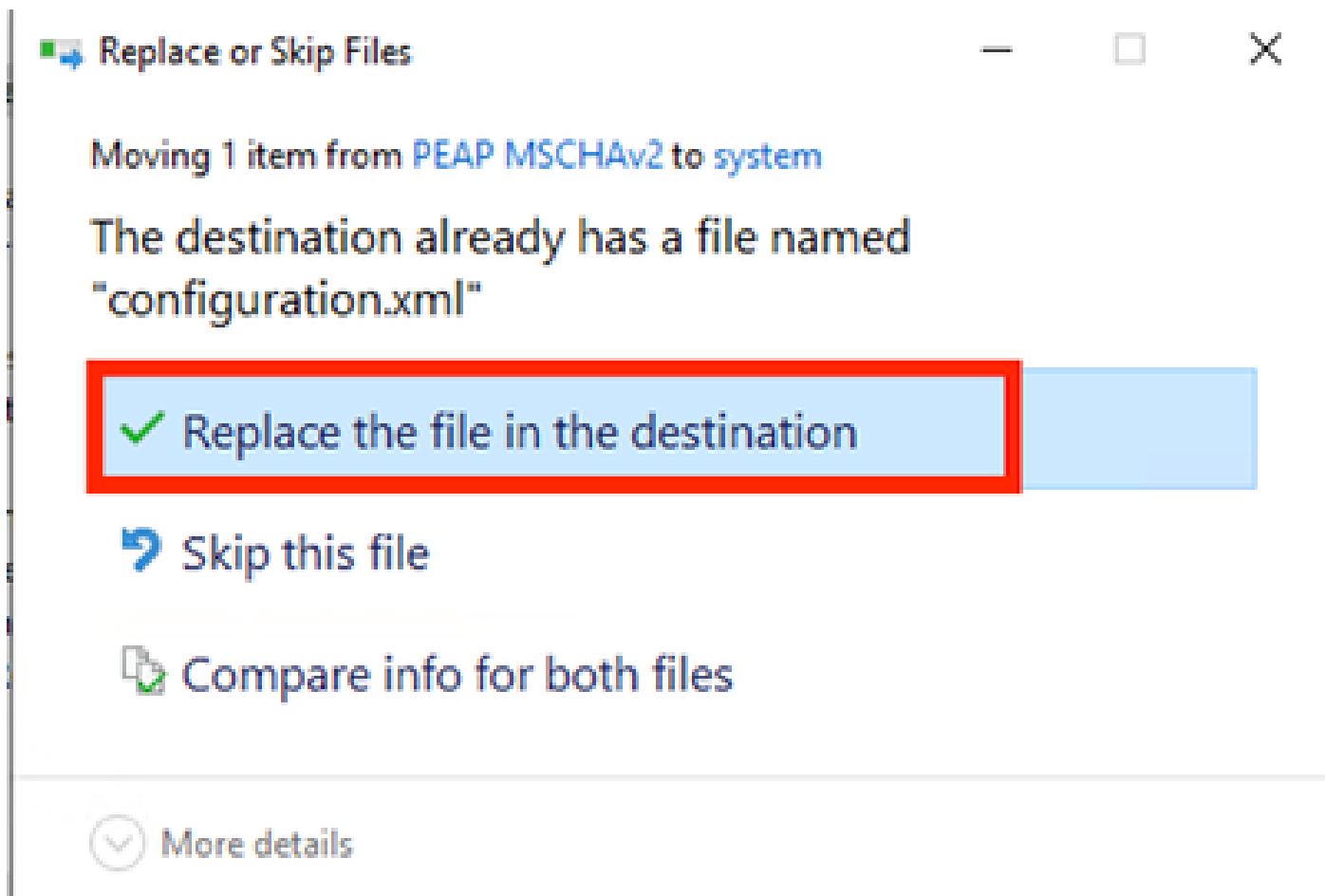
Enregistrez le profil Secure Client Network Access Manager sous le nom configuration.xml avec l'option Fichier > Enregistrer sous.

Pour que la fonction Secure Client Network Access Manager utilise le profil qui vient d'être créé, remplacez le fichier configuration.xml du 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

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

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

Cliquez sur Add.

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Onglet Réseau de NAM Profile Editor

Entrez un nom dans le profil réseau.

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

File Help

Networks
Profile: Untitled

Name: **EAP-FAST**

Group Membership

In group: Local networks

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network
 Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: seconds

Media Type
Security Level

Section Type de support

Cliquez sur Next (Suivant).

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

File Help

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

Security

Key Management
None

Encryption

AES GCM 128
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails
 EAP succeeds but key management fails

Next Cancel

Section Éditeur de profil de niveau de sécurité

Cliquez sur Next pour passer à la section Connection Type.

File Help

Networks
Profile: Untitled

Network Connection Type

Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

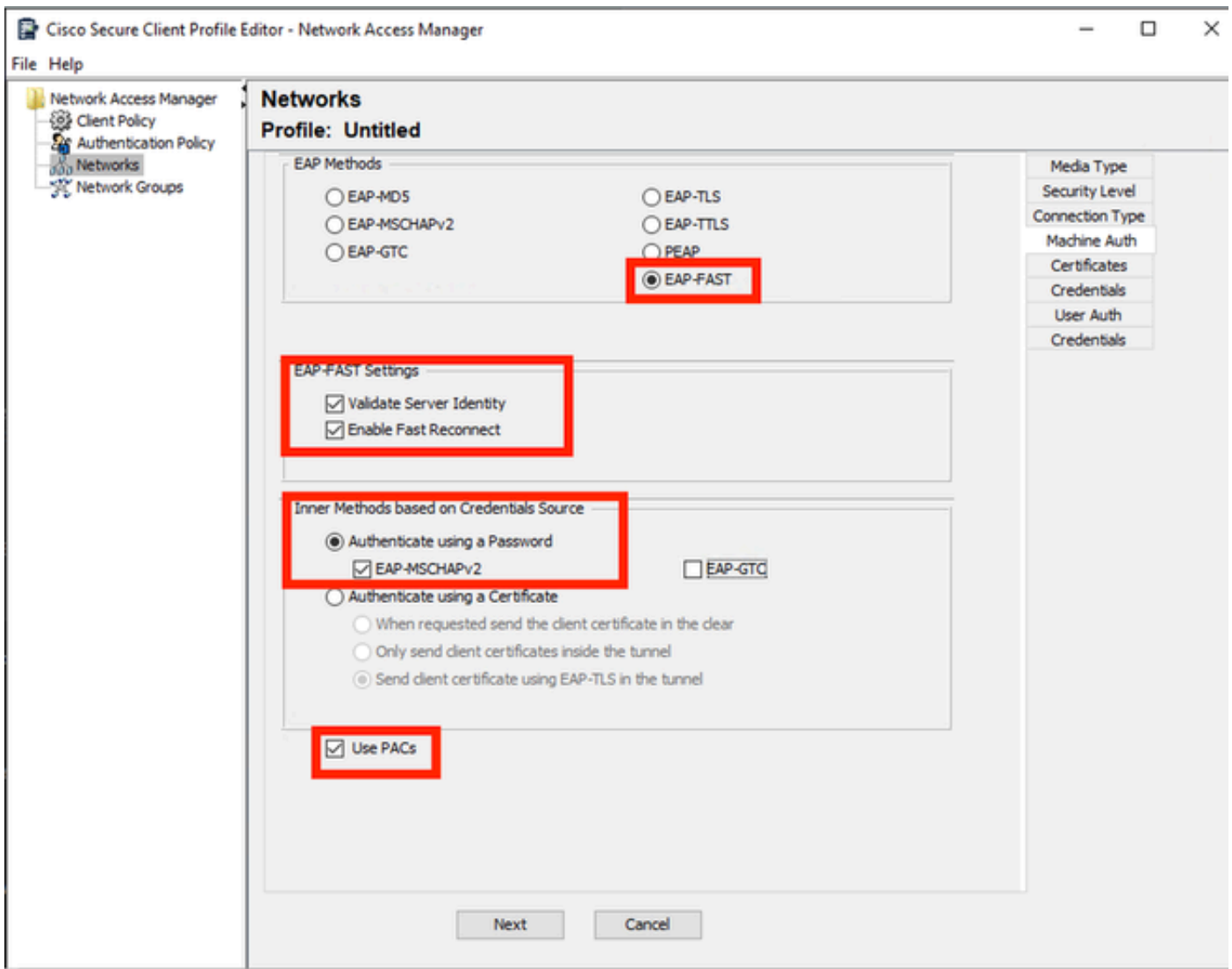
Media Type
Security Level
Connection Type
Machine Auth
Credentials
User Auth
Credentials

Next Cancel

Section Type de connexion

Configurez simultanément l'authentification des utilisateurs et des ordinateurs en sélectionnant la troisième option.

Cliquez sur Next (Suivant).



Section Authentication machine

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

Cliquez sur Next (Suivant).

Dans la section Certificates, dans Certificate Trusted Server Rules, le nom commun de la règle 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.

Networks

Profile: Untitled

Certificate Trusted Server Rules

<new>
Subject Alternative Name ends with c.com

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Add Save

Certificate Trusted Authority

Trust any Root Certificate Authority (CA) Installed on the OS

Include Root Certificate Authority (CA) Certificates

--

Add Remove

Next Cancel

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

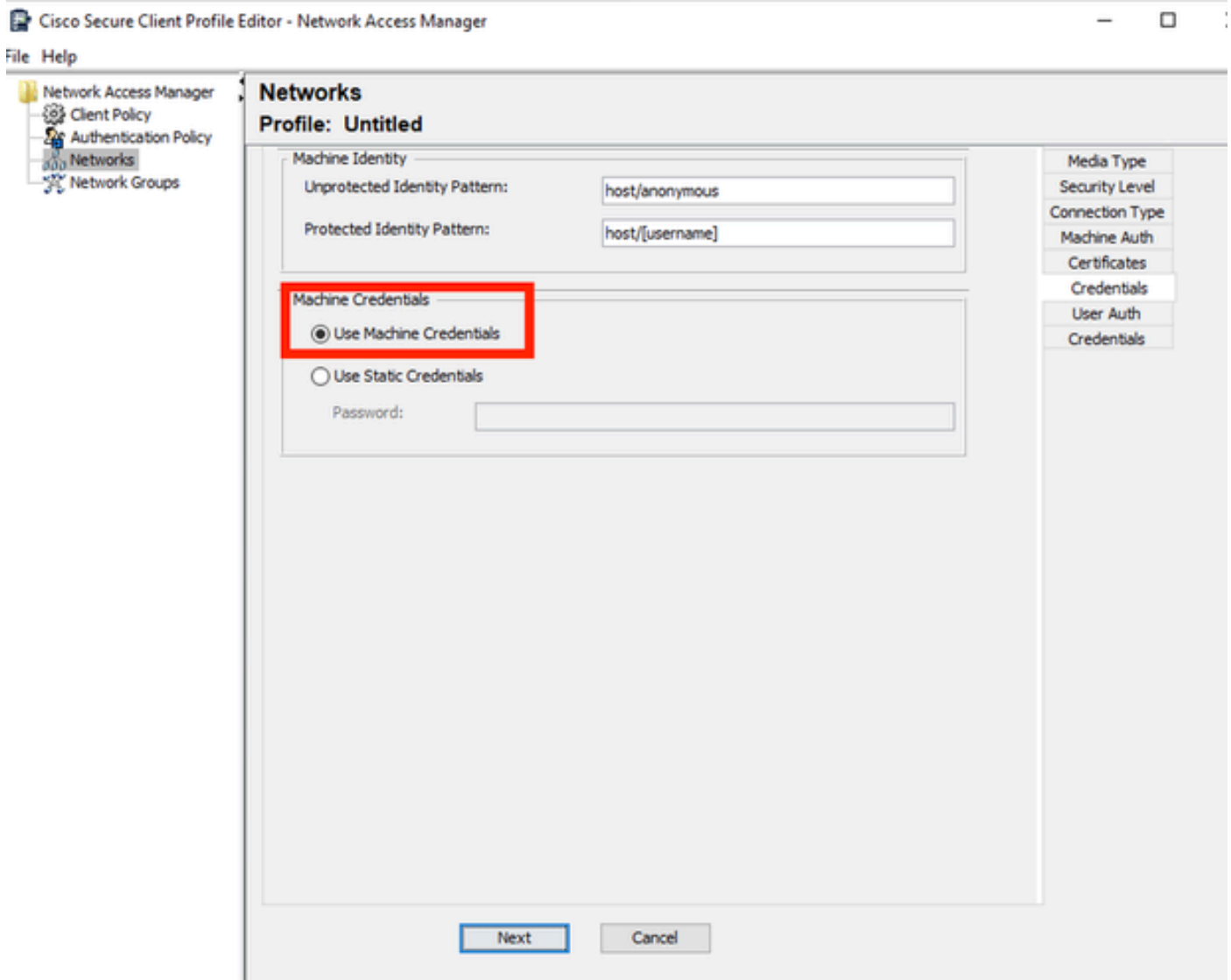
Credentials

Section Autorisation du certificat du serveur d'authentification machine

Deux options peuvent être sélectionnées dans l'autorité de confiance du certificat. Pour 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.

