Configuration de l'authentification des ordinateurs et des utilisateurs avec EAP-TTLS

Table des matières

Introduction

Ce document décrit comment configurer l'authentification de l'ordinateur et de l'utilisateur avec EAP-TTLS (EAP-MSCHAPv2) sur le NAM du client sécurisé et Cisco ISE.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance de ces sujets avant de procéder à ce déploiement :

- Cisco Identity Services Engine (ISE)
- Module NAM (Secure Client Network Analysis Module)
- Protocoles EAP

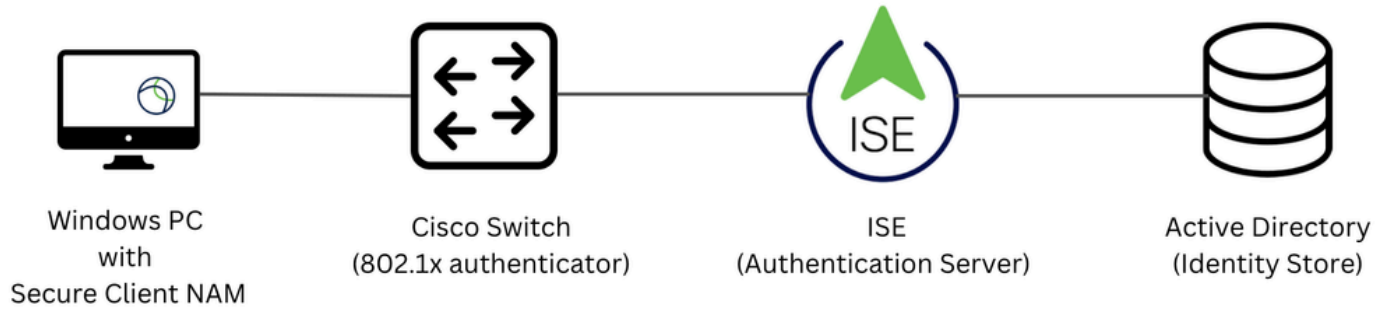
Composants utilisés

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

- Identity Services Engine (ISE) version 3.4
- Commutateur C9300 avec logiciel Cisco IOS® XE, version 16.12.01
- Windows 10 Professionnel Version 22H2 Construit 19045.3930

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.

Topologie du réseau



Topologie du réseau

Configurer

Configurations

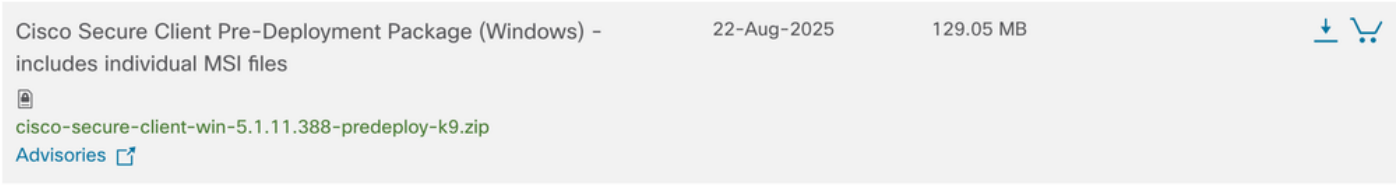
Partie 1 : Télécharger et installer le NAM (Network Access Manager) du client sécurisé

Étape 1. Accédez à Téléchargement de logiciels Cisco. Dans la barre de recherche de produits, saisissez Secure Client 5.

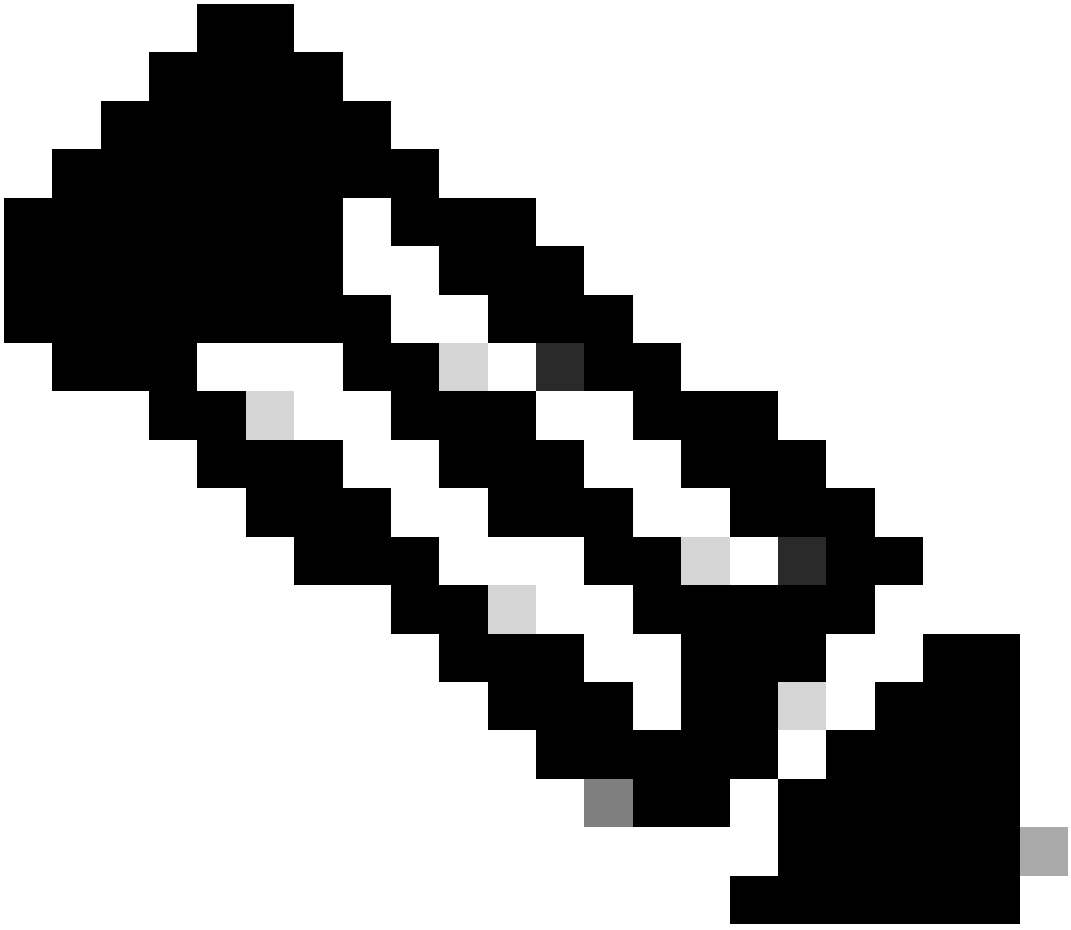
Cet exemple de configuration utilise la version 5.1.11.388. L'installation est effectuée à l'aide de la

méthode de pré-déploiement.

Sur la page de téléchargement, localisez et téléchargez Cisco Secure Client Pre-Deployment Package (Windows).

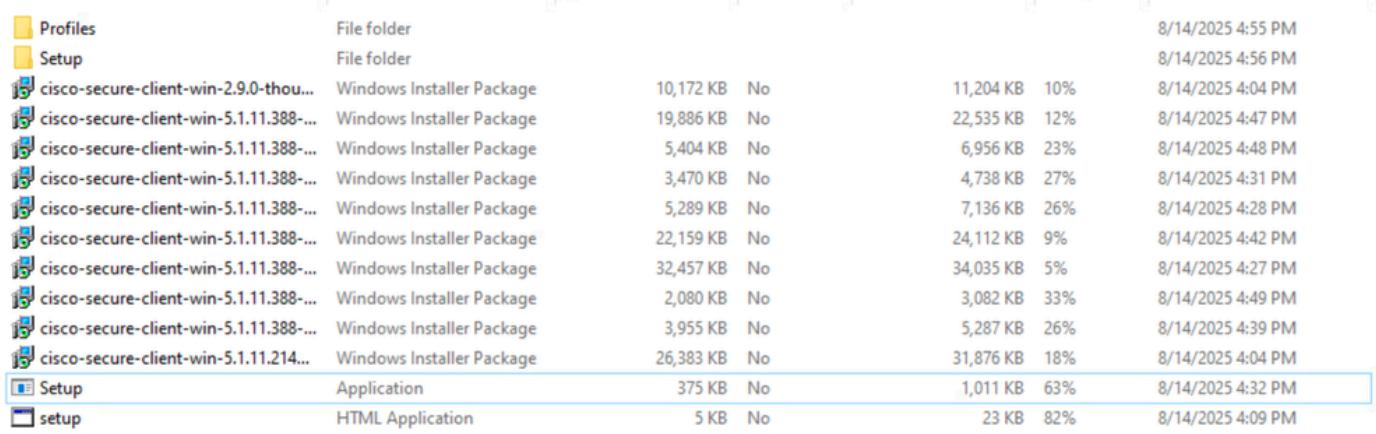


Fichier zip de prédéploiement



Remarque : Cisco AnyConnect est obsolète et n'est plus disponible sur le site de téléchargement de logiciels Cisco.

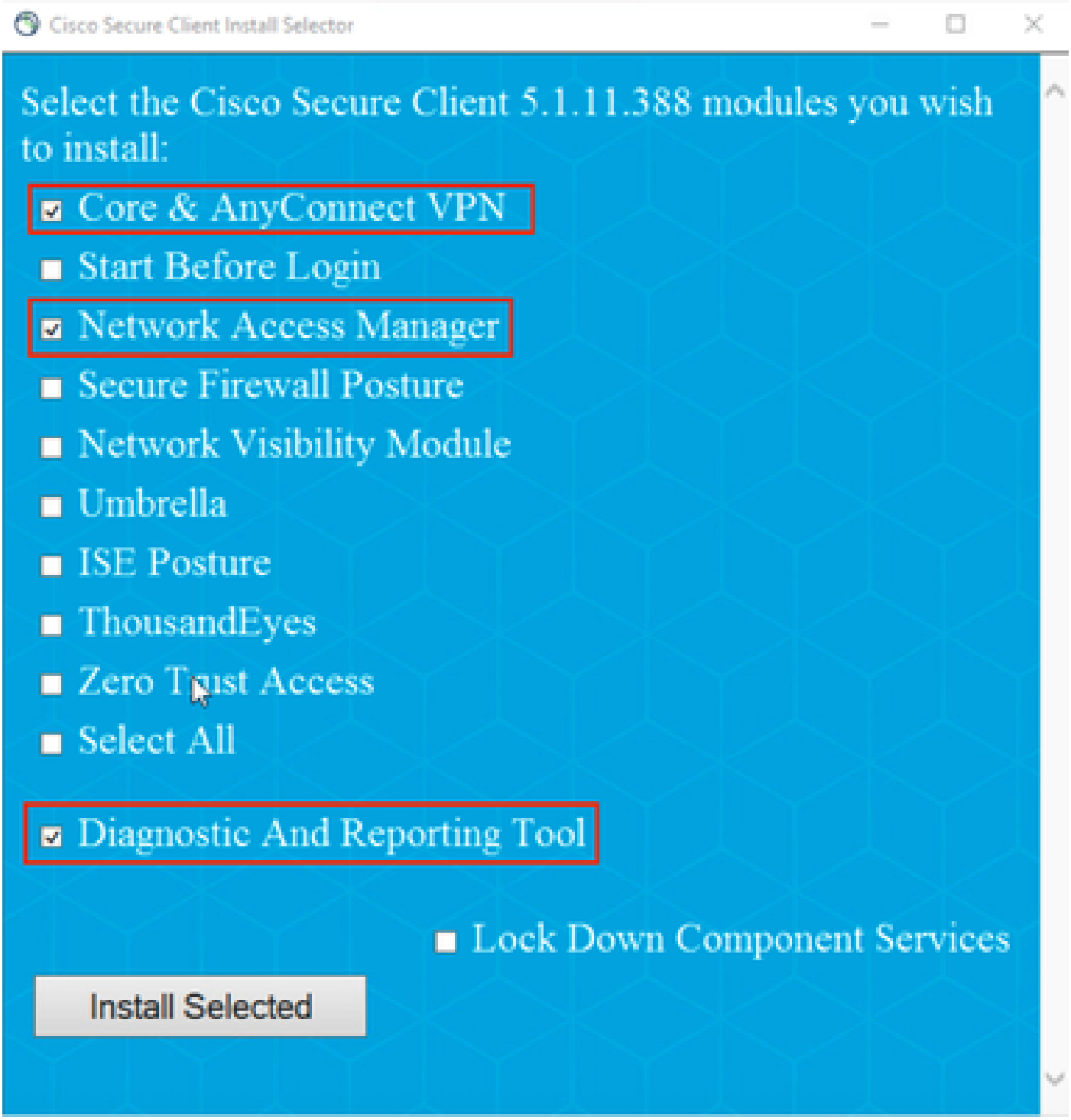
Étape 2. Une fois téléchargé et extrait, cliquez sur Setup.