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).

Cliquez sur Next (Suivant).



Section Authentications d'authentification machine

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

Cliquez sur Next (Suivant).

File Help

Networks
Profile: Untitled

EAP Methods

EAP-MD5 EAP-TLS
 EAP-MSCHAPv2 EAP-TTLS
 EAP-GTC PEAP
 EAP-FAST

Extend user connection beyond log off

EAP-FAST Settings

Validate Server Identity
 Enable Fast Reconnect
 Disable when using a Smart Card

Inner Methods based on Credentials Source

Authenticate using a Password
 EAP-MSCHAPv2 EAP-GTC
 Authenticate using a Certificate
 When requested send the client certificate in the clear
 Only send client certificates inside the tunnel
 Send client certificate using EAP-TLS in the tunnel
 Authenticate using a Token and EAP-GTC

Use PACs

Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials

Next Cancel

Section Authentification utilisateur

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

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

Pour la section Inner Method based on credentials source, sélectionnez Authenticate using a Password et EAP-MSCHAPv2 comme méthode.

Sélectionnez Utiliser PAC.

Cliquez sur Next (Suivant).

Dans la section Certificates, dans Certificate Trusted Server Rules, 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.

Networks

Profile: C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml

The screenshot shows the 'Certificate Trusted Server Rules' section of a configuration wizard. A rule is defined with the field 'Common Name', the match 'ends with', and the value 'c.com'. The 'Certificate Trusted Authority' section has the option 'Trust any Root Certificate Authority (CA) Installed on the OS' selected. A sidebar on the right contains a list of configuration options, with 'Certificates' highlighted.

Certificate Field	Match	Value
Common Name	ends with	c.com

Trust any Root Certificate Authority (CA) Installed on the OS
 Include Root Certificate Authority (CA) Certificates

Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials

Next Cancel

Section Autorisation du certificat du serveur d'authentification utilisateur

Deux options peuvent être sélectionnées dans l'autorité de confiance du certificat. Pour 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.

Cliquez sur Next (Suivant).

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

Protected Identity Pattern:

User Credentials

Use Single Sign On Credentials

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Use Static Credentials

Password:

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

Credentials

Done Cancel

Identifiants d'authentification utilisateur

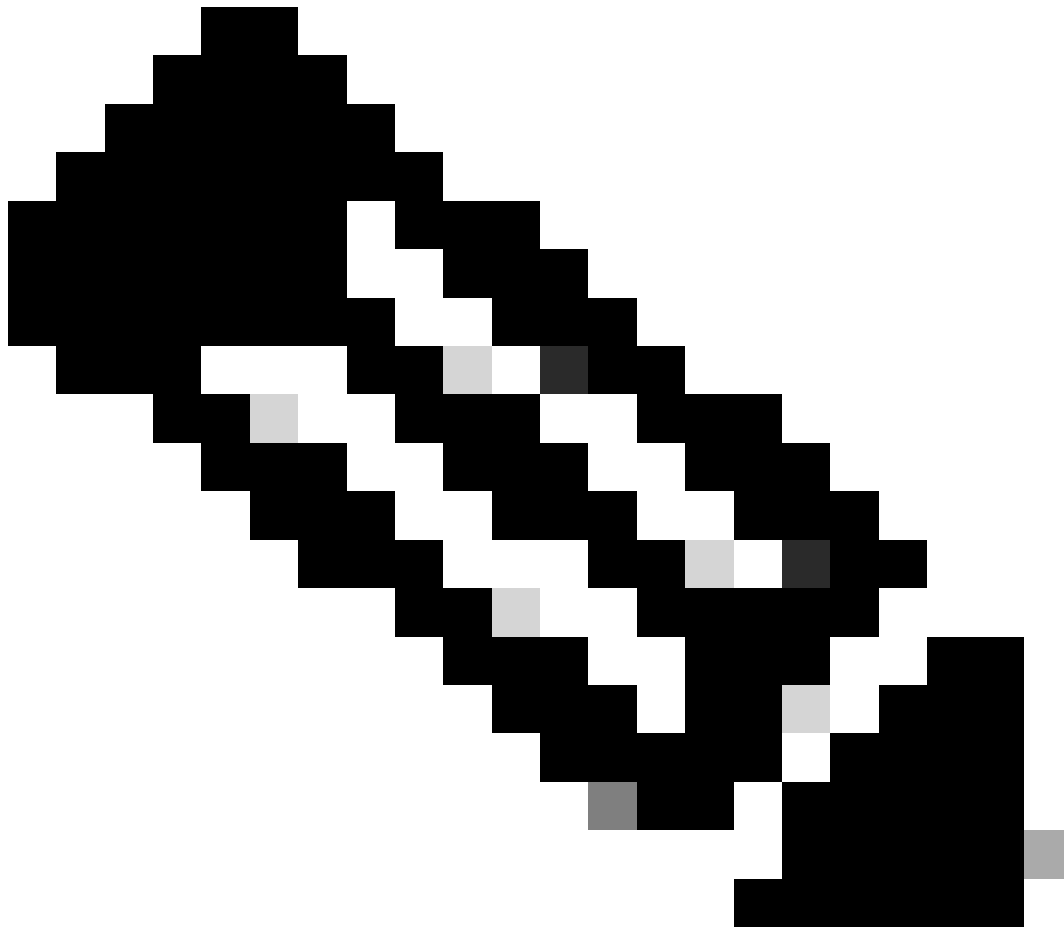
Dans la section Informations d'identification, seule la section Informations d'identification utilisateur est modifiée.

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

Cliquez sur le bouton Terminé.

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

Pour que Secure Client Network Access Manager utilise le profil qui vient d'être créé, remplacez le fichier configuration.xml dans le répertoire suivant par le nouveau :



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

6. Scénario 3 : configuration du demandeur NAM du client sécurisé pour l'authentification du certificat utilisateur EAP TLS

Ouvrez NAM Profile Editor et accédez à la section Networks.

Cliquez sur Add.

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Section Création de réseau

Attribuez un nom au profil réseau, dans ce cas, le nom est associé au protocole EAP utilisé pour ce scénario.

Sélectionnez Global pour Appartenance au groupe. Et Les Supports Réseau Câblés.

Networks
Profile: Untitled

Name: EAP-TLS

Group Membership

In group: Local networks

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network

Corporate Network

Association Timeout: 5 seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: 40 seconds

Media Type
Security Level

Section Type de support

Cliquez sur Next (Suivant).

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

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) startPeriod (sec.)

heldPeriod (sec.) maxStart

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails

EAP succeeds but key management fails

Security

Key Management
None

Encryption

AES GCM 128

AES GCM 256

Media Type

Security Level

Connection Type

Next Cancel

Niveau de sécurité

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

Networks
Profile: Untitled

Network Connection Type

Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Media Type

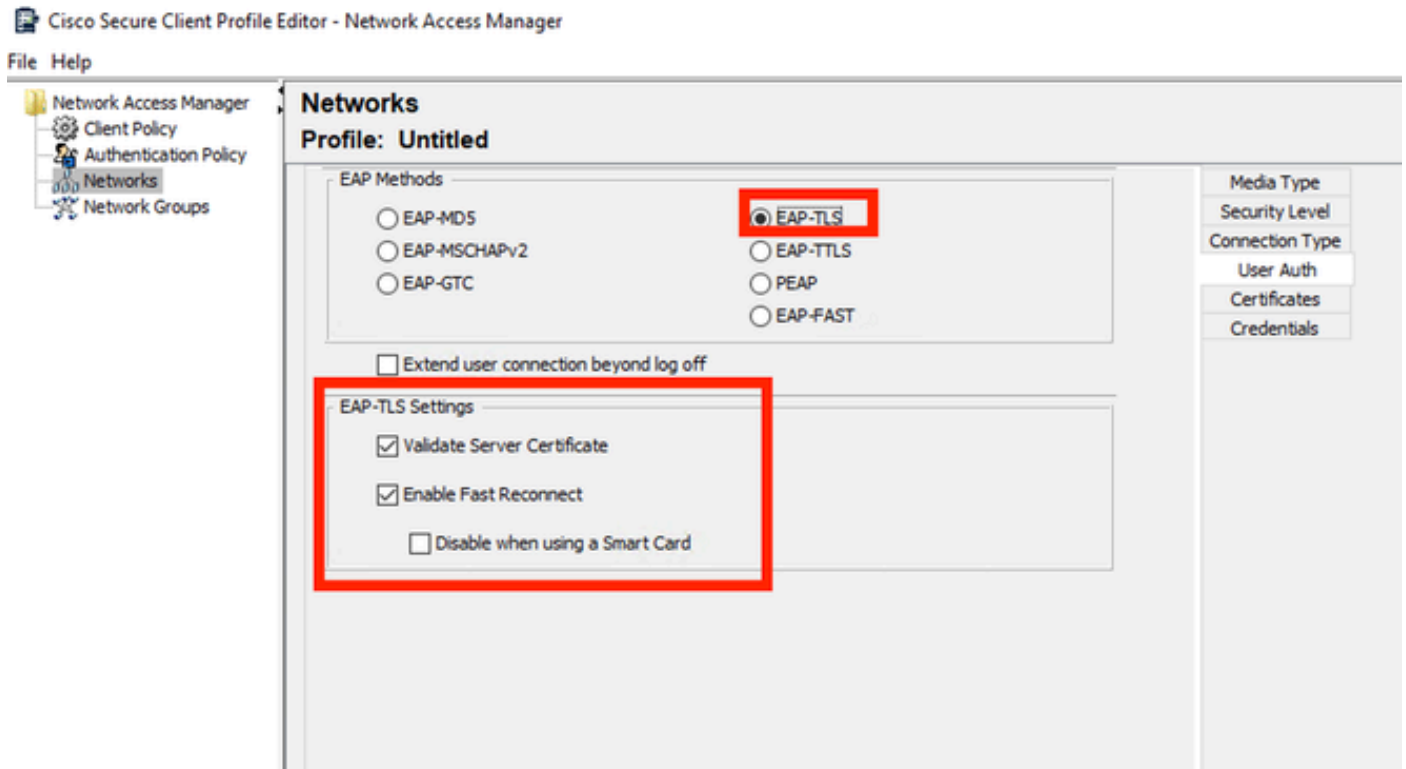
Security Level

Connection Type

User Auth

Credentials

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



Section User Auth

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.

Dans la section Certificate Trusted Authority, sélectionnez Trust any Root Certificate Authority (CA) installée sur le système d'exploitation.

The screenshot shows the 'Networks' section of the Cisco Secure Client Profile Editor. The main window is titled 'Profile: Untitled'. On the left, a navigation pane shows 'Network Access Manager', 'Client Policy', 'Authentication Policy', 'Networks', and 'Network Groups'. The 'Networks' section is active, displaying two configuration panels: 'Certificate Trusted Server Rules' and 'Certificate Trusted Authority'. In the 'Certificate Trusted Server Rules' panel, a rule is listed with the value 'Common Name ends with c.com'. Below this, there are dropdown menus for 'Certificate Field' (set to 'Subject Alt. Name') and 'Match' (set to 'exactly matches'), followed by an empty 'Value' input field and 'Add' and 'Save' buttons. The 'Certificate Trusted Authority' panel has two radio button options: 'Trust any Root Certificate Authority (CA) Installed on the OS' (which is selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these options is an empty list box and 'Add' and 'Remove' buttons. On the right side of the main window, there is a vertical menu with options: 'Media Type', 'Security Level', 'Connection Type', 'Clear Auth', 'Certificates', and 'Credentials'. The 'Certificates' option is highlighted with a red box. At the bottom of the main window, there are 'Next' and 'Cancel' buttons.

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

Cliquez sur Next (Suivant).

Dans la section Informations d'identification et de connexion de l'utilisateur, ne modifiez pas les valeurs par défaut dans la première partie.

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

User Credentials

Use Single Sign On Credentials (Requires Smart Card)

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Certificate Source

Smart Card or OS certificates

Smart Card certificates only

Remember Smart Card Pin

Remember Forever

Remember while User is Logged On

Never Remember

Smart Card Removal Policy

Disconnect from Network

Use Certificate Matching Rule (Max 10)

Rule Logic OR AND

Field	Operator	Value

Media Type

Security Level

Connection Type

User Auth

Certificates

Credentials

Section User Auth Credentials

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 d'usage de certificat (10 max).

Cliquez sur Add.

Certificate Matching Rule Entry [X]

Certificate Field: Issuer.CN Match: Equals

Value: My Internal OR 3rd Party CA.com

OK Cancel

Use Certificate Matching Rule (Max 10)

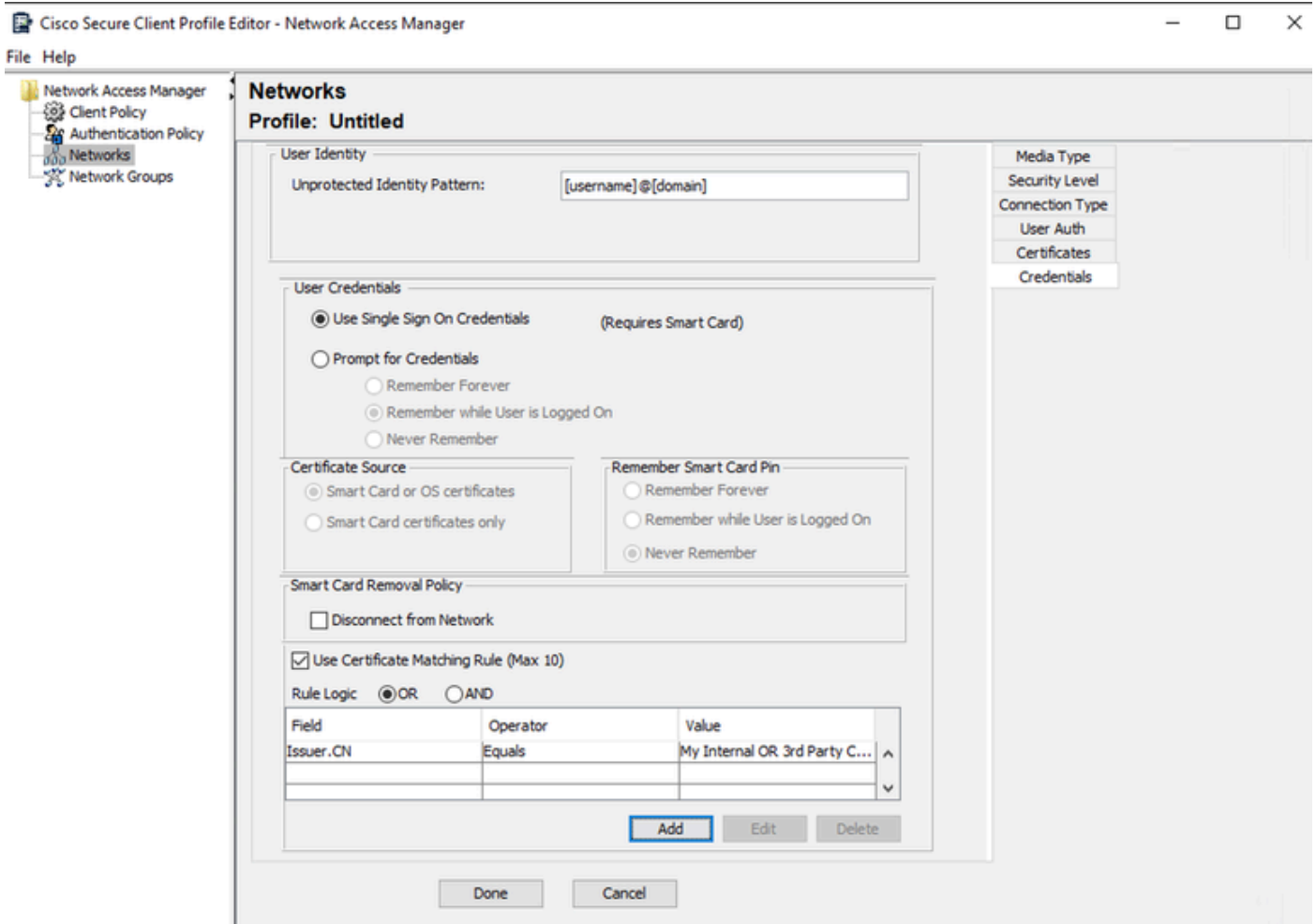
Logic: OR AND

Id	Operator	Value

Add Edit Delete

Fenêtre Règle de correspondance de certificat

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



Section User Auth Certificate Credentials

Cliquez sur Done pour terminer la configuration.

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

Pour que Secure Client Network Access Manager utilise le profil qui vient d'être créé, 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.

7. Configurez ISR 1100 et ISE pour autoriser les authentications en fonction du scénario 1 PEAP MSCHAPv2

configuration du routeur ISR 1100

Cette section couvre la configuration de base que le NAD doit avoir pour que dot1x fonctionne.



Remarque : pour un déploiement ISE multinoeud, pointez vers n'importe quel noeud sur lequel le personnage Policy Server Node est activé. Vous pouvez le vérifier en accédant à 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>
```

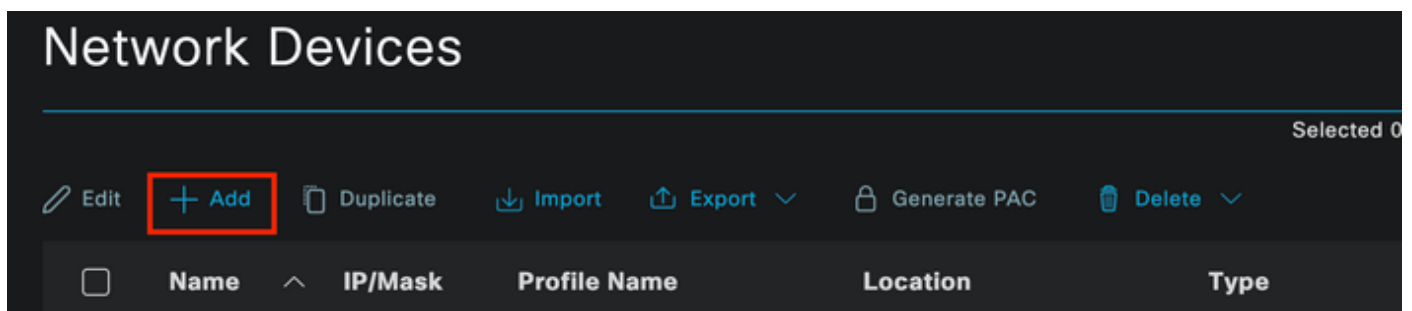
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication priority dot1x mab  
  authentication port-control auto  
  dot1x pae authenticator  
  spanning-tree portfast
```

Configurez Identity Service Engine 3.2.

Configurez le périphérique réseau.

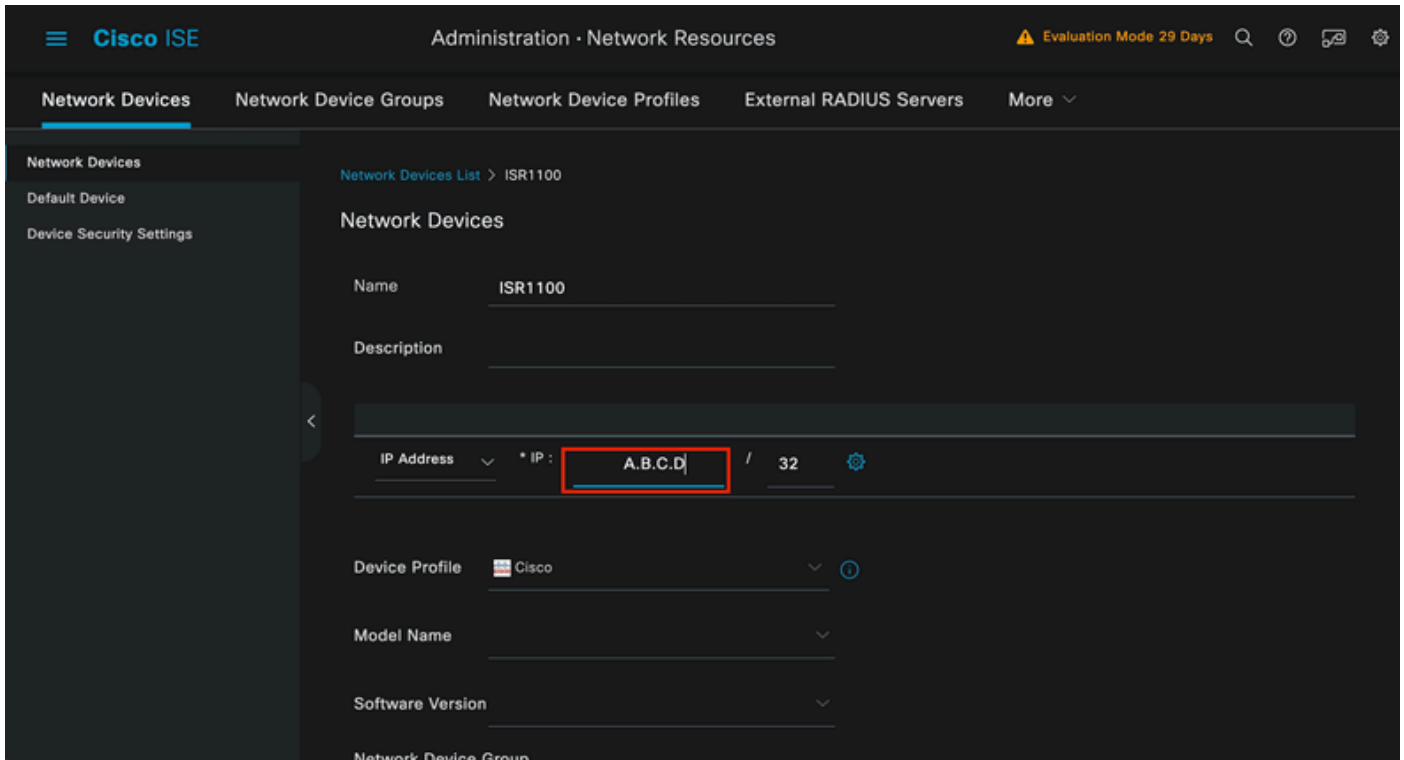
Ajoutez le NAD ISR à l'administration ISE > Ressources réseau > Périphériques réseau.

Cliquez sur Add.