Profiles	File folder					8/14/2025 4:55 PM
Setup	File folder					8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%	8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%	8/14/2025 4:47 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,404 KB	No	6,956 KB	23%	8/14/2025 4:48 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,470 KB	No	4,738 KB	27%	8/14/2025 4:31 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,289 KB	No	7,136 KB	26%	8/14/2025 4:28 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	22,159 KB	No	24,112 KB	9%	8/14/2025 4:42 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	32,457 KB	No	34,035 KB	5%	8/14/2025 4:27 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	2,080 KB	No	3,082 KB	33%	8/14/2025 4:49 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,955 KB	No	5,287 KB	26%	8/14/2025 4:39 PM
cisco-secure-client-win-5.1.11.214...	Windows Installer Package	26,383 KB	No	31,876 KB	18%	8/14/2025 4:04 PM
Setup	Application	375 KB	No	1,011 KB	63%	8/14/2025 4:32 PM
setup	HTML Application	5 KB	No	23 KB	82%	8/14/2025 4:09 PM

Fichier Zip De Prédéploiement

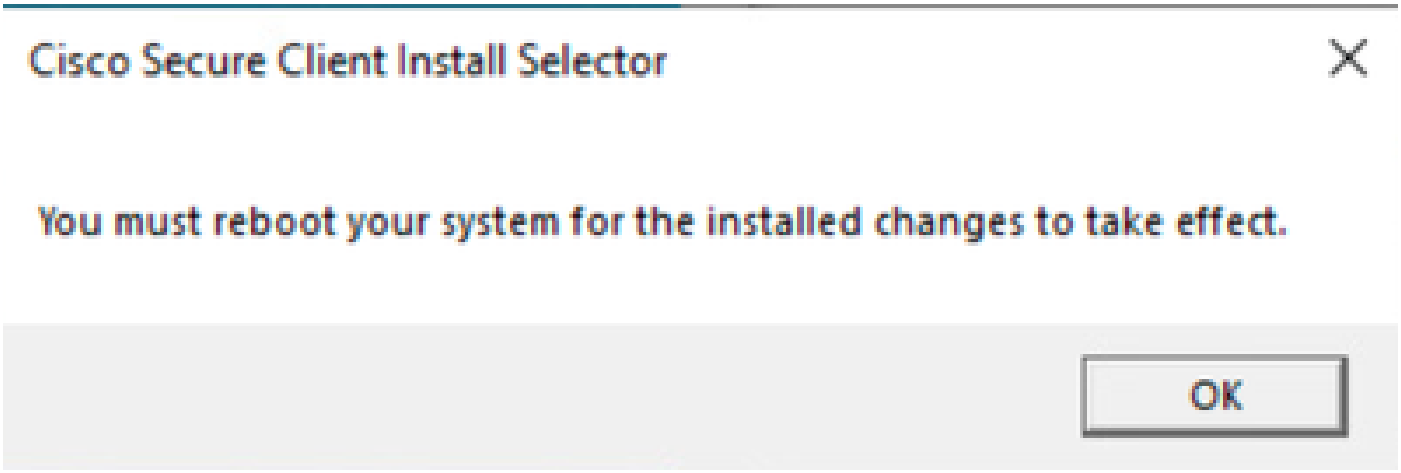
Étape 3 : installation des modules VPN Core et AnyConnect, Network Access Manager et des outils de diagnostic et de création de rapports



Installation du client sécurisé

Cliquez sur Instal Selected.

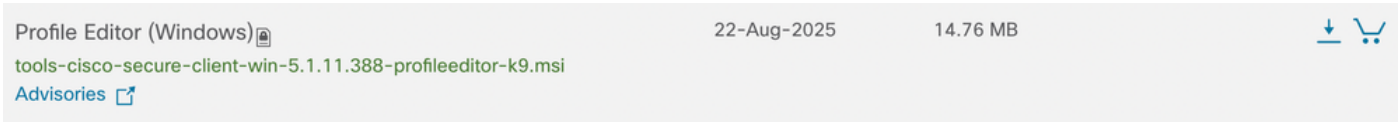
Étape 4. Un redémarrage est nécessaire après l'installation. Cliquez sur OK et redémarrez votre périphérique.



Fenêtre contextuelle Redémarrage requis

Partie 2 : Télécharger et installer Secure Client NAM Profile Editor

Étape 1. L'Éditeur de profil se trouve sur la même page de téléchargement que le client sécurisé. Cet exemple de configuration utilise la version 5.1.11.388.



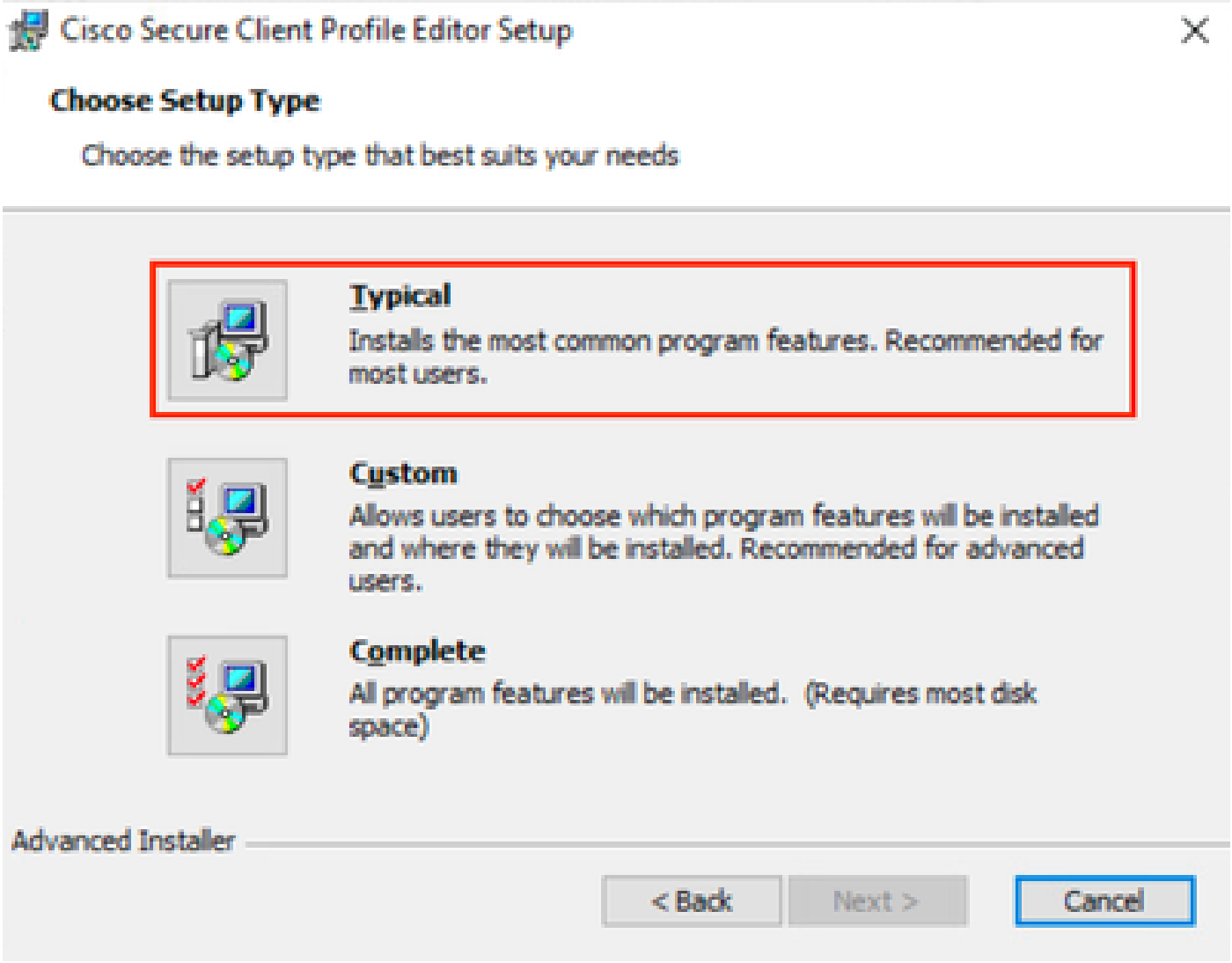
Éditeur de profil

Téléchargez et installez l'Éditeur de profil.

Étape 2 : exécution du fichier MSI

Démarrage de la configuration de Profile Editor

Étape 3. Utilisez l'option Typical setup et installez l'Éditeur de profil NAM.

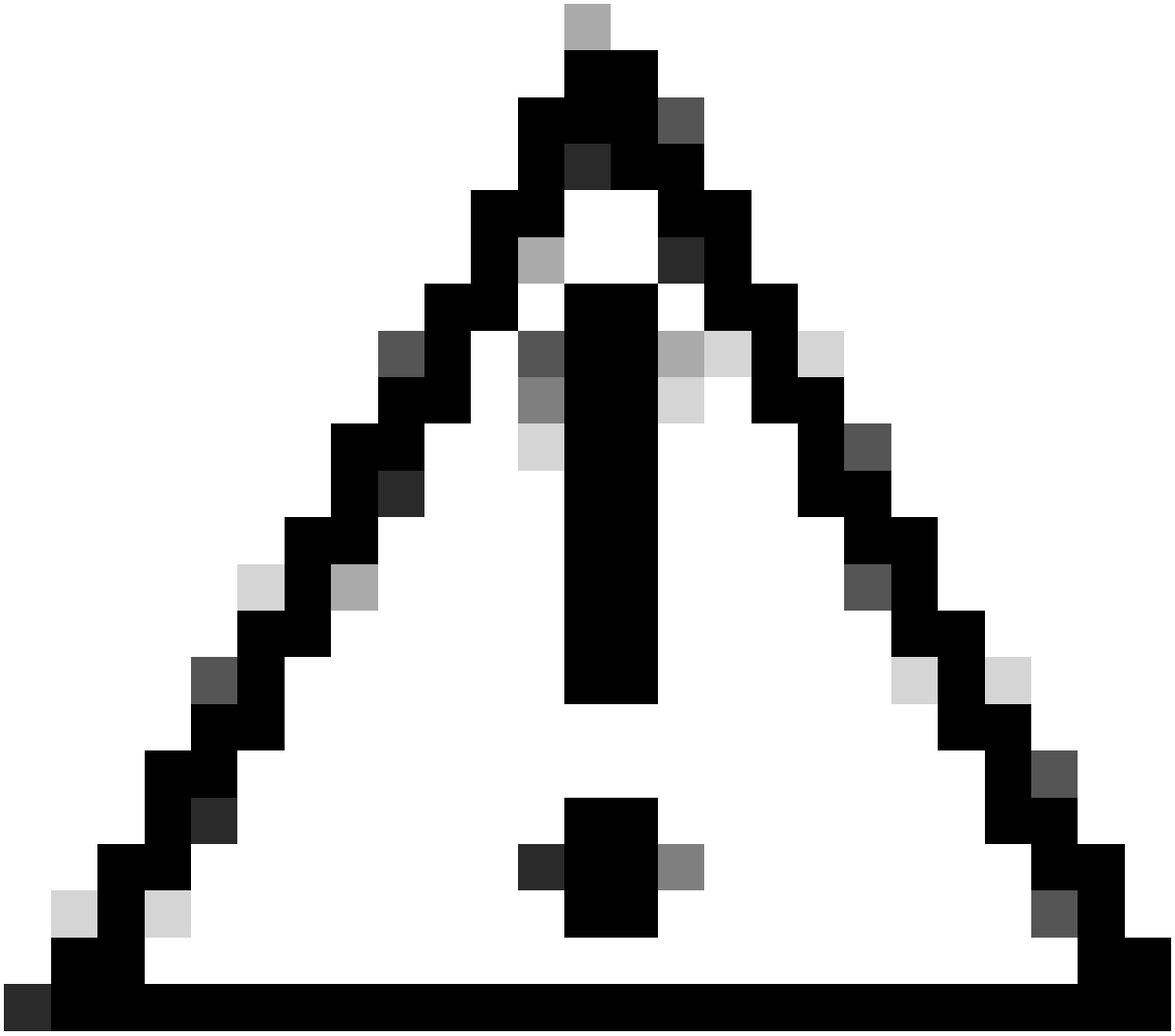


Configuration de Profile Editor

Partie 3 : Autoriser NAM à accéder aux informations d'identification du cache Windows

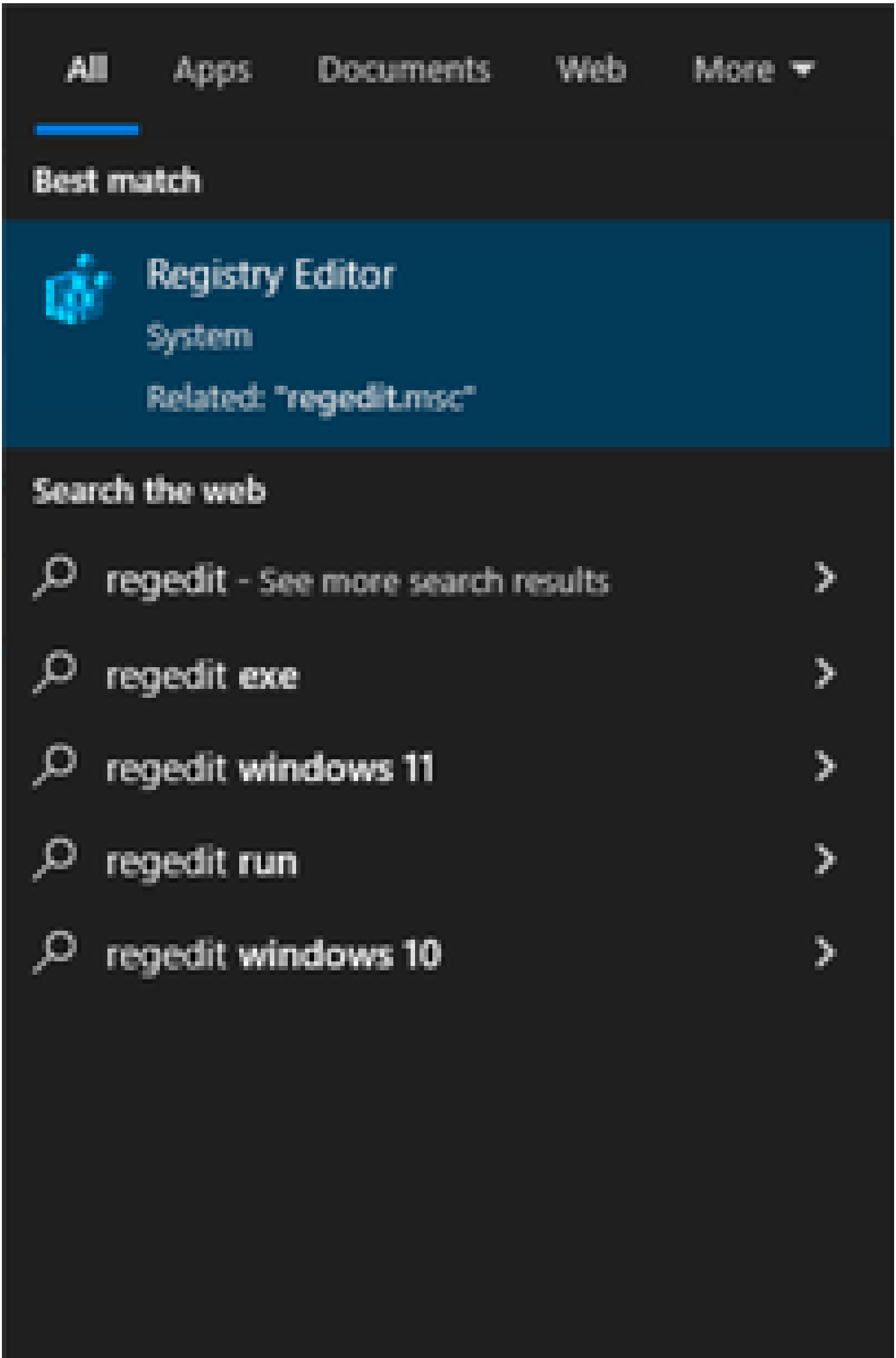
Par défaut, sous Windows 10, Windows 11 et Windows Server 2012, le système d'exploitation empêche le Gestionnaire d'accès réseau (NAM) de récupérer le mot de passe machine requis pour l'authentification machine. Par conséquent, l'authentification de l'ordinateur à l'aide du mot de passe de l'ordinateur ne fonctionne pas sauf si un correctif de Registre est appliqué.

Pour permettre à NAM d'accéder aux informations d'identification de l'ordinateur, appliquez le correctif Microsoft KB 2743127 sur le bureau du client.



Mise en garde : Une modification incorrecte du registre Windows peut entraîner de graves problèmes. Assurez-vous de sauvegarder le Registre avant d'effectuer des modifications.

Étape 1. Dans la barre de recherche Windows, entrez regedit, puis cliquez sur Éditeur du Registre.

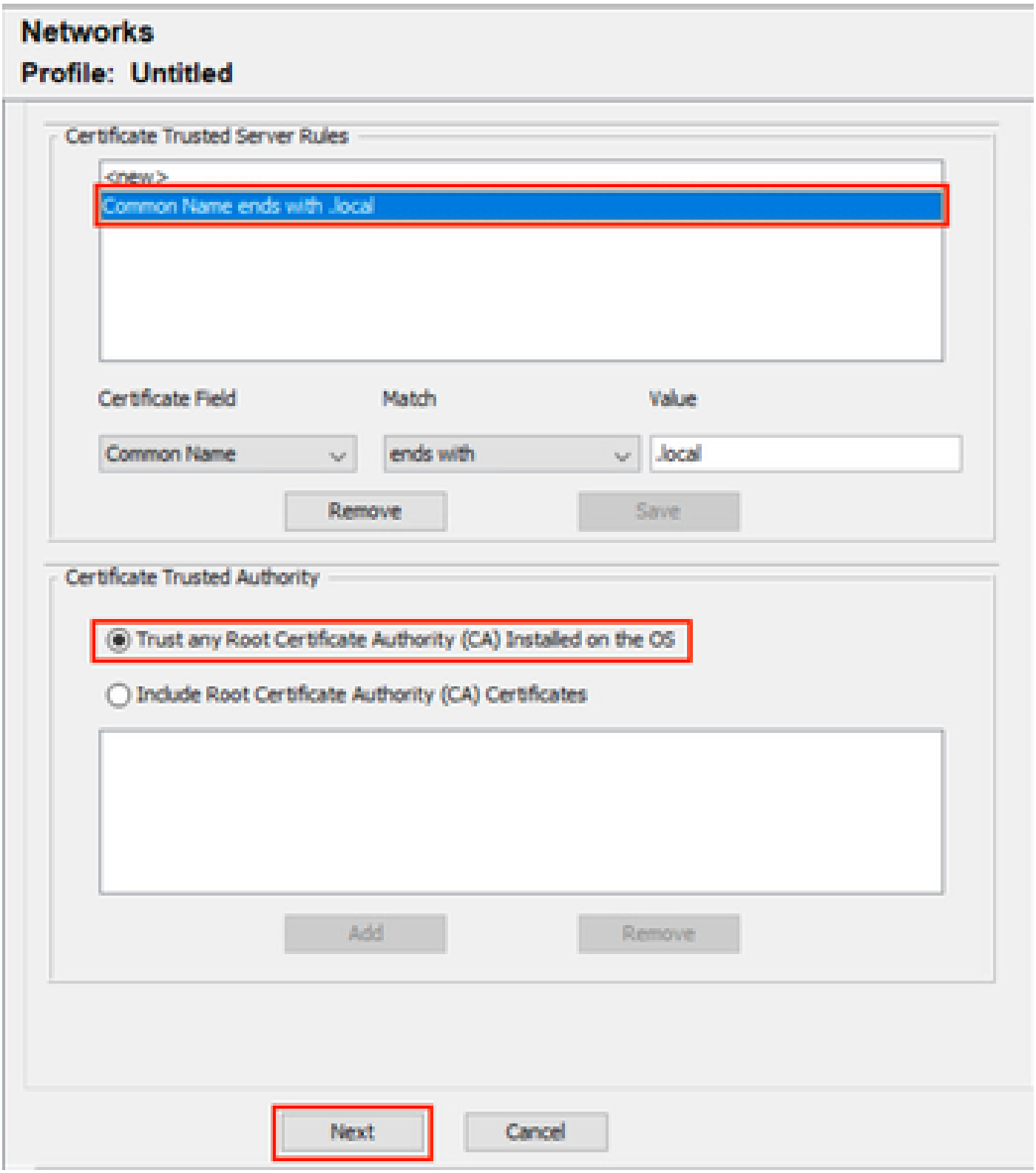

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

Dans cet exemple, le certificat de noeud PSN est émis par varshaah.varshaah.local. Par conséquent, la règle Nom commun se termine par .local est utilisée. Cette règle valide le certificat que le serveur présente pendant le flux EAP-TTLS.

Vous pouvez également spécifier le nom commun du certificat d'authentification EAP PSN (Policy Service Node).

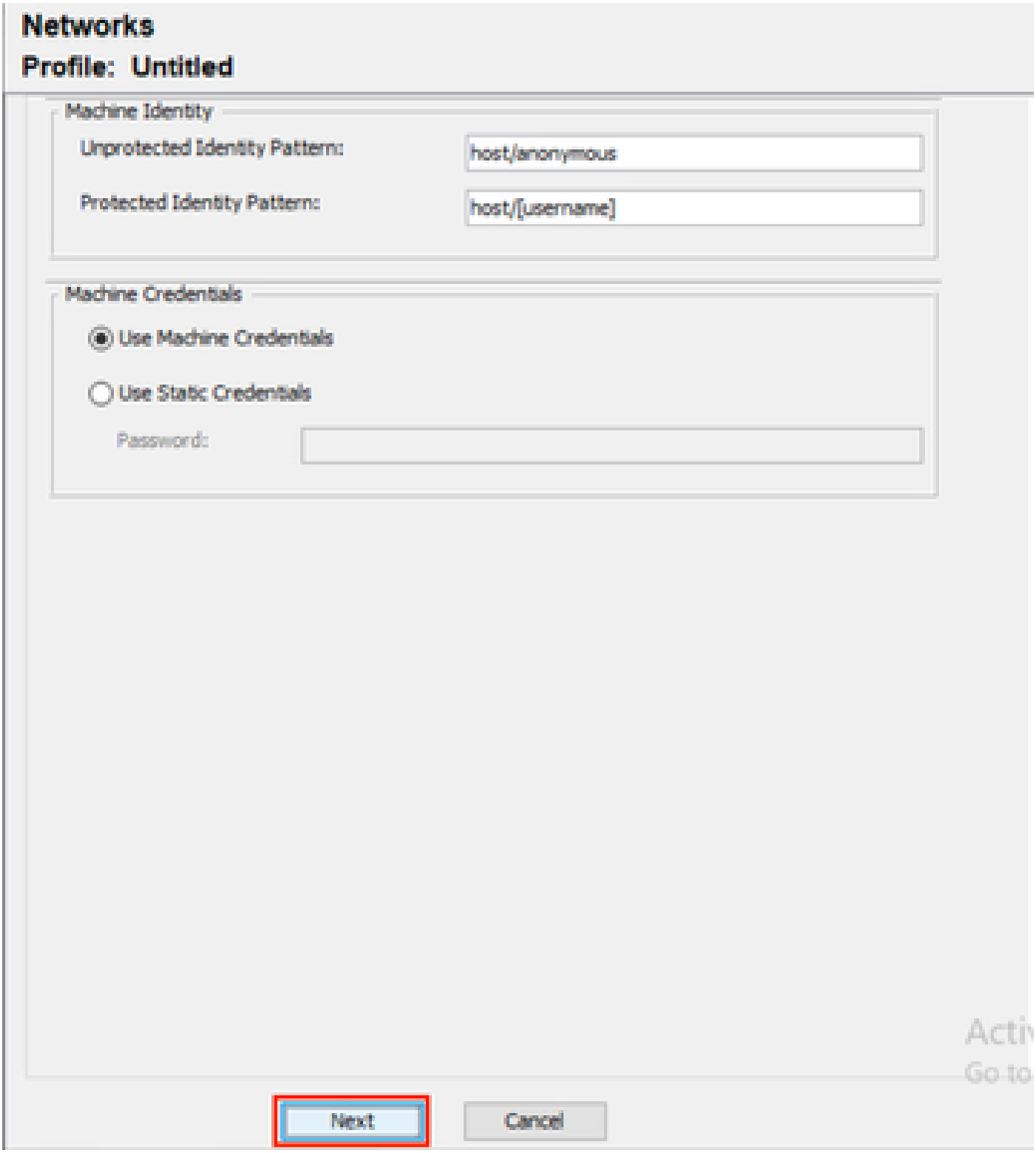
- Deux options sont disponibles sous Certificate Trusted Authority.
  Dans ce scénario, l'option Trust any Root Certificate Authority (CA) installée sur le système d'exploitation est utilisée au lieu d'ajouter un certificat CA spécifique.