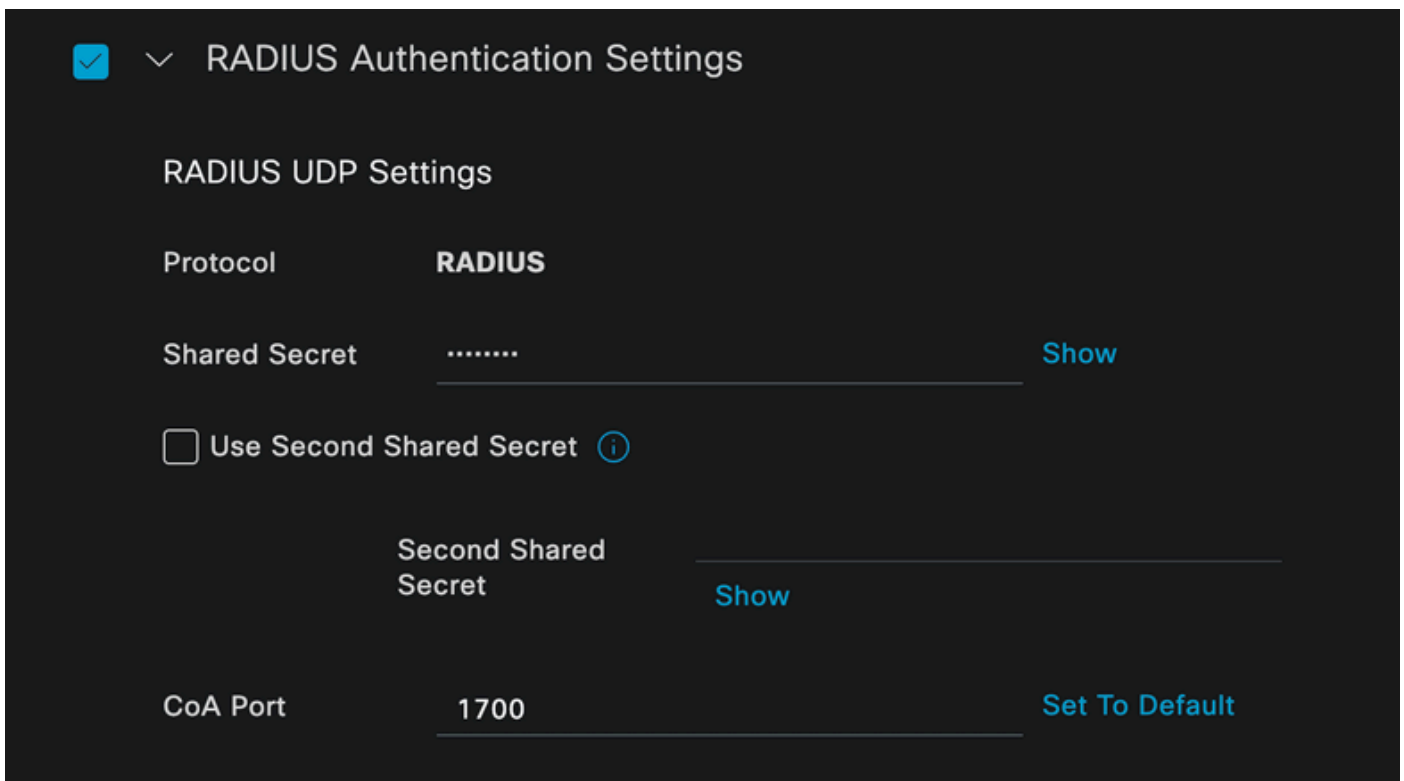
Section Network Device

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



Création de périphériques réseau

Au bas de la même page, ajoutez le même secret partagé que celui que vous avez utilisé dans la configuration de votre périphérique réseau.



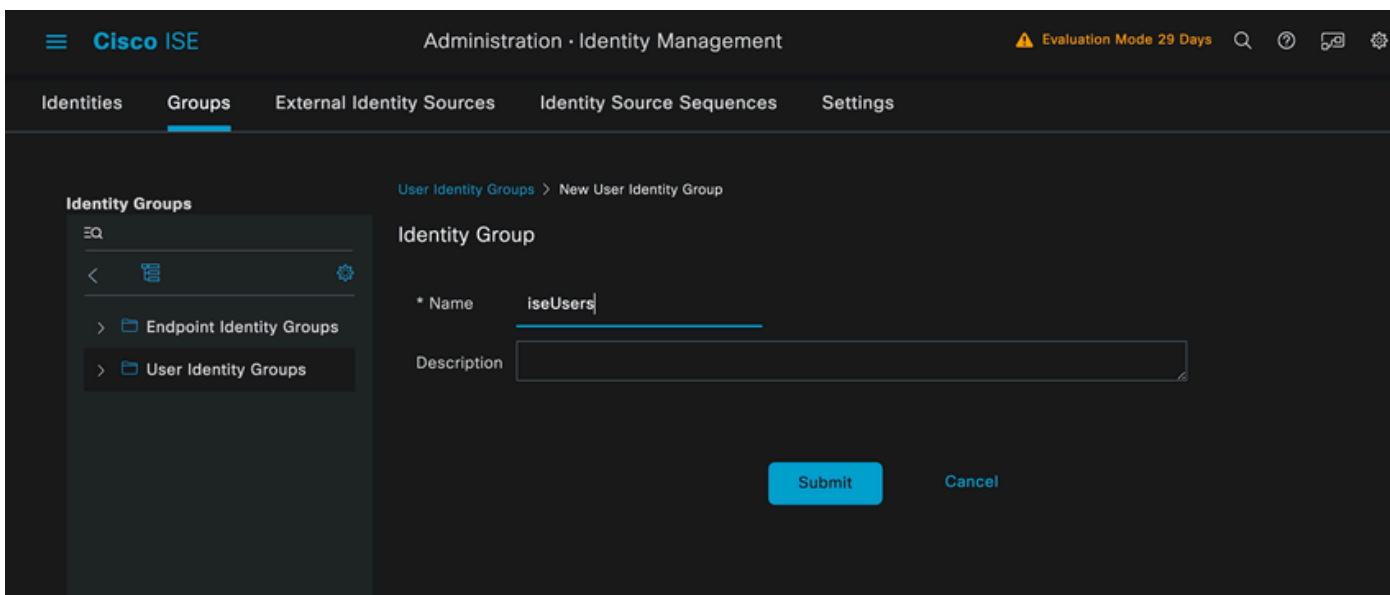
Paramètres du rayon du périphérique réseau

Enregistrez les modifications.

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

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

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

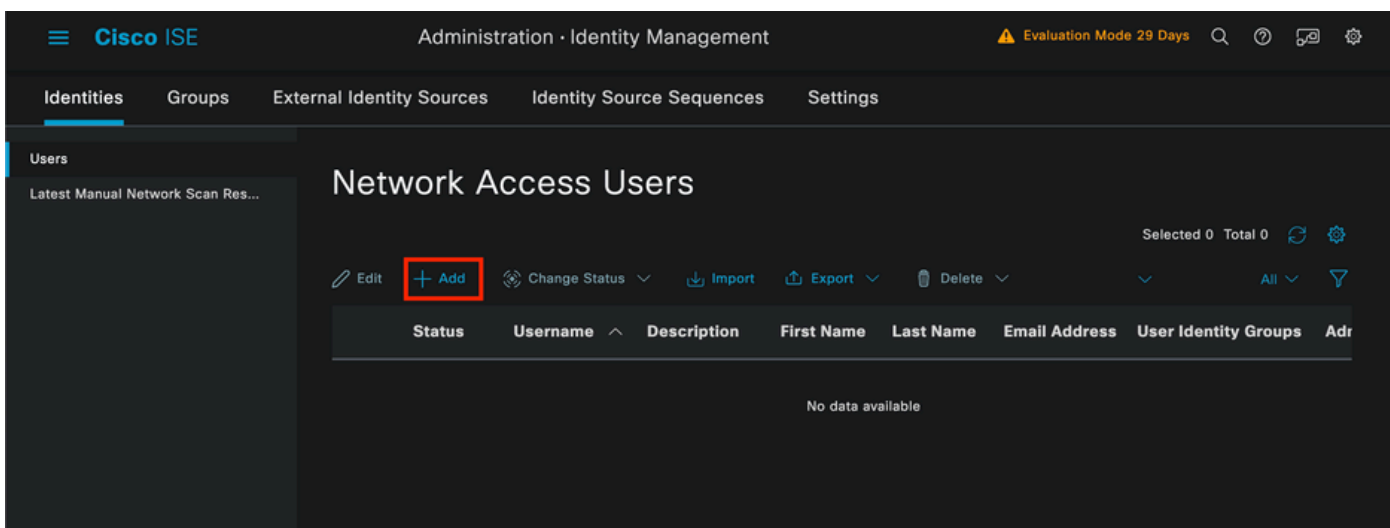


Création de groupe d'identités

Cliquez sur Submit.

Accédez à Administration > Gestion des identités > Onglet Identité.

Cliquez sur Add.



Section Utilisateurs d'accès réseau

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

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Création d'utilisateurs d'accès réseau

Attribuez un mot de passe à l'utilisateur. VainillaSE97 est utilisé.

Passwords

Password Type: ▼

Password Lifetime:

- With Expiration ⓘ
Password will expire in 60 days
- Never Expires ⓘ

Password

Re-Enter Password

* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Section Mot de passe de création utilisateur

Affectez l'utilisateur au groupe iseUsers.

User Groups

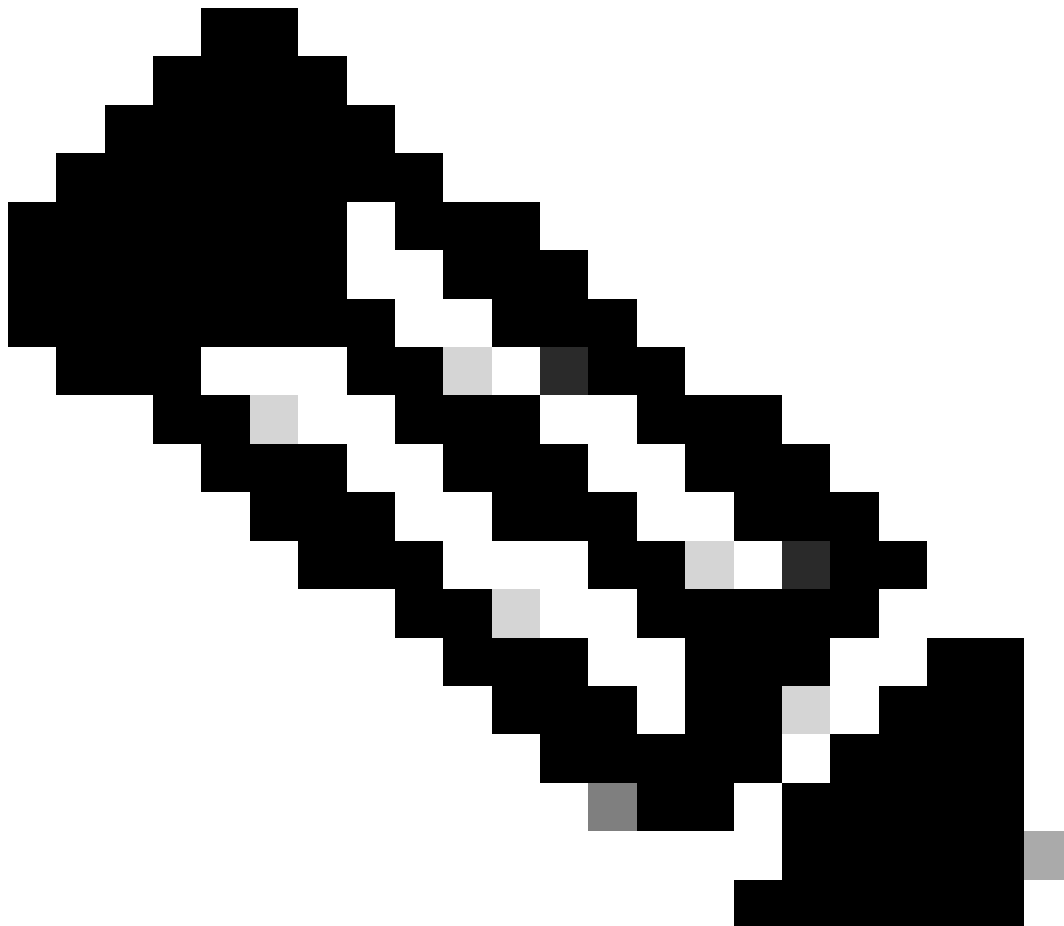
ⓘ +

Attribution de groupe d'utilisateurs

Configurez l'ensemble de stratégies.

Accédez au menu ISE > Policy > Policy Sets.

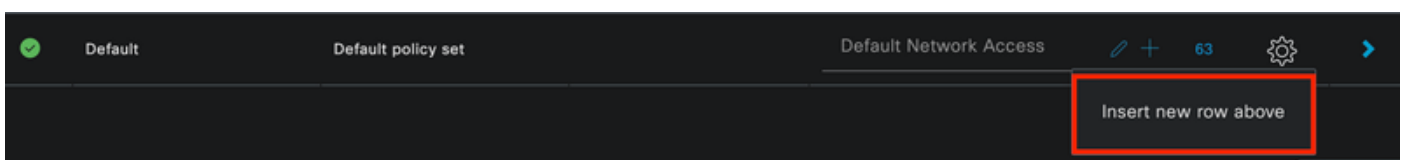
Le jeu de stratégies par défaut peut être utilisé. Cependant, un réseau appelé câblé est créé pour cet exemple.