  Avec cette option, le périphérique Windows approuve tout certificat EAP signé par un certificat inclus dans Certificats - Utilisateur actuel > Autorités de certification racines de confiance > Certificats (géré par le système d'exploitation).
- Cliquez sur Next pour continuer.



Certificats NAM Profile Editor

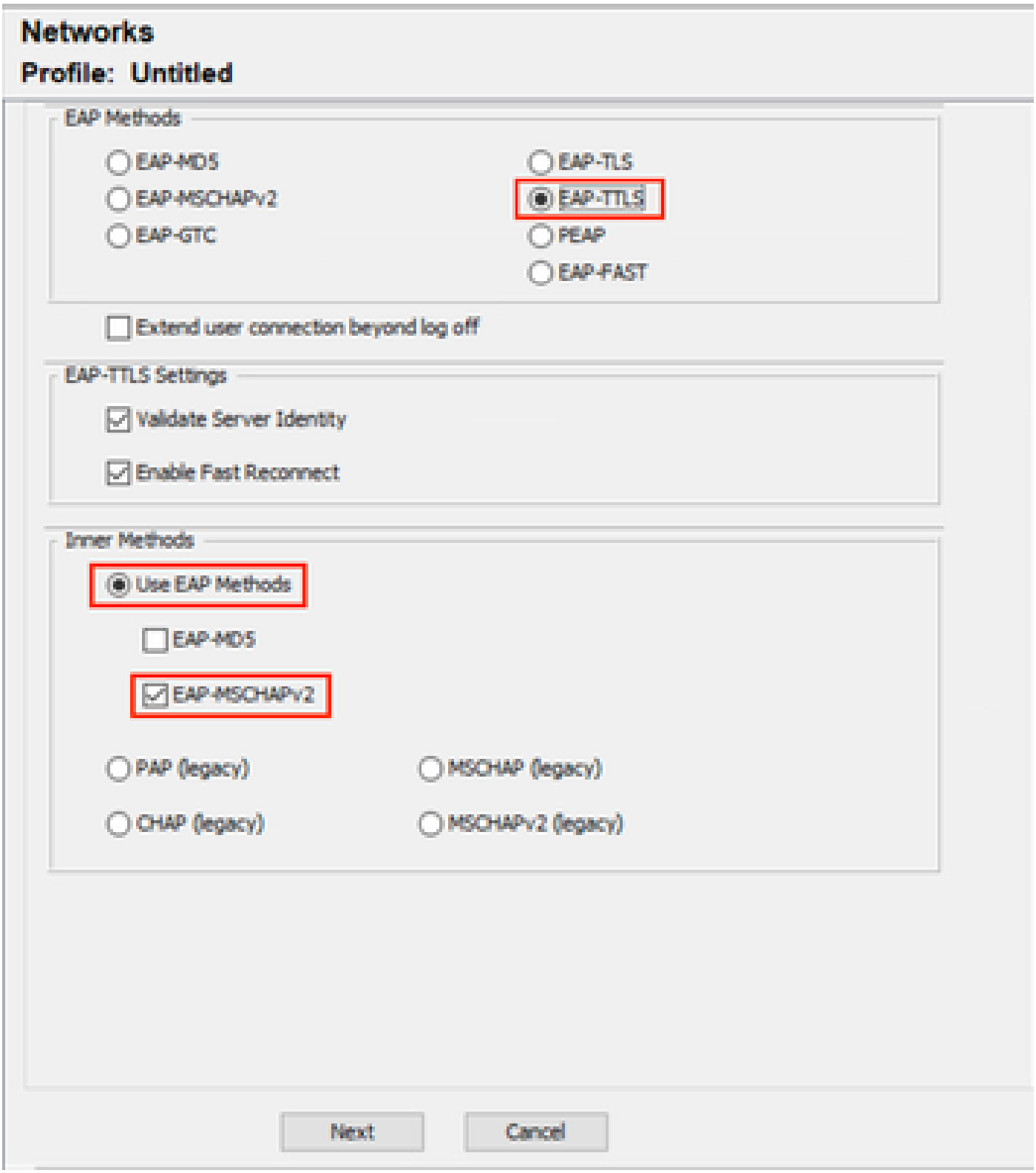
Étape 6. Dans la section Informations d'identification de la machine, sélectionnez Utiliser les informations d'identification de la machine, puis cliquez sur Suivant.



Informations d'identification NAM Profile Editor

Étape 7 : configuration de la section User Auth

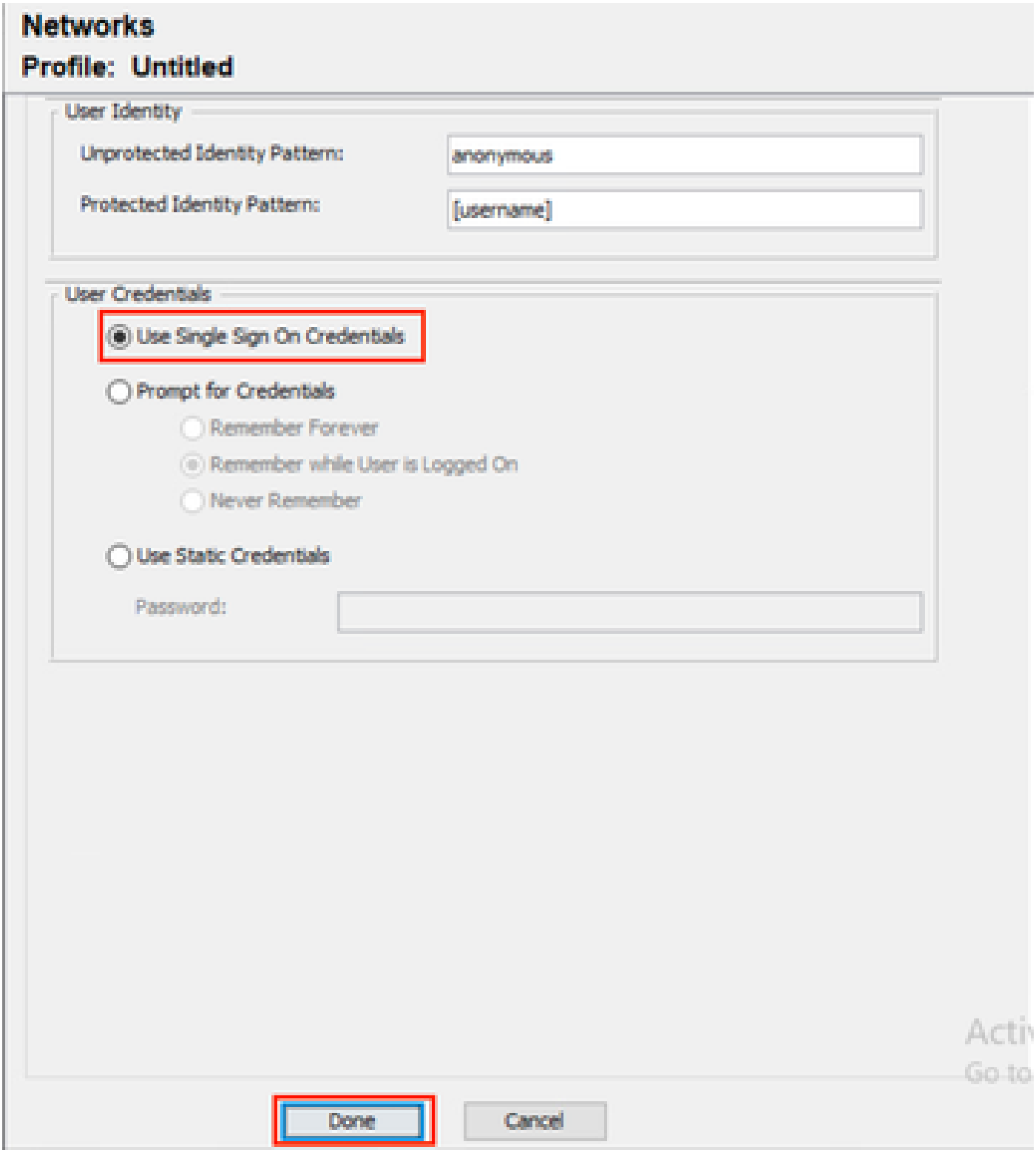
- Sélectionnez EAP-TTLS sous Méthodes EAP.
- Sous Inner Methods, sélectionnez Use EAP Methods et sélectionnez EAP-MSCHAPv2.
- Cliquez sur Next (Suivant).



Authentification utilisateur NAM Profile Editor

Étape 8. Dans Certificates, configurez les mêmes règles de validation de certificat que celles décrites à l'étape 5.

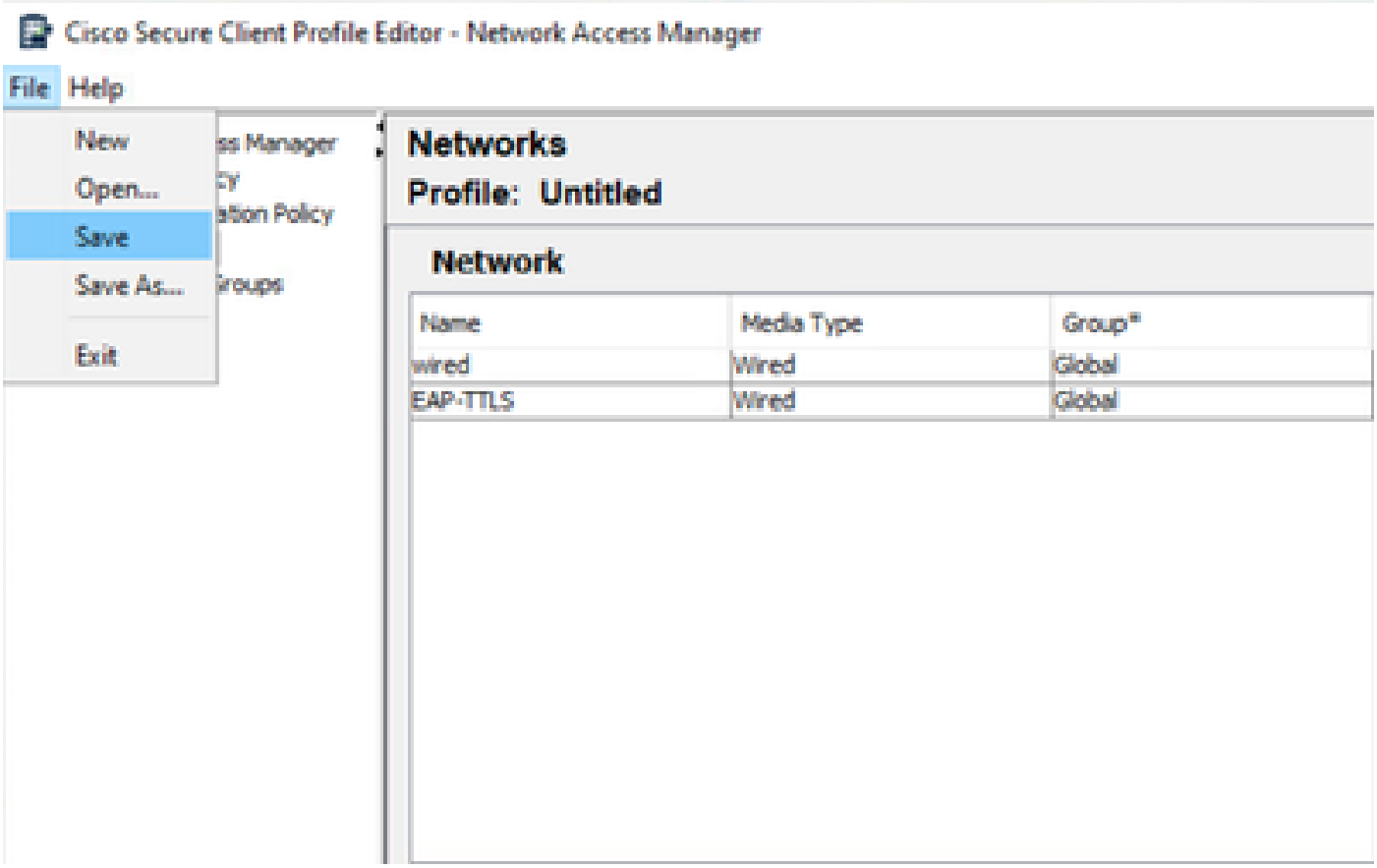
Étape 9. Dans Informations d'identification de l'utilisateur, sélectionnez Utiliser les informations d'identification de l'authentification unique, puis cliquez sur Terminé.



Informations d'identification utilisateur NAM Profile Editor

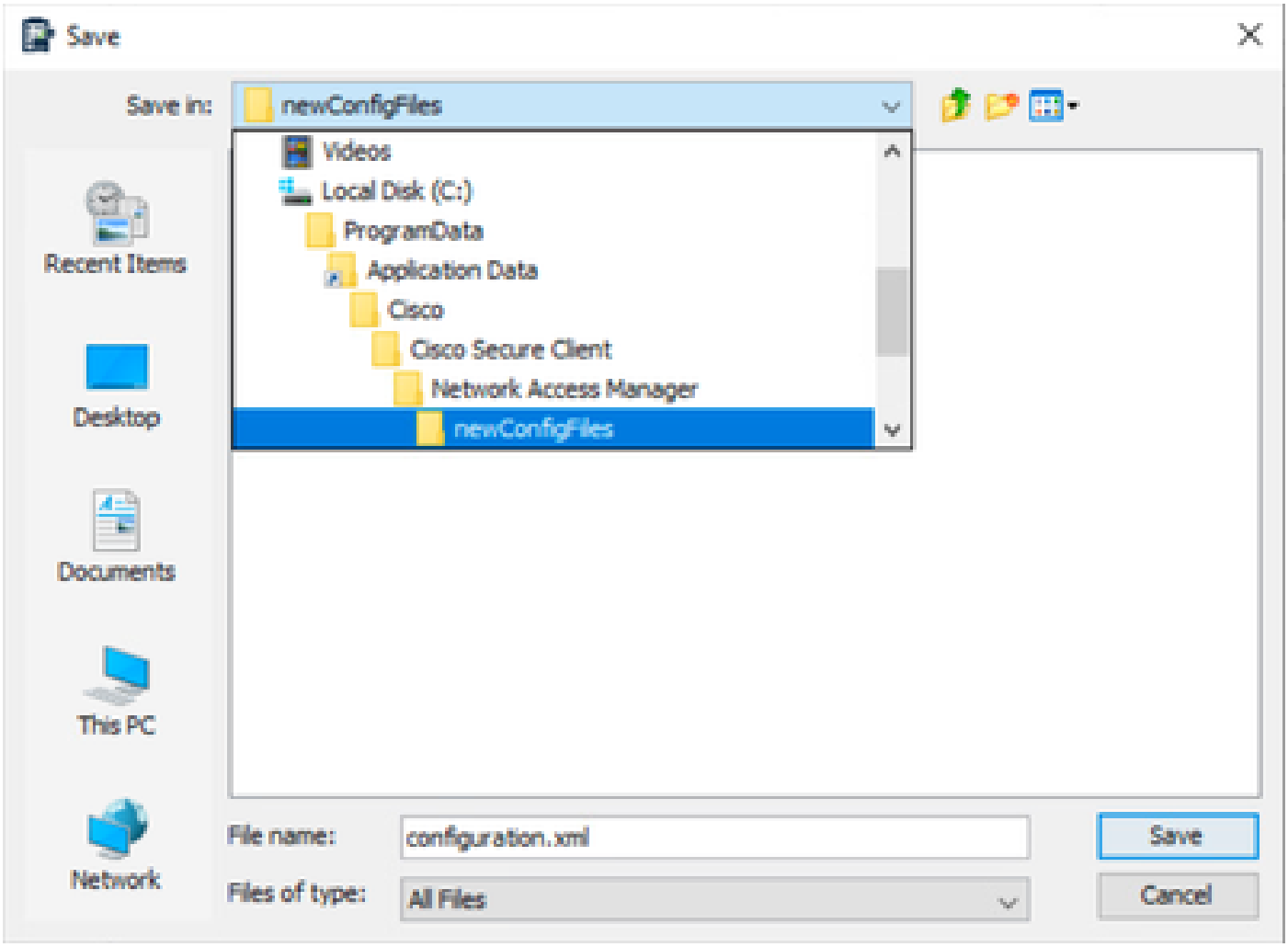
Partie 6 : Enregistrer le fichier de configuration réseau

Étape 1. Cliquez sur File > Save.



Éditeur de profil NAM Enregistrer la configuration réseau

Étape 2. Enregistrez le fichier sous le nom configuration.xml dans le dossier newConfigFiles.

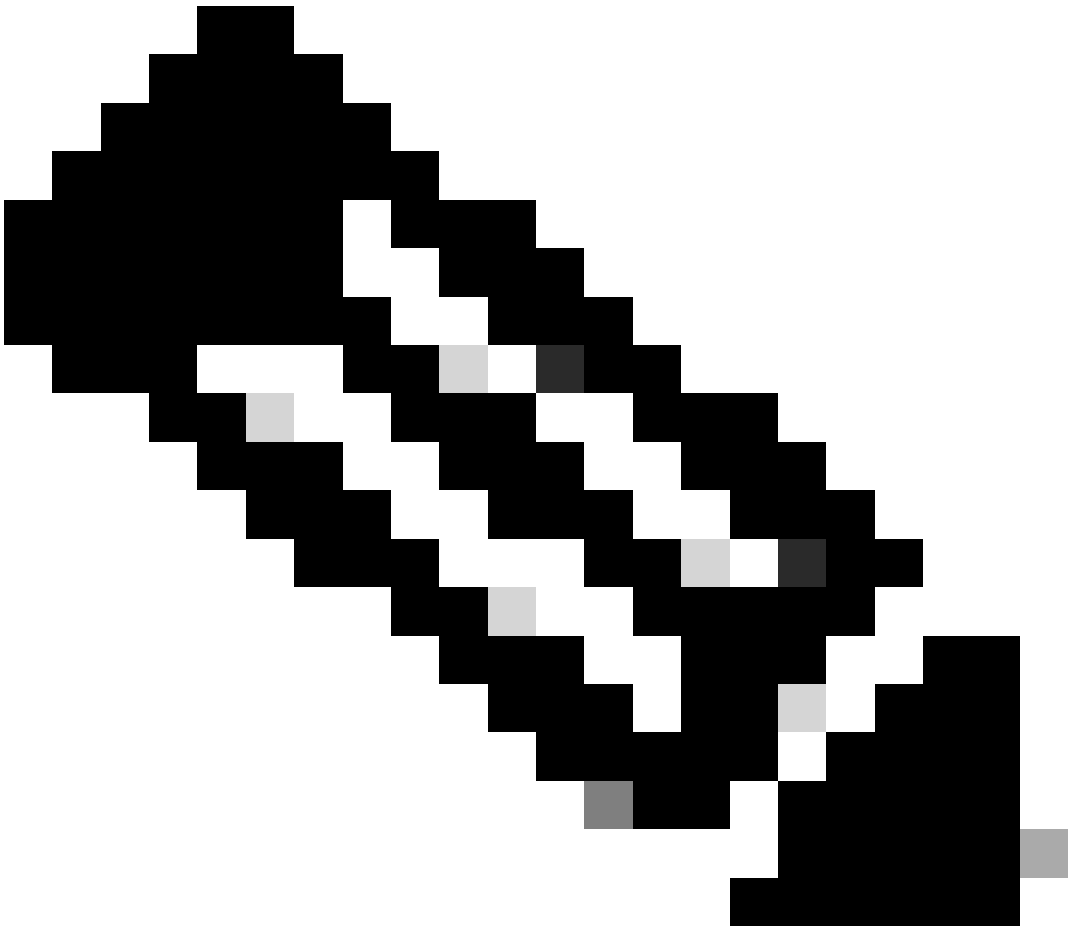


Enregistrer la configuration réseau

Partie 7 : Configurer AAA sur le commutateur

```
C9300-1#sh run aaa
!
aaa authentication dot1x default group labgroup
aaa authorization network default group labgroup
aaa accounting dot1x default start-stop group labgroup
aaa accounting update newinfo periodic 2880
!
!
!
!
aaa server radius dynamic-author
 client 10.76.112.135 server-key cisco
!
!
radius server labserver
 address ipv4 10.76.112.135 auth-port 1812 acct-port 1813
 key cisco
!
!
aaa group server radius labgroup
 server name labserver
!
```

```
!
!
!
aaa new-model
aaa session-id common
!
!



C9300-1(config)#dot1x system-auth-control
```



> Remarque : La commande dot1x system-auth-control n'apparaît pas dans le résultat de la commande show running-config, mais elle est nécessaire pour activer 802.1X globalement.

Configurez l'interface du commutateur pour 802.1X :

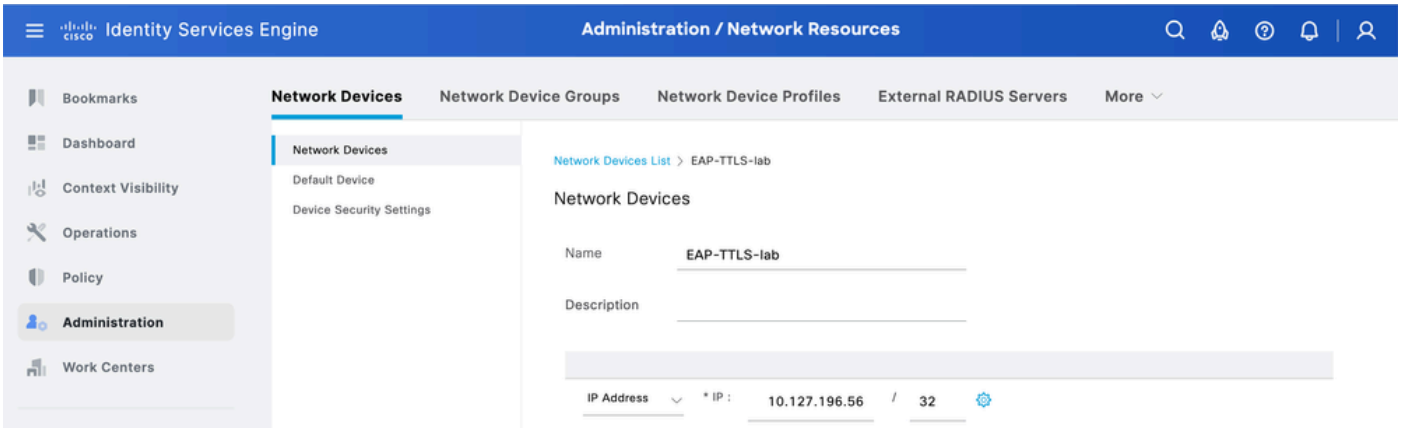
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