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

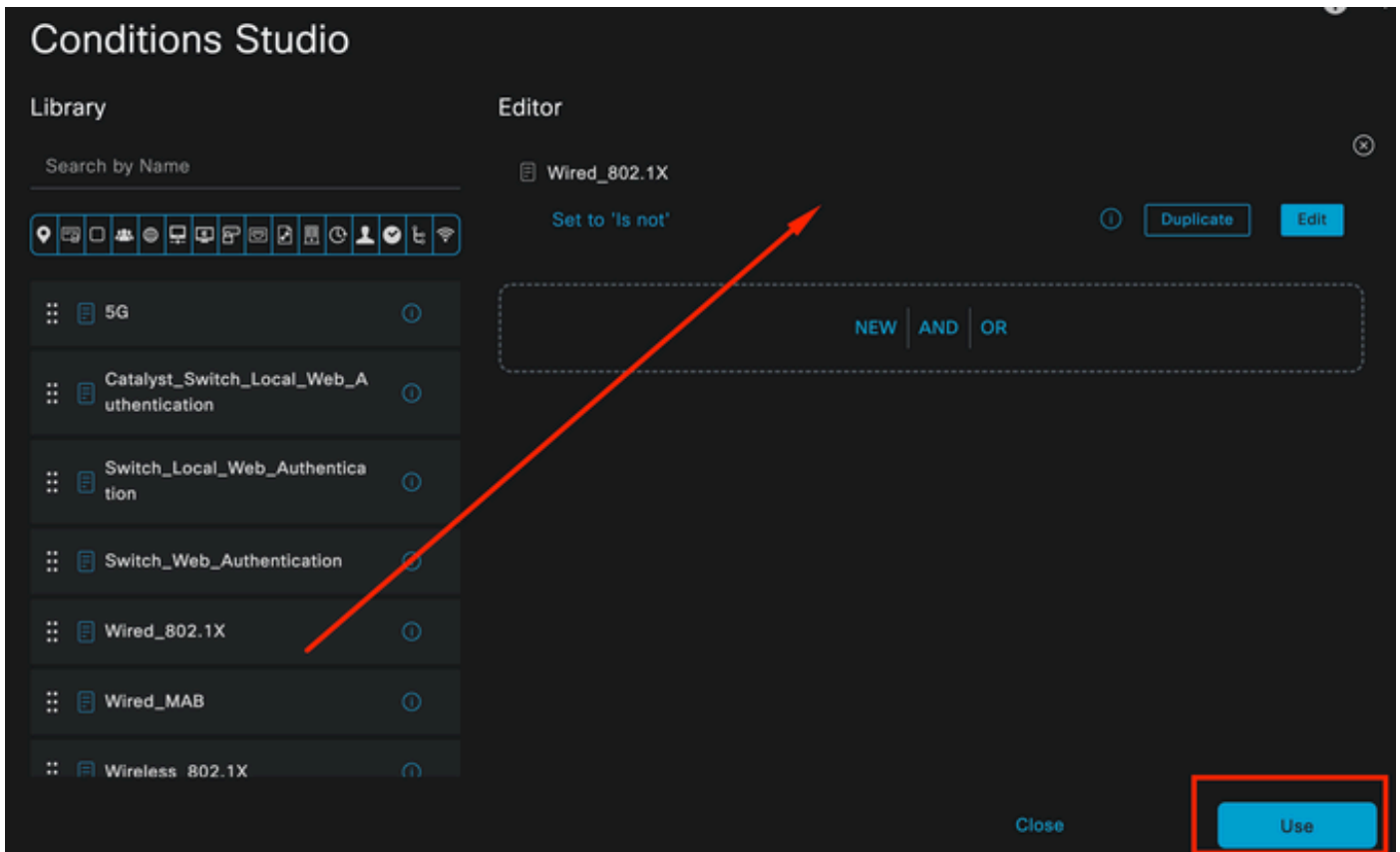


Remarque : si l'icône Ajouter ou Plus n'est pas visible, vous pouvez cliquer sur l'icône d'engrenage d'un jeu de stratégies, puis sélectionner Insérer une nouvelle ligne au-dessus.



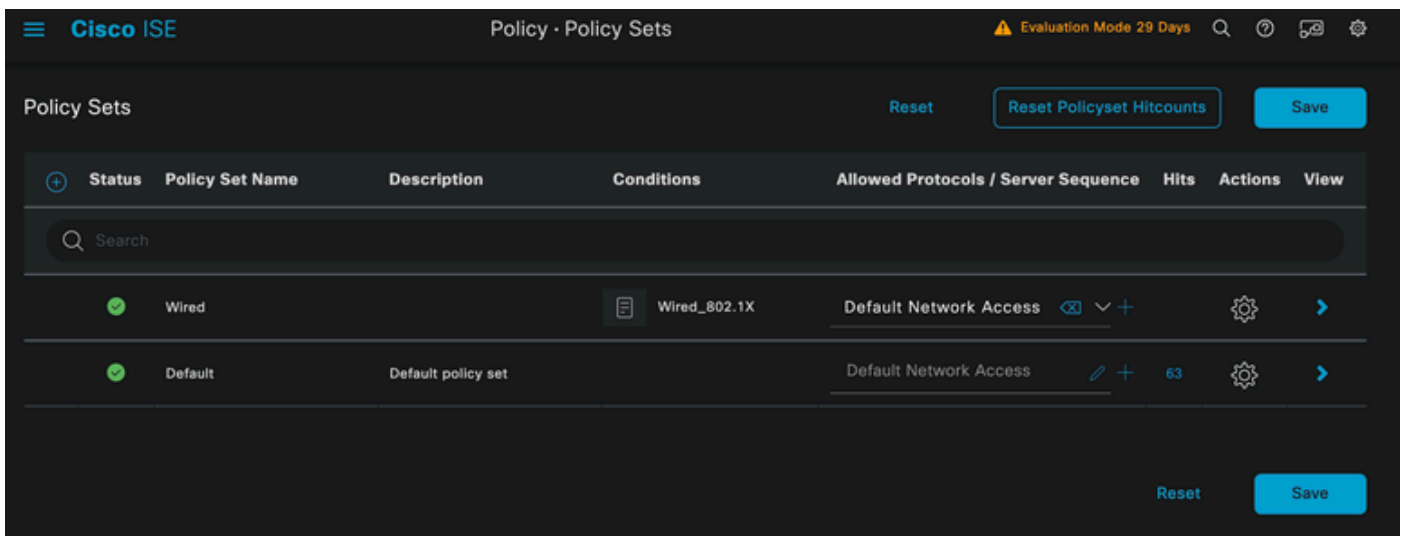
Options des icônes engrenage

La condition utilisée est Wired 8021x. Faites-le glisser, puis cliquez sur Utiliser.



Studio de condition de stratégie d'authentification

Sélectionnez Accès réseau par défaut dans la section Protocoles autorisés.



Vue générale Jeux de stratégies

Cliquez sur Save.

2.d. Configurez les stratégies d'authentification et d'autorisation.

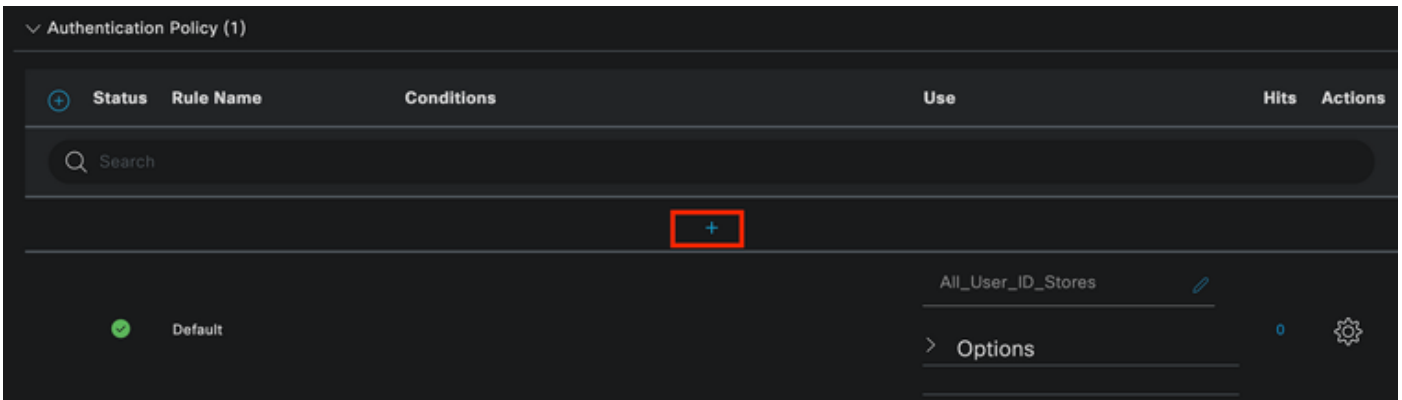
Cliquez sur l'icône >.



Ensemble de stratégies câblées

Développez la section Authentication Policy.

Cliquez sur l'icône +.



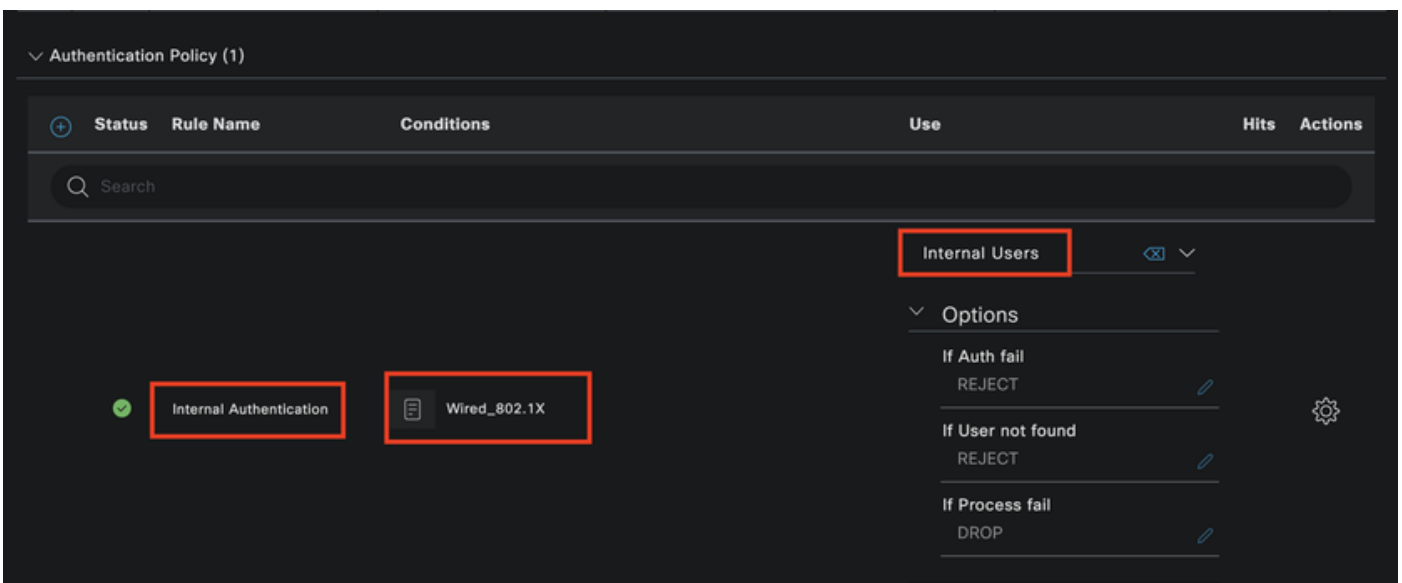
Stratégie d'authentification

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

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

La condition préconfigurée Wired Dot1x est utilisée.

Enfin, dans la colonne Use, sélectionnez Internal Users.



Stratégie d'authentification

Stratégie d'autorisation.

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

The screenshot shows the Cisco ISE Policy configuration interface. The page title is "Policy · Policy Sets". The top right corner indicates "Evaluation Mode 29 Days". The main content area is titled "Options" and shows a tree view with "Authorization Policy (1)" selected. Below this is a table with columns: Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. A search bar is present above the table. A red box highlights a "+" icon in the Conditions column. Below the table, there is a "DenyAccess" profile and a "Select from list" dropdown. At the bottom right, there are "Reset" and "Save" buttons.

Politique d'autorisation

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

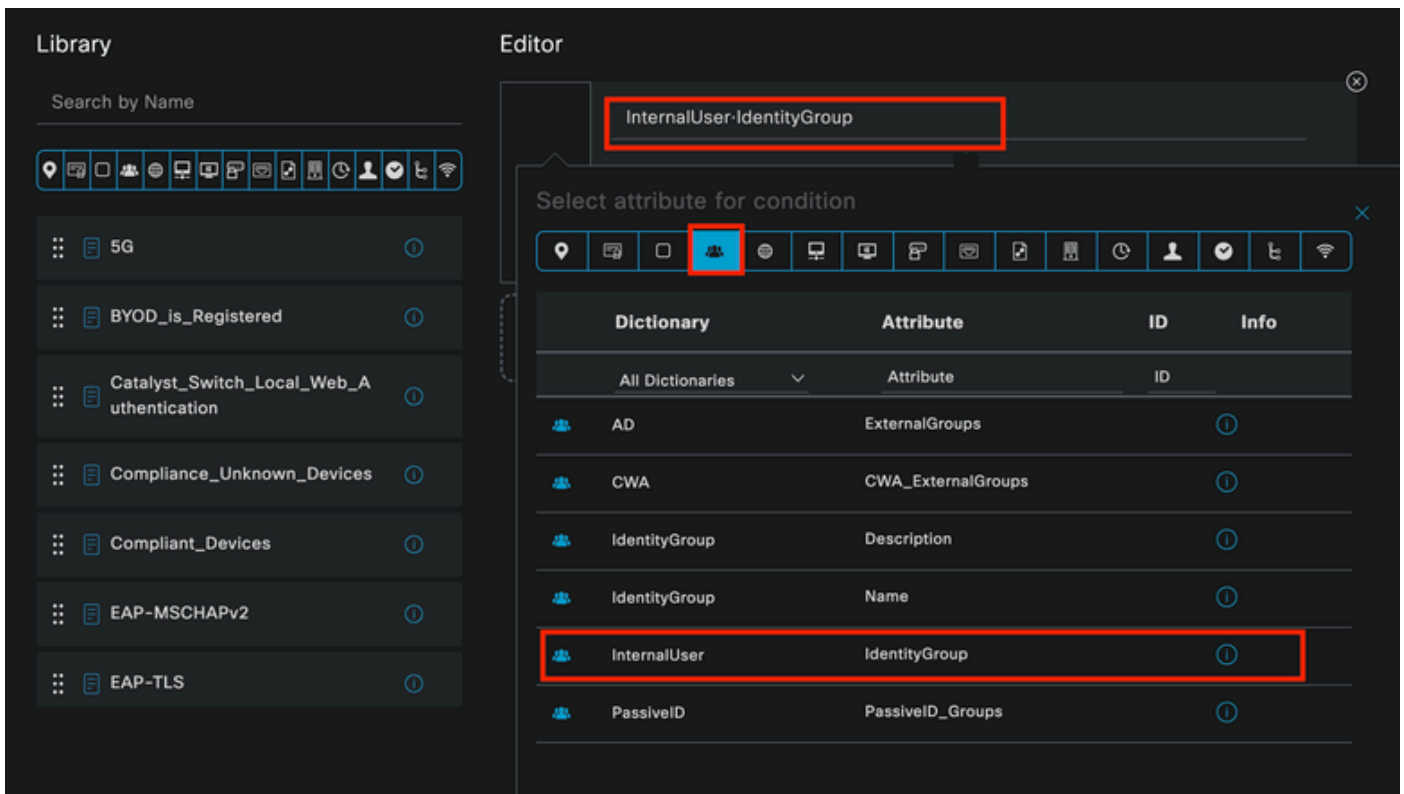
Pour créer une condition pour cette stratégie d'autorisation, cliquez sur l'icône + dans la colonne Conditions.

Le groupe IseUsers est utilisé.

Cliquez sur la section Attribut.

Sélectionnez l'icône IdentityGroup.

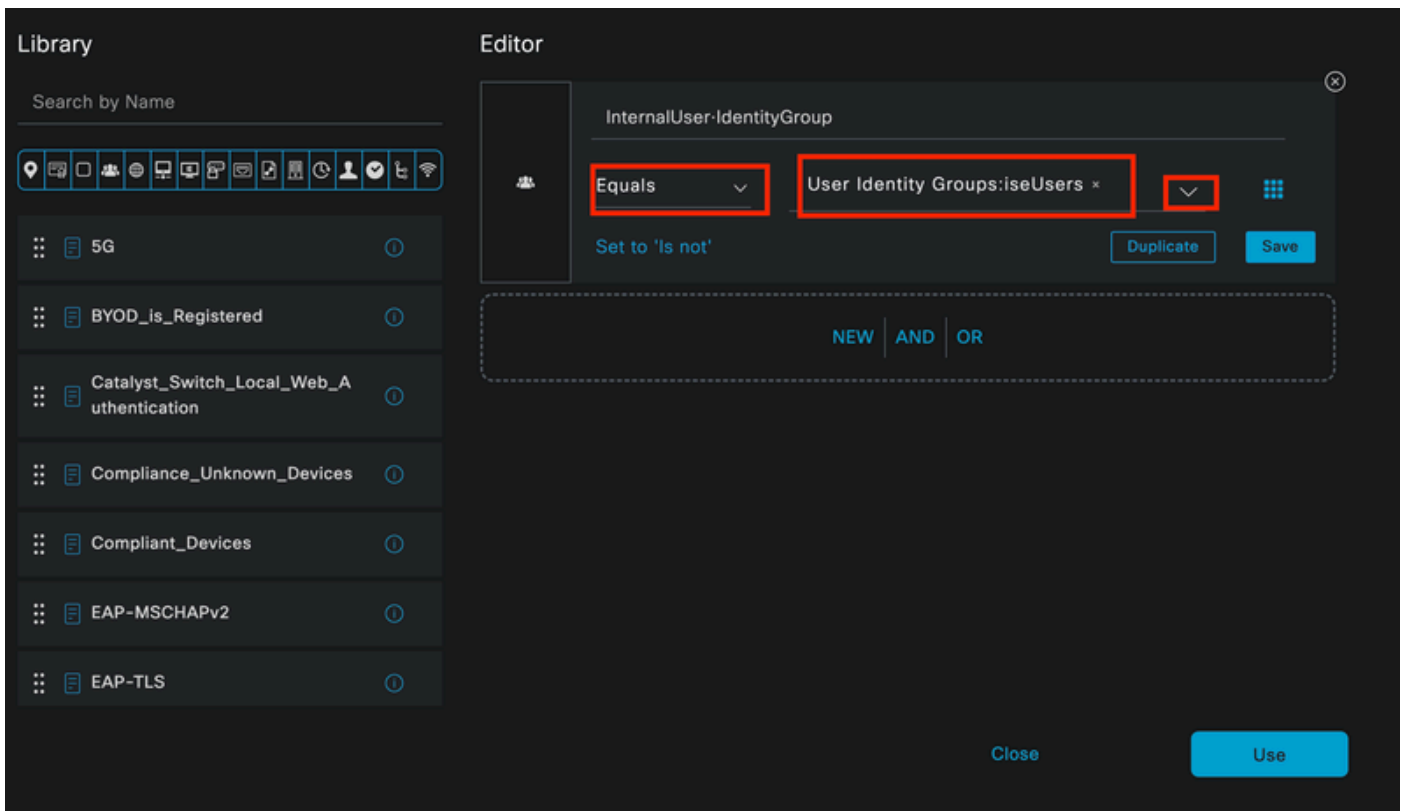
Dans le dictionnaire, sélectionnez le dictionnaire InternalUser fourni avec l'attribut IdentityGroup.



Création de condition

Sélectionnez l'opérateur Est égal à.

Dans Groupes d'identités d'utilisateur, sélectionnez le groupe IseUsers.

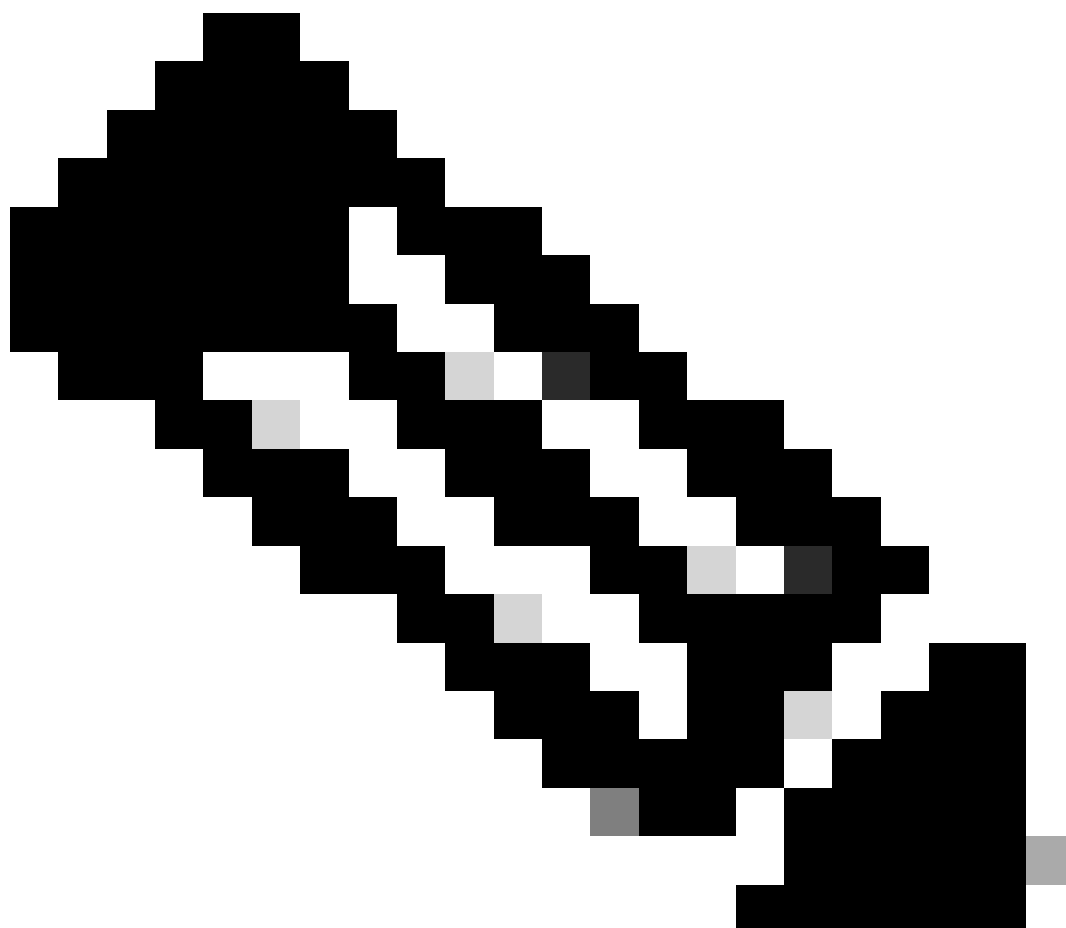


Création de condition

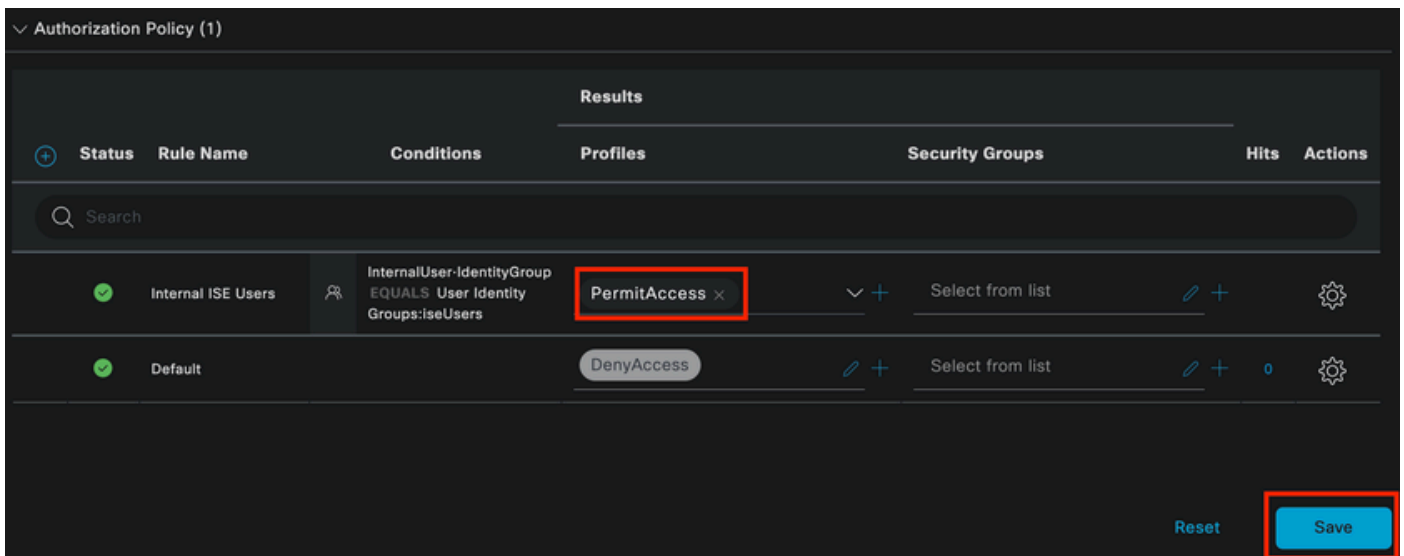
Cliquez sur Utiliser.