Current configuration : 242 bytes
!
interface GigabitEthernet1/0/44
 switchport access vlan 96
 switchport mode access
 device-tracking
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 authentication periodic

 mab
 dot1x pae authenticator
end
```

Partie 8 : Configurations ISE

Étape 1 : configuration du commutateur sur ISE

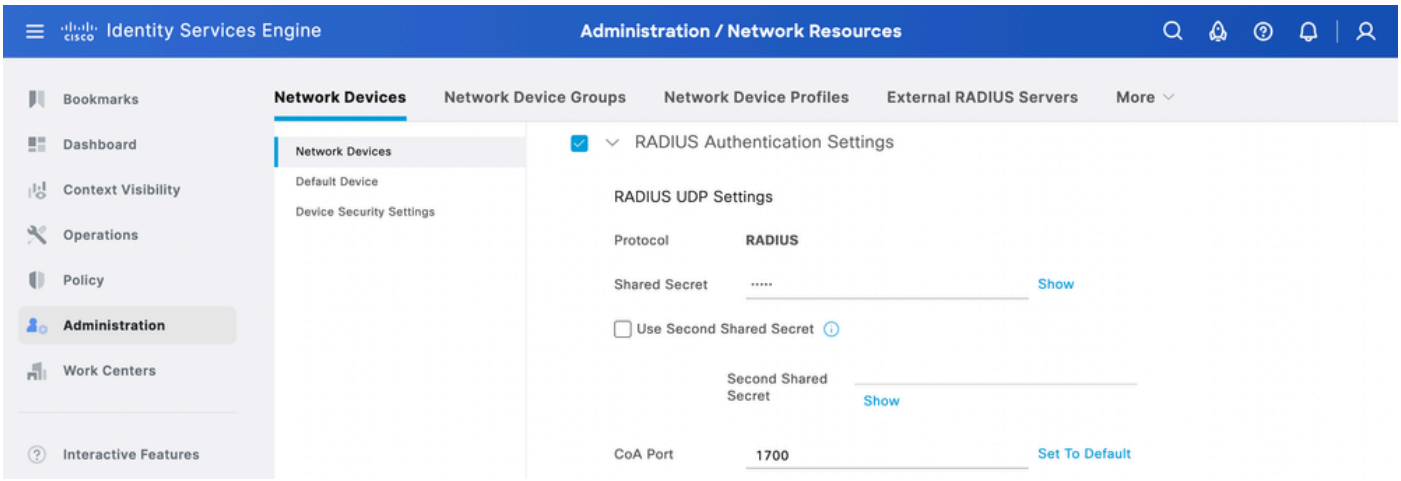
Accédez à Administration > Network Resources > Network Devices et cliquez sur Add.

Saisissez ici le nom et l'adresse IP du commutateur.



Ajout de périphérique réseau ISE

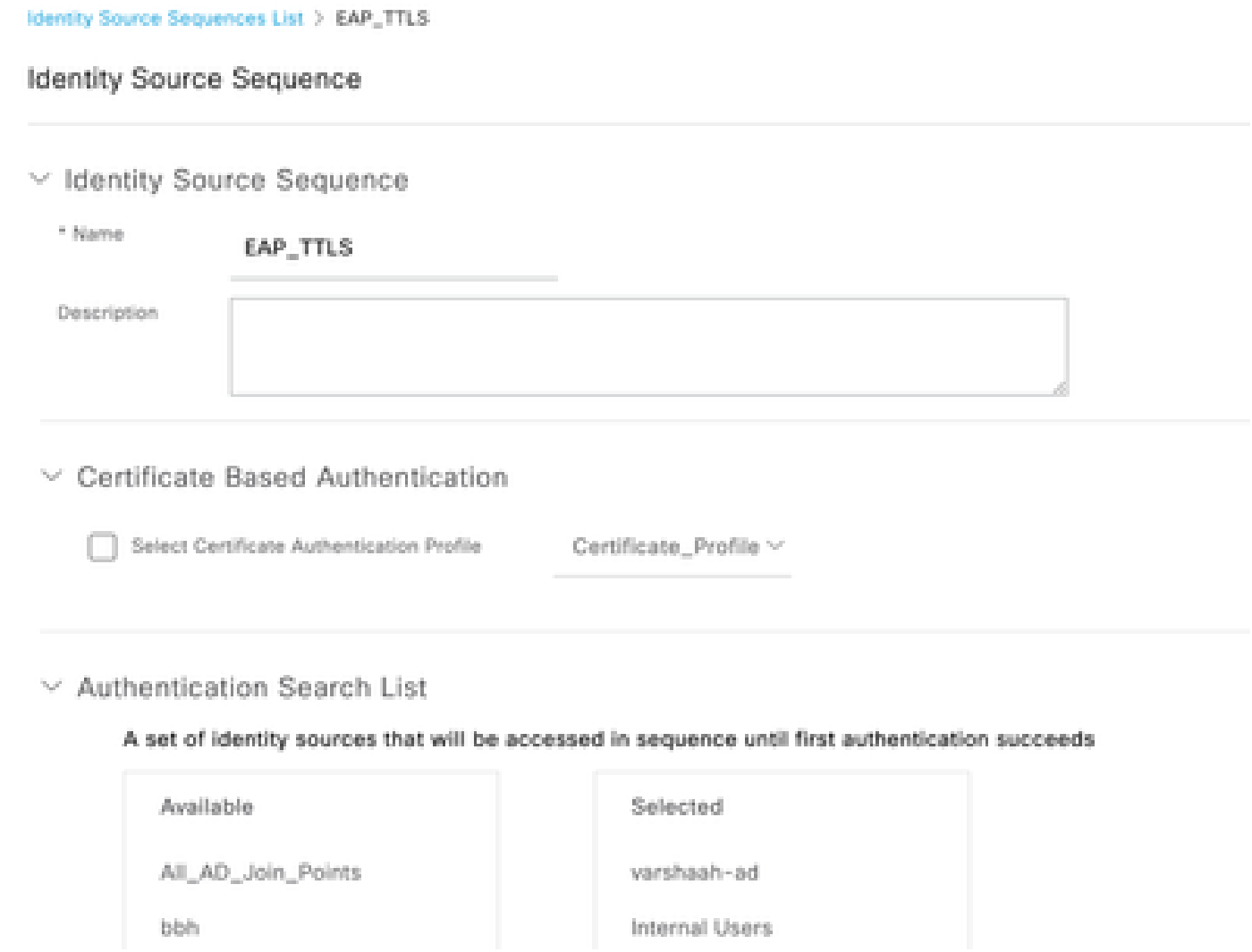
Entrez le secret partagé RADIUS, identique à celui configuré précédemment sur le commutateur.



RADIUS Secret partagé ISE

Étape 2 : configuration de la séquence source d'identité

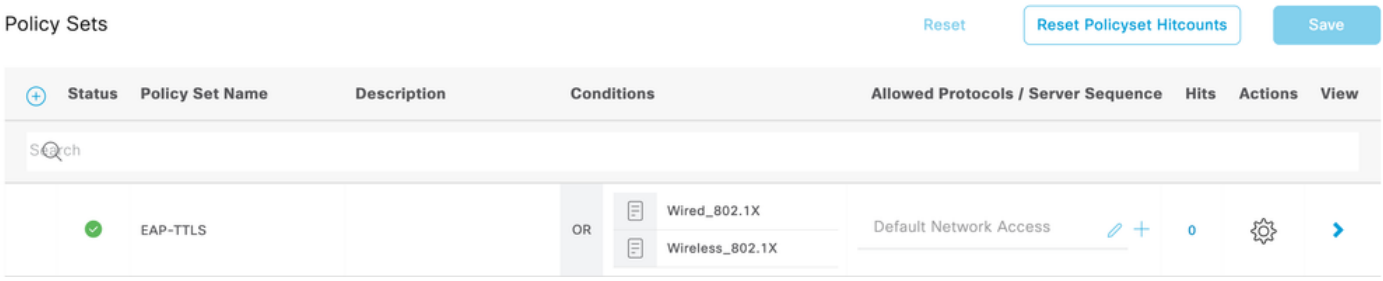
- Accédez à Administration > Identity Management > Identity Source Sequences.
- Cliquez sur Add pour créer une nouvelle séquence source d'identité.
- Configurez les sources d'identité sous Liste de recherche d'authentification.



Séquence source d'identité ISE

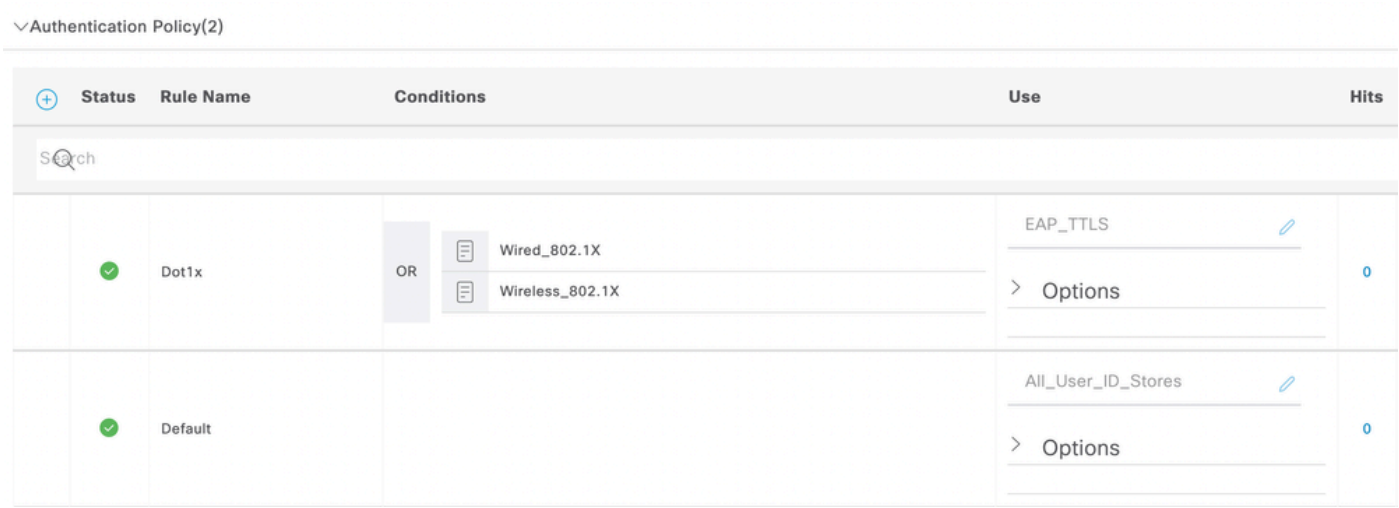
Étape 3 : configuration du jeu de stratégies

Accédez à Policy > Policy Sets et créez un nouveau jeu de stratégies. Configurez les conditions sur Wired_802.1x OU Wireless_802.1x. Pour les protocoles autorisés, sélectionnez Default Network Access :



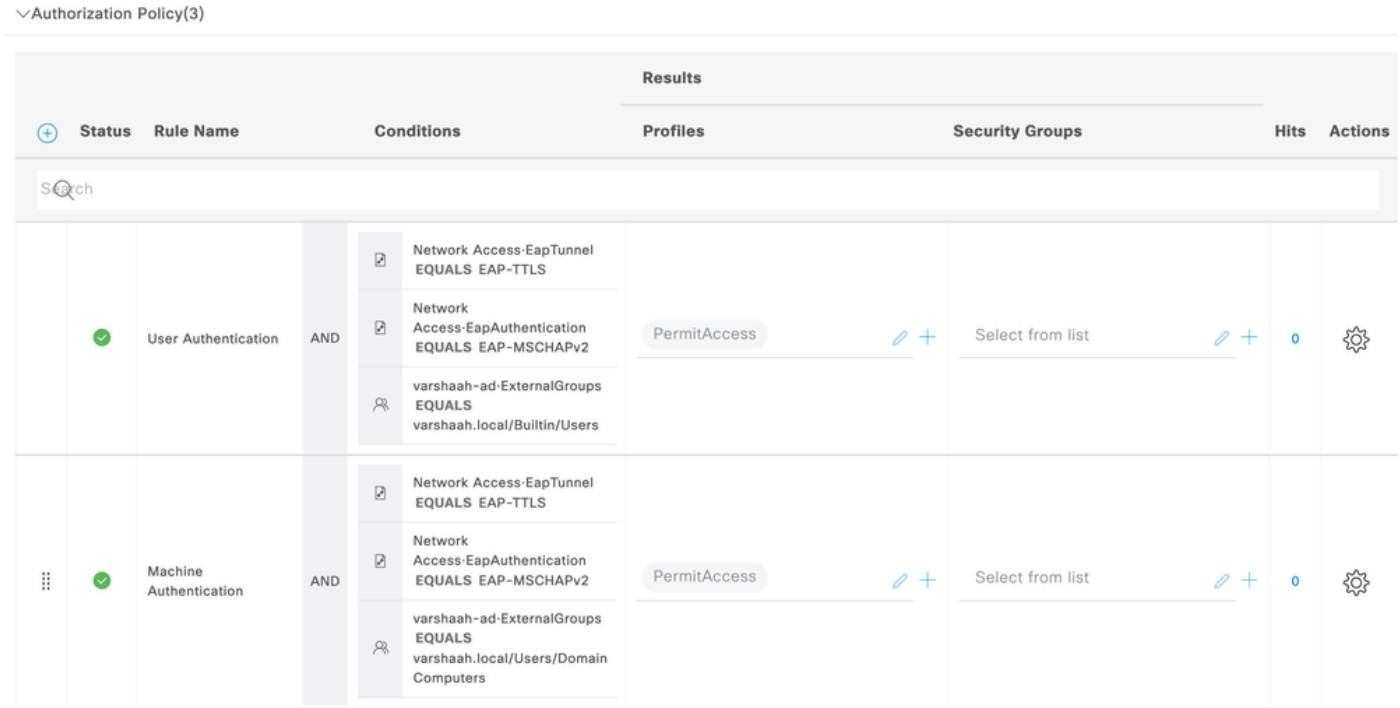
Jeu de stratégies EAP-TTLS

Créez la stratégie d'authentification pour dot1x et choisissez la séquence source d'identité créée à l'étape 4.



Politique d'authentification EAP-TTLS

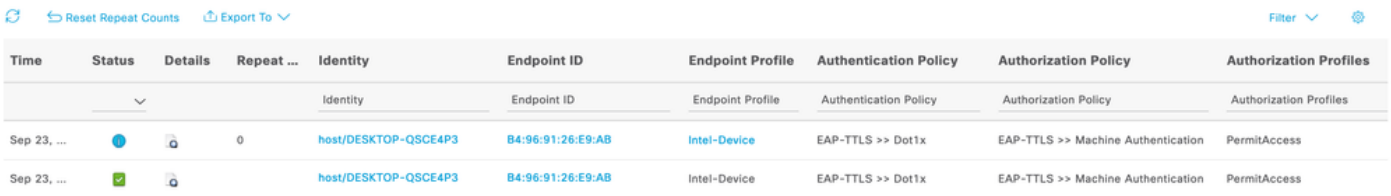
Pour la stratégie d’autorisation, créez la règle avec trois conditions. La première condition vérifie que le tunnel EAP-TTLS est utilisé. La deuxième condition vérifie que EAP-MSCHAPv2 est utilisé comme méthode EAP interne. La troisième condition vérifie le groupe AD correspondant.



Politique d'autorisation Dot1x

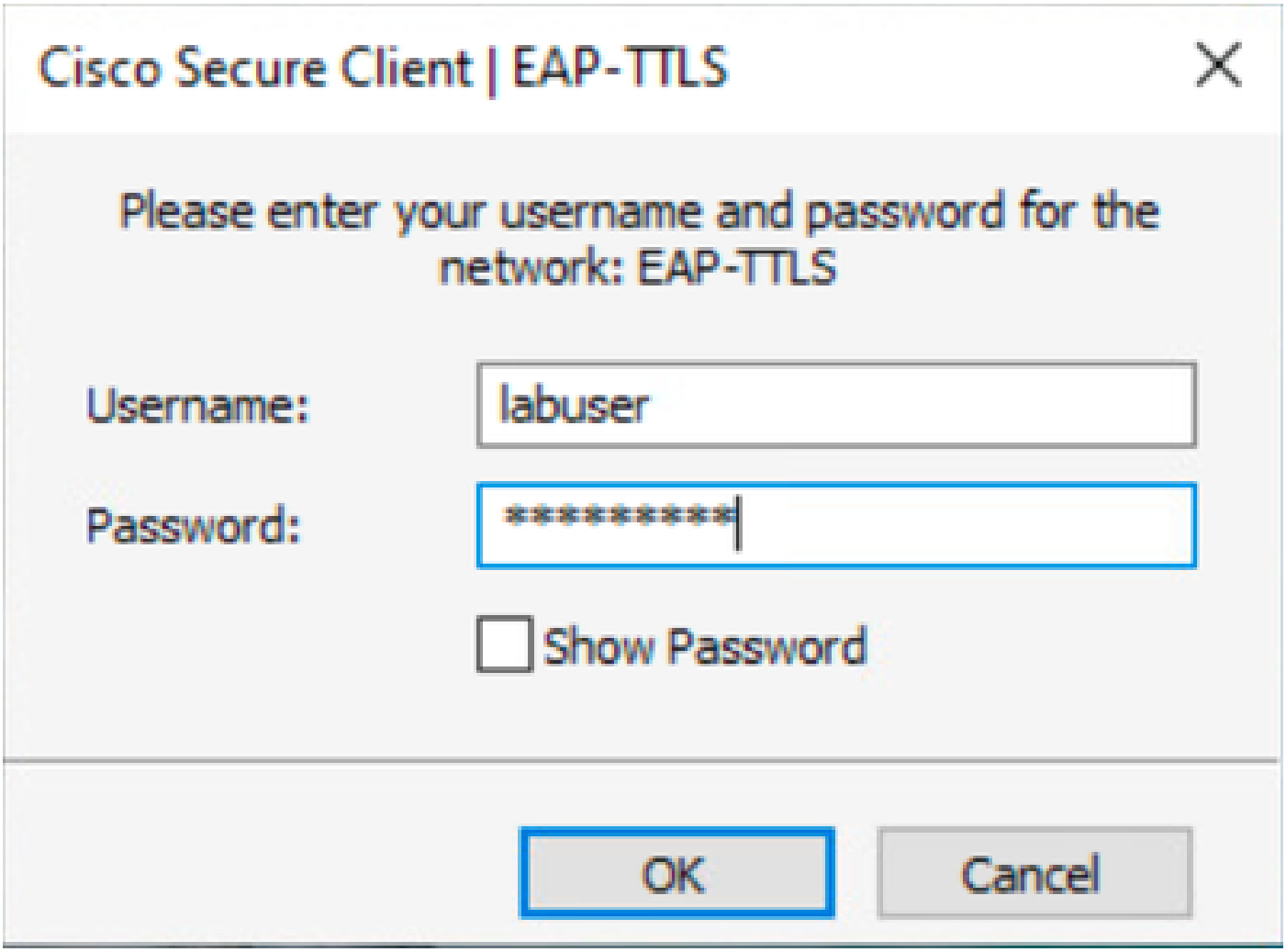
Vérifier

Vous pouvez redémarrer l'ordinateur Windows 10 ou vous déconnecter, puis vous connecter. Lorsque l'écran de connexion Windows s'affiche, l'authentification de la machine est déclenchée.

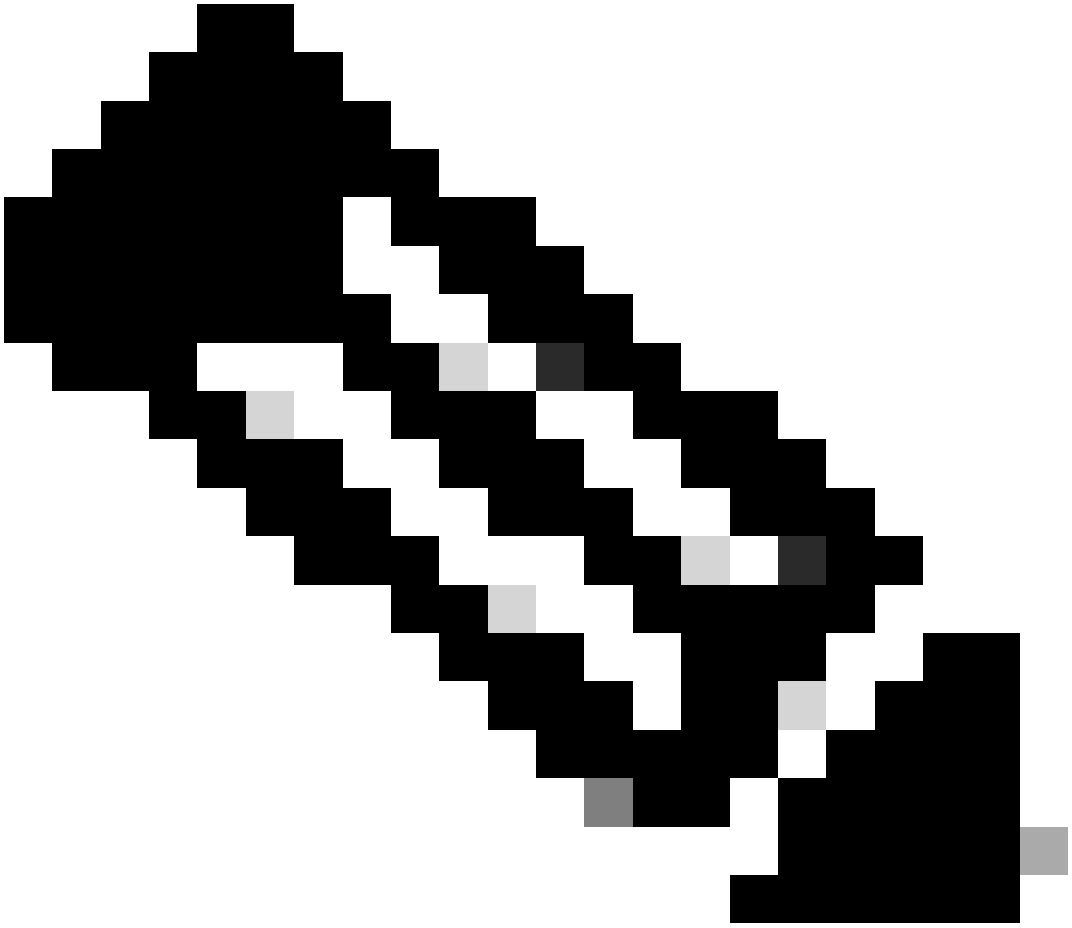


Authentification Live Log Machine

Lorsque vous vous connectez au PC avec des informations d'identification, l'authentification de l'utilisateur est déclenchée.