Ajoutez le profil d'autorisation des résultats.

Le profil préconfiguré Autoriser l'accès est utilisé.



Remarque : notez que les authentifications arrivant à ISE et atteignant cet ensemble de stratégies Wired Dot1x qui ne font pas partie des utilisateurs ISEUsers du groupe d'identité des utilisateurs, ont atteint la stratégie d'autorisation par défaut, qui a pour résultat DenyAccess.



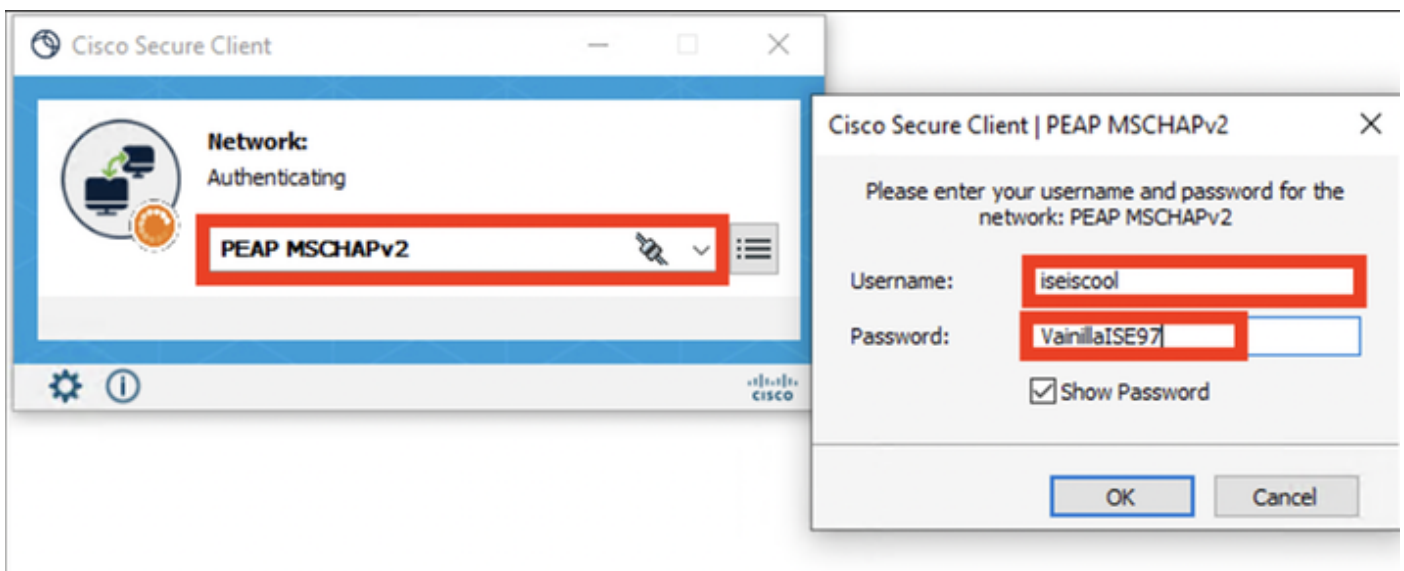
Politique d'autorisation

Cliquez sur Save.

Vérifier

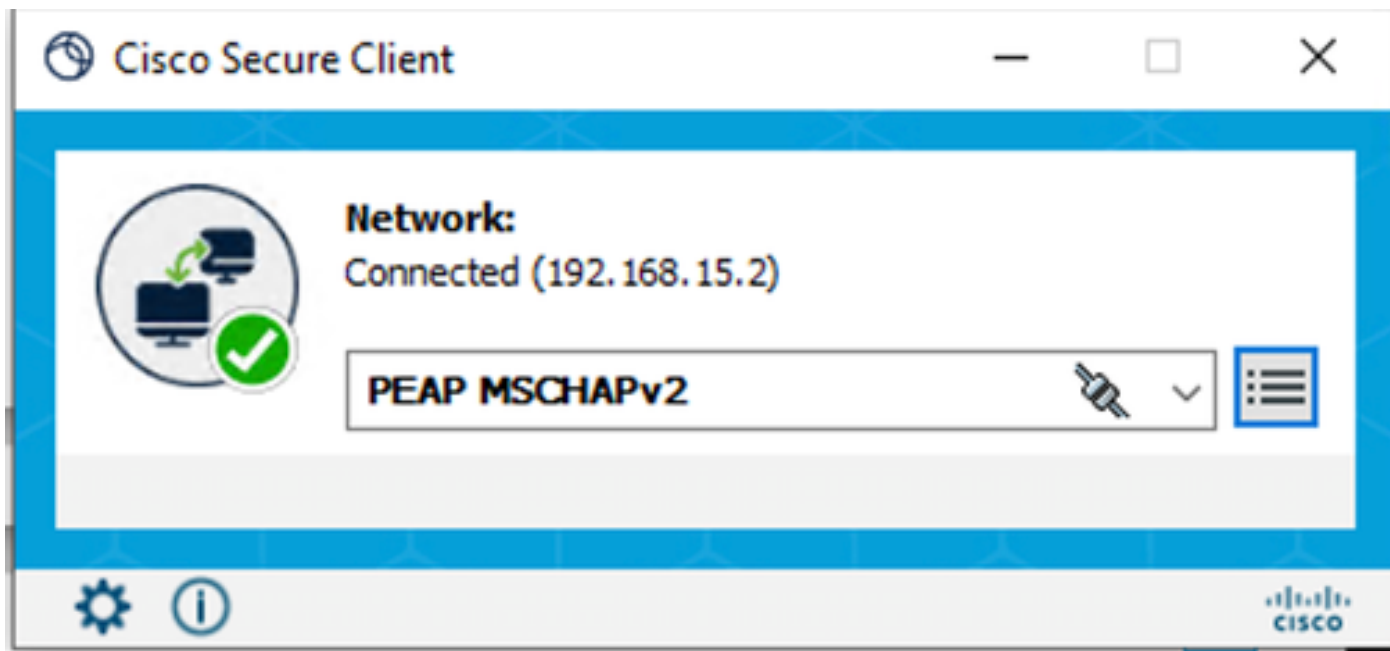
Une fois la configuration terminée, Secure Client demande les informations d'identification et spécifie l'utilisation du profil PEAP MSCHAPv2.

Les informations d'identification précédemment créées sont entrées.



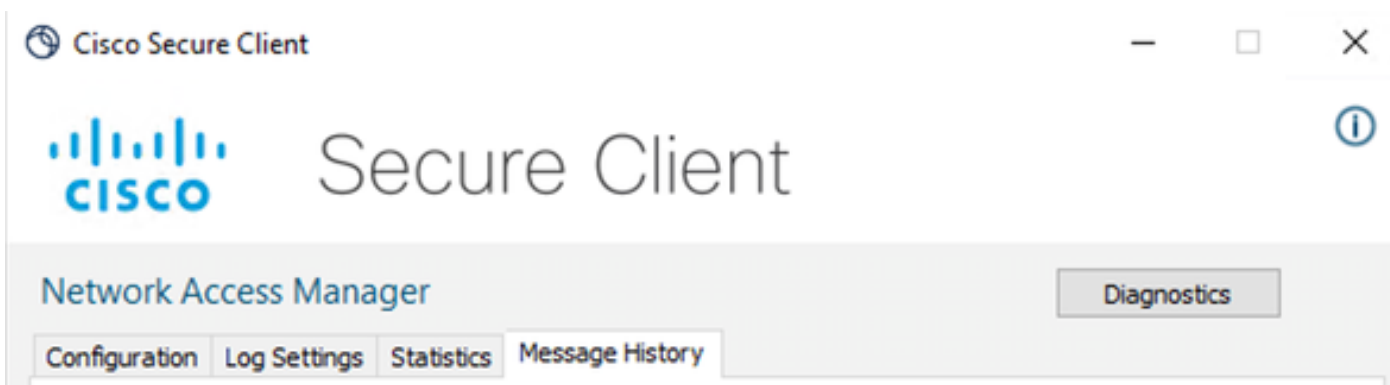
NAM du client sécurisé

Si le terminal s'authentifie correctement, NAM indique qu'il est connecté.



NAM du client sécurisé

En cliquant sur l'icône d'informations et en accédant à la section Historique des messages, les détails de chaque étape effectuée par NAM sont affichés.



Historique des messages du client sécurisé

```
7:06:01 PM PEAP MSCHAPv2 : Authenticating
7:06:21 PM PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM PEAP MSCHAPv2 : Connected
```

Historique des messages du client sécurisé

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 comme :

- Horodatage.
- Adresse Mac.
- Jeu de stratégies utilisé.
- Stratégie d'authentification.

- Stratégie d'autorisation.
- Autres informations pertinentes.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (25), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below the cards, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 5 minutes). A table of logs is displayed below, with columns for Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint..., Authentication Policy, Authorization Policy, Authoriz..., IP Address, and Network De... The table shows two records for the time 'Apr 23, 2024 06:38:07.0...' and 'Apr 23, 2024 06:38:06.8...'. The first record has a status of 'Success' and the second has a status of 'Success'. The table is updated as of 'Tue Apr 23 2024 13:02:14 GMT-0600 (Central Standard Time)' and shows 2 records.