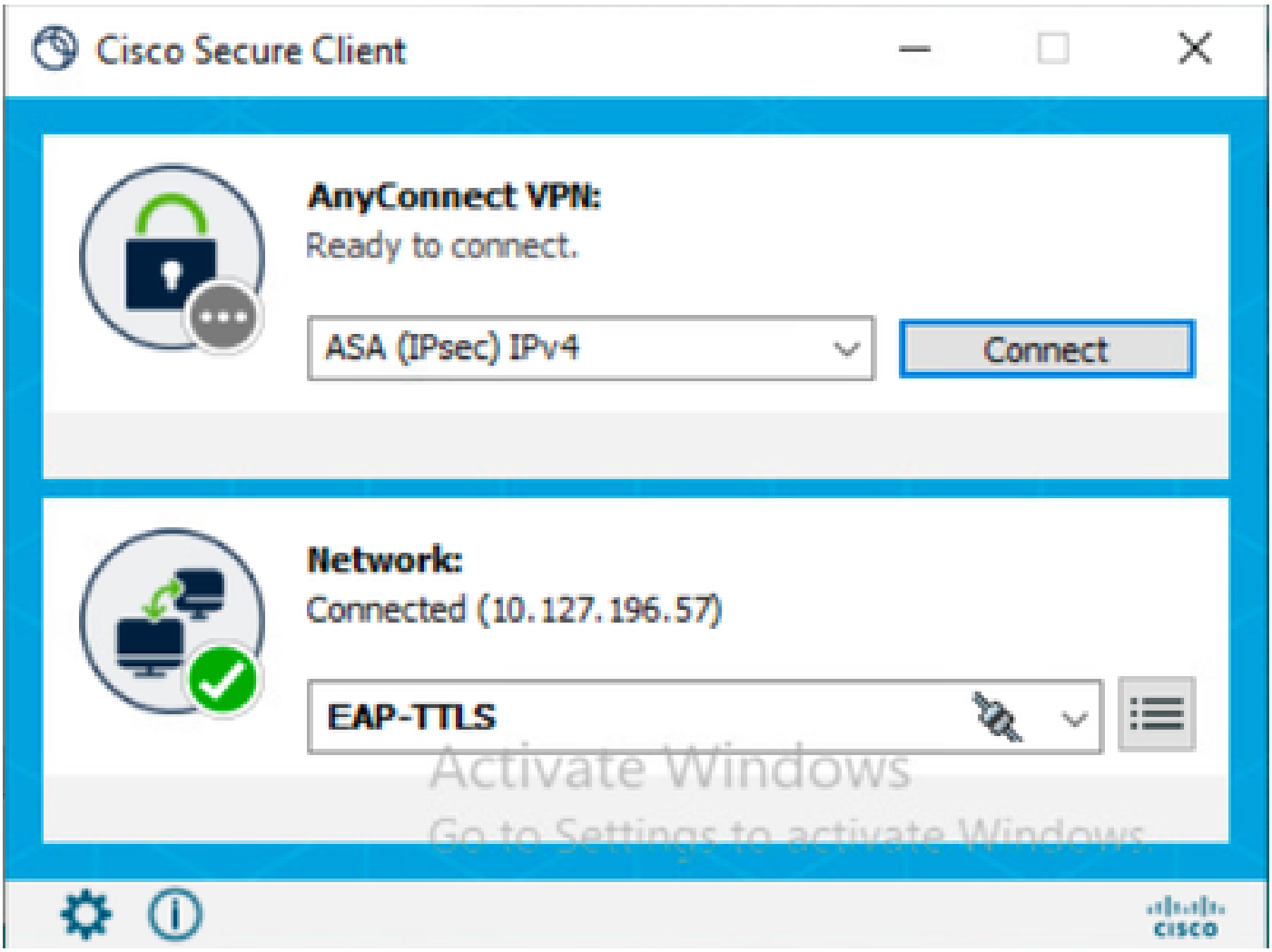


Identifiants d'authentification

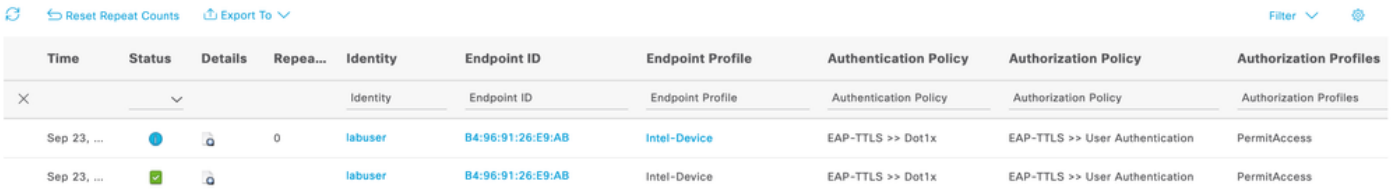


Remarque : Cet exemple utilise les informations d'identification utilisateur Active Directory pour l'authentification. Vous pouvez également créer un utilisateur interne dans Cisco ISE et utiliser ces informations d'identification pour vous connecter.

Une fois les informations d'identification saisies et vérifiées, le point d'extrémité est connecté au réseau avec l'authentification utilisateur.



EAP-TTLS connecté



Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
				Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
Sep 23, ...			0	labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess
Sep 23, ...				labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess

Authentification utilisateur Live Log

Analyser les journaux en direct ISE RADIUS

Cette section illustre les entrées du journal RADIUS en direct pour une authentification réussie de l'ordinateur et de l'utilisateur.

Authentification machine

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24431 Authenticating machine against Active Directory - varshaah-ad 24325 Resolving identity - host/DESKTOP-QSCE4P3 ... ... 24343 RPC Logon request succeeded - DESKTOP-QSCE4P3$@varshaah.local **24470 Machine authentication against Active Directory is successful - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - host/DESKTOP-QSCE4P3 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Authentification utilisateur

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - labuser@varshaah.local ... ... 24343 RPC Logon request succeeded - labuser@varshaah.local **24402 User authentication against Active Directory succeeded - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - labuser 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Analyser les journaux NAM

Les journaux NAM, en particulier après l'activation de la consignation étendue, contiennent une grande quantité de données, dont la plupart ne sont pas pertinentes et peuvent être ignorées. Cette section répertorie les lignes de débogage pour illustrer chaque étape que le NAM effectue pour établir une connexion réseau. Lorsque vous parcourez un journal, ces phrases clés peuvent être utiles pour localiser une partie du journal correspondant au problème.

Authentification machine