Journaux en direct ISE RADIUS

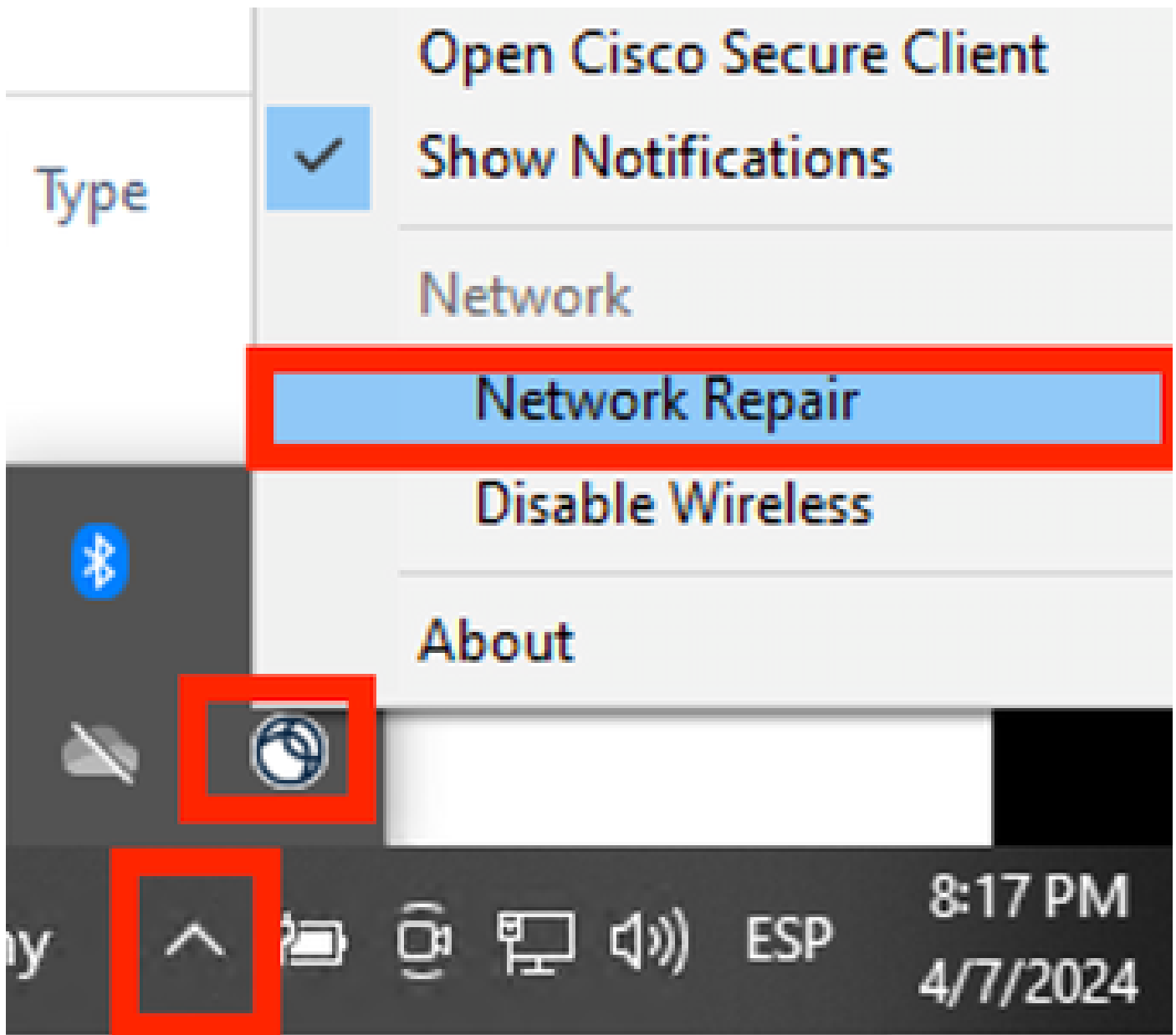
Comme vous pouvez voir qu'il applique les stratégies correctes et que le résultat est un état d'authentification réussi, il est conclu que la configuration est correcte.

Dépannage

Problème : le profil NAM n'est pas utilisé par le client sécurisé.

Si le nouveau profil qui a été créé dans l'éditeur de profil n'est pas utilisé par NAM, utilisez l'option Réparation du réseau pour Secure Client.

Vous pouvez trouver cette option en naviguant jusqu'à la barre Windows > en cliquant sur l'icône circumflex > Cliquez avec le bouton droit sur l'icône Secure Client > Cliquez sur Network Repair.



Section Réparation du réseau

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

1. Activer la journalisation étendue NAM

Ouvrez NAM, puis cliquez sur l'icône d'engrenage.



Interface NAM

Accédez à l'onglet Log Settings. Cochez la case Enable Extended Logging.

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



Network Access Manager Diagnostics

Configuration Log Settings Statistics Message History

Use extended logging to collect additional information about product operations.

Enable Extended Logging

IHV:

Filter Driver:

Credential Provider

Packet Capture

Maximum Packet Capture File Size (MB):

Paramètres du journal NAM du client sécurisé

2. Reproduisez la question.

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.

3. Collectez l'offre groupée Secure Client DART.

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



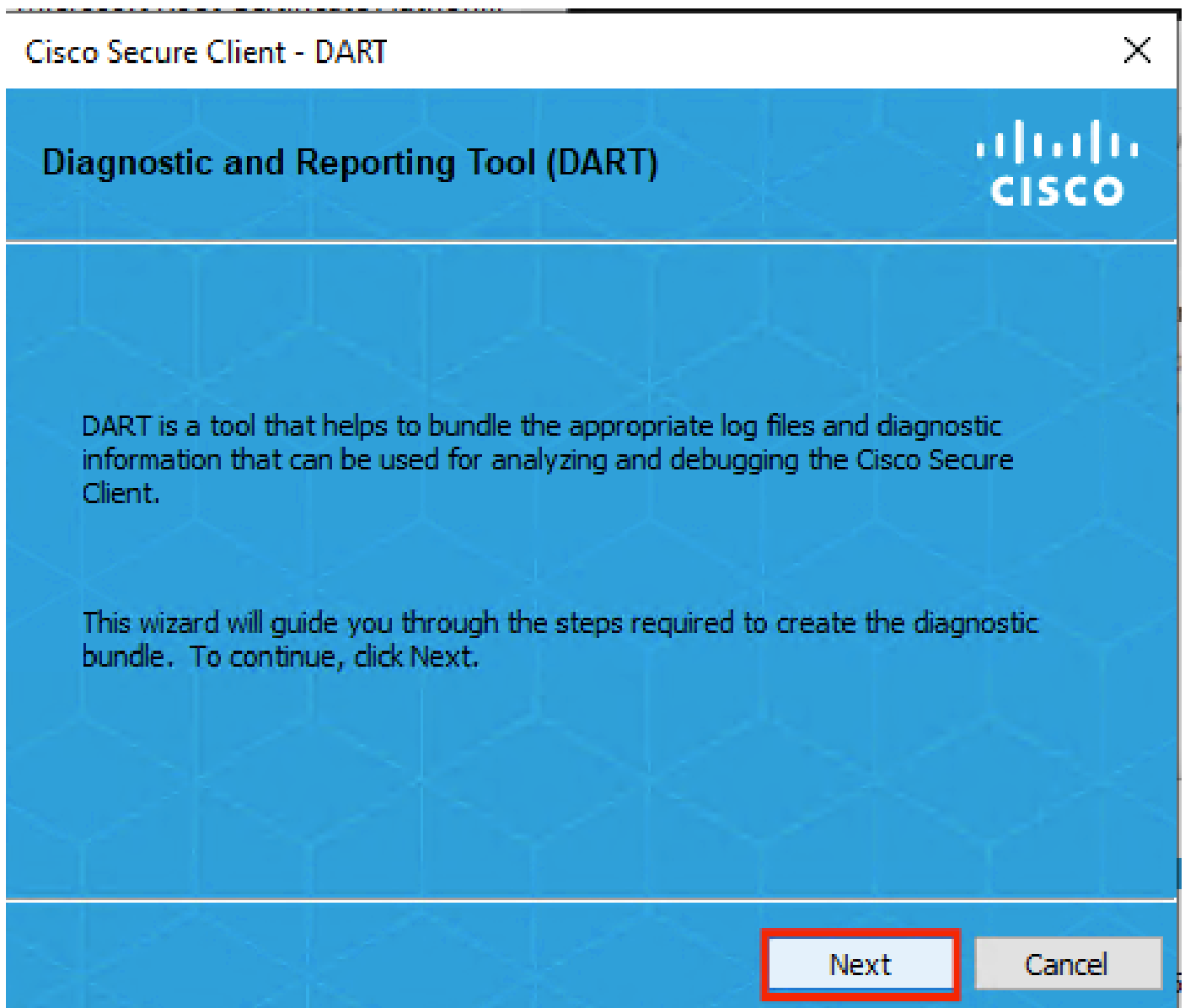
Cisco Secure Client Diagnostics and Reporting Tool

App

Module DART

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

Cliquez sur Next dans la première fenêtre.




Module DART

Cliquez à nouveau sur Next, afin que le lot de journaux puisse être enregistré sur le bureau.

Cisco Secure Client - DART




Bundle Creation Option 

Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

Default - Bundle will be saved to Desktop

Custom

 DART requires administrative privileges to clear Cisco Secure Client logs.

[Clear All Logs](#)

[Back](#) [Next](#) [Cancel](#)

Module DART

Si nécessaire, cochez la case Enable Bundle Encryption.



Bundle Encryption Option



Enable Bundle Encryption

Mask Password

Encryption Password

Confirm Password

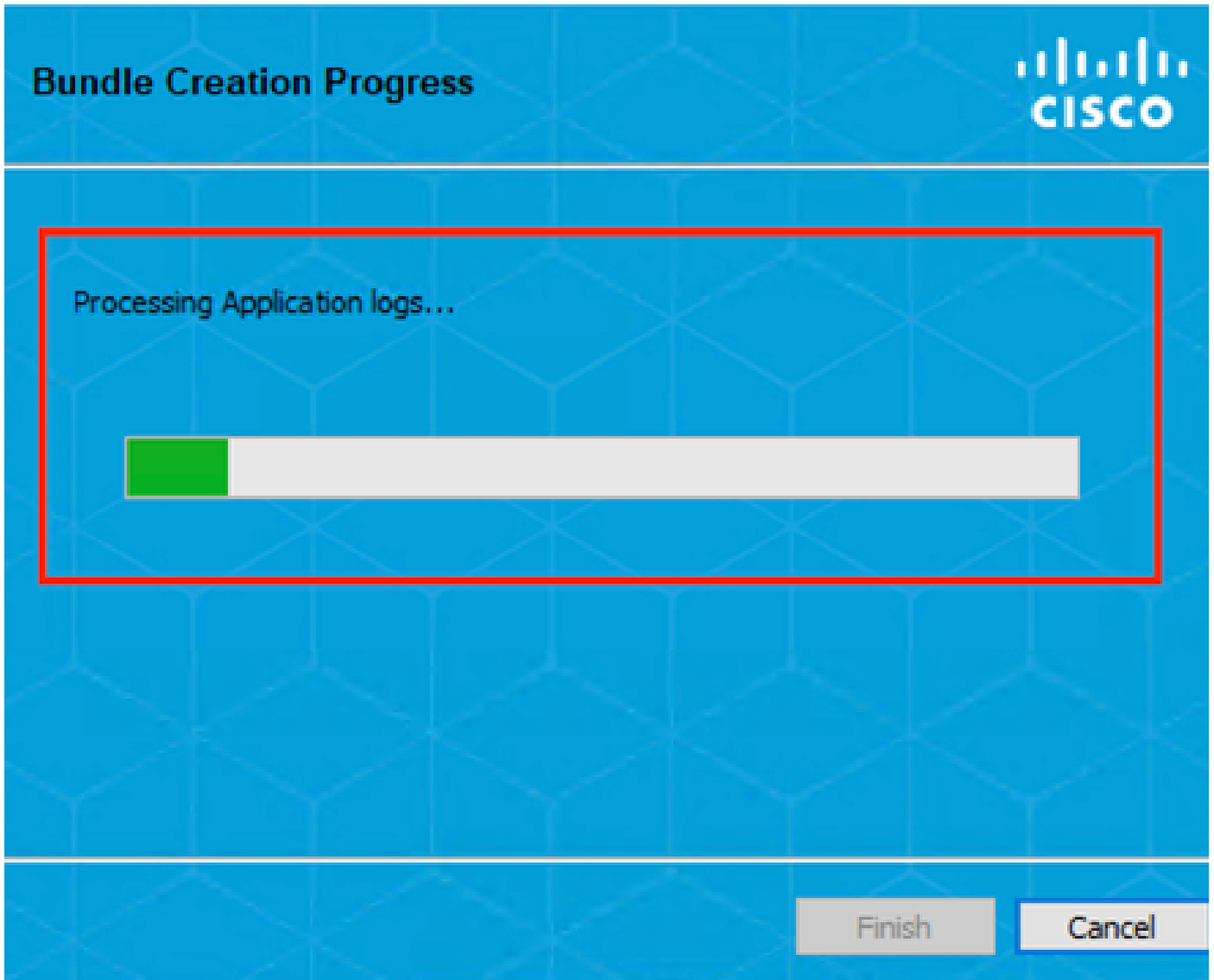
Back

Next

Cancel

Module DART

La collecte du journal DART démarre.



The image shows a dialog box titled "Bundle Creation Progress" with the Cisco logo in the top right corner. The main content area is highlighted with a red border and contains the text "Processing Application logs..." above a progress bar. The progress bar is approximately 10% complete, with a green segment on the left. At the bottom right, there are two buttons: "Finish" and "Cancel".

DART Log Collection

Cela peut prendre 10 minutes ou plus jusqu'à la fin du processus.

Bundle Creation Result




The bundle was created successfully in C:\Users\LAB5\Desktop\DARTBundle_0423_1538.zip.

[Email Bundle](#)[Finish](#)

Résultat de la création du bundle DART

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

Name	Date modified	Type
 DARTBundle_0423_1538	4/24/2024 1:14 PM	Compressed (zipped) Folder

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.

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.