```
2160: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: 80
```

Le client reçoit un paquet EAP-TTLS du commutateur réseau, ce qui lance la session EAP-TTLS. Il s'agit du point de départ du tunnel d'authentification de la machine.

```
2171: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: EA
2172: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
2173: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
```

Le client reçoit le message Server Hello de ISE et commence à valider le certificat du serveur (CN=varshaah.varshaah.local). Le certificat se trouve dans le magasin de confiance du client et est ajouté pour validation.

```
2222: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Validating th
2223: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Server certif
```

Le certificat du serveur a été validé, ce qui a terminé l'établissement du tunnel TLS.

```
2563: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2564: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: NE
2565: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

Le client signale que l'authentification a réussi. L'interface est débloquée, et l'ordinateur d'état interne passe à USER_T_NOT_DISCONNECTED, indiquant que l'ordinateur peut maintenant transmettre le trafic.

```
2609: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2610: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2611: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2612: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2613: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2614: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2615: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

L'adaptateur signale authenticated, et le NAM AccessStateMachine passe à ACCESS_AUTHENTICATED. Cela confirme que l'authentification de l'ordinateur a réussi et que l'accès au réseau est complet.

Authentification utilisateur

```
100: DESKTOP-QSCE4P3: Sep 25 2025 14:01:26.669 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Network EAP-TT
```

Le client NAM commence le processus de connexion EAP-TTLS.

```
195: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Binding adapte
198: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
```

Le NAM lie la carte physique au réseau EAP-TTLS et passe à l'état ACCESS_ATTACHED, confirmant que la carte est prête pour l'authentification.

```
204: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
247: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3680][comp=SAE]: STAT
```

Le client passe de ATTACHED à CONNECTING, en commençant l'échange 802.1X.

```
291: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.388 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
```

Le client envoie un message EAPOL-Start pour déclencher le processus d’authentification.

```
331: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: PORT
332: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
340: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: EAP
```

Le commutateur demande une identité et le client se prépare à répondre avec une identité externe.

```
402: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9580]: EAP-CB: creden
422: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: processin
460: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

NAM envoie l'identité du routeur. Par défaut, il s'agit de l'anonymous, indiquant que l'échange est pour l'authentification de l'utilisateur (pas de l'ordinateur).

```
488: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP sugges
```

```
489: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP reques
490: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: EAP metho
491: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

Le client et le serveur acceptent tous deux d'utiliser EAP-TTLS comme méthode de routeur.

```
660: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
661: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
```

Le client envoie Client Hello et reçoit le Server Hello, qui inclut le certificat ISE.

```
706: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: 802
717: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
718: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
719: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
726: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
```

Le certificat du serveur est présenté. Le client recherche le fichier CN varshaah.varshaah.local, trouve une correspondance et valide le certificat. La connexion s'interrompt pendant la vérification du certificat X.509.

```
729: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
730: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EAP
1110: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1111: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

Le tunnel est établi. NAM demande et prépare maintenant l'identité et les informations d'identification protégées pour l'authentification interne.

```
1527: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1528: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1573: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1574: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1575: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
```

La connexion TLS est terminée. Un tunnel sécurisé est maintenant établi pour l'authentification interne.

```
1616: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-6-INFO_MSG: %[tid=9664]: Protected iden
1620: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
1689: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

L'identité protégée (nom d'utilisateur) est envoyée et acceptée par ISE.

```
1708: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9456][comp=SAE]: EAP
1738: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.758 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Protected pas
1741: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.200 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

ISE demande le mot de passe. NAM envoie le mot de passe protégé à l'intérieur du tunnel TLS.

```
1851: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1852: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1853: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1854: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
```

ISE valide le mot de passe, envoie EAP-Success, et NAM passe à AUTHENTICATED. À ce stade, l'authentification de l'utilisateur est terminée et le client a accès au réseau.

Dépannage

Lors du dépannage des problèmes liés à Network Access Manager (NAM) avec Cisco ISE et l'intégration du commutateur, les journaux doivent être collectés à partir des trois composants : Secure Client (NAM), Cisco ISE et le commutateur.

Journaux du client sécurisé (NAM)

1. Activez la journalisation étendue NAM en suivant ces étapes.
2. Reproduisez le problème. Si le profil réseau ne s'applique pas, exécutez Network Repair dans Secure Client.
3. Collectez l'ensemble DART à l'aide de l'outil Diagnostics and Reporting Tool (DART).

Journaux Cisco ISE

Activez ces débogages sur ISE pour capturer l'authentification et les interactions de répertoire :

- runtime-AAA
- nsf

- nsf-session

Journaux des commutateurs

Débogages de base

```
request platform software trace rotate all
set platform software trace smd switch active R0 radius debug
set platform software trace smd switch active R0 aaa debug
set platform software trace smd switch active R0 dot1x-all debug
set platform software trace smd switch active R0 eap-all debug
debug radius all
```

Débogages avancés (si requis)

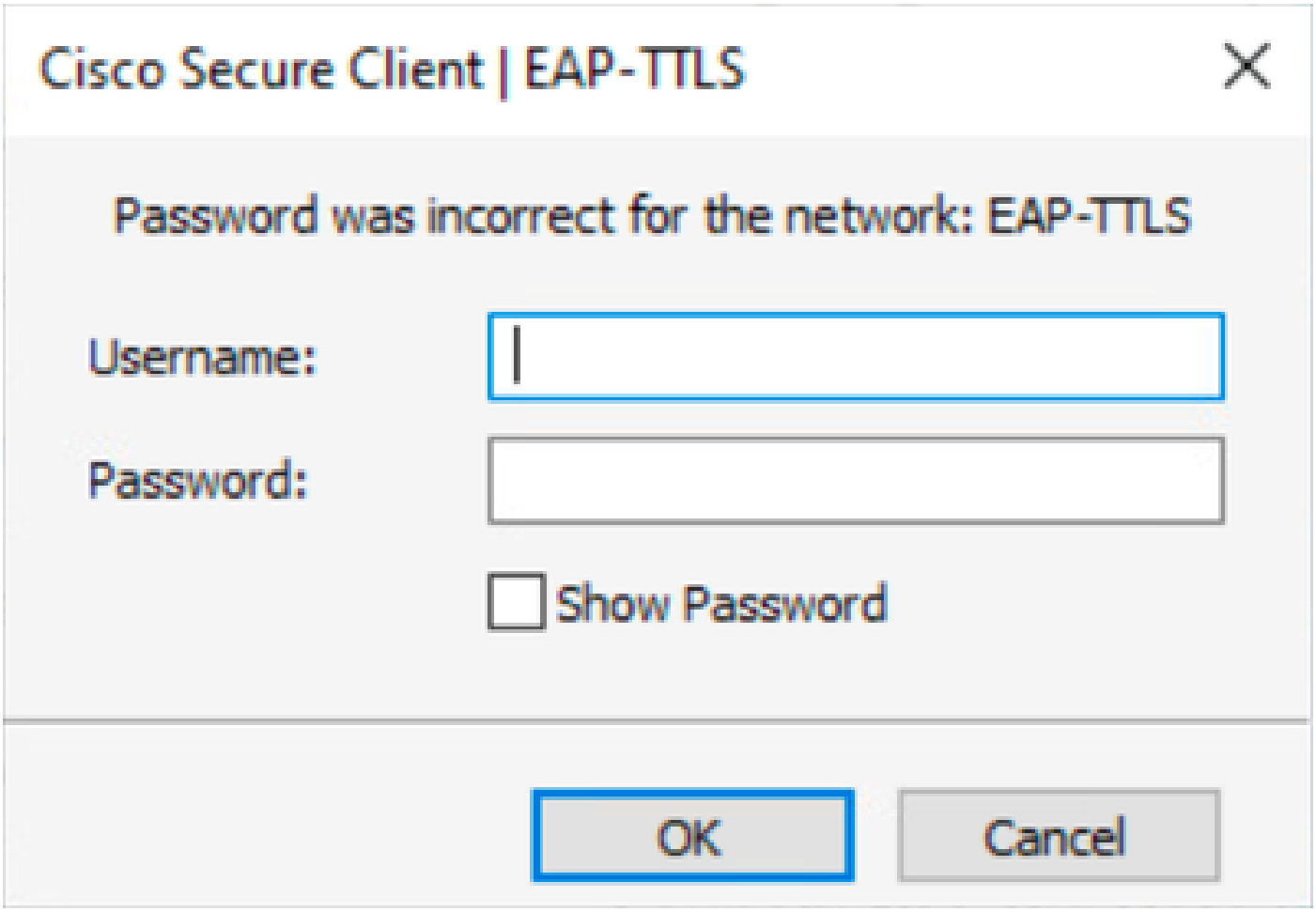
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

Commandes show

```
show version
show debugging
show running-config aaa
show authentication session interface gix/x details
show dot1x interface gix/x
show aaa servers
show platform software trace message smd switch active R0
```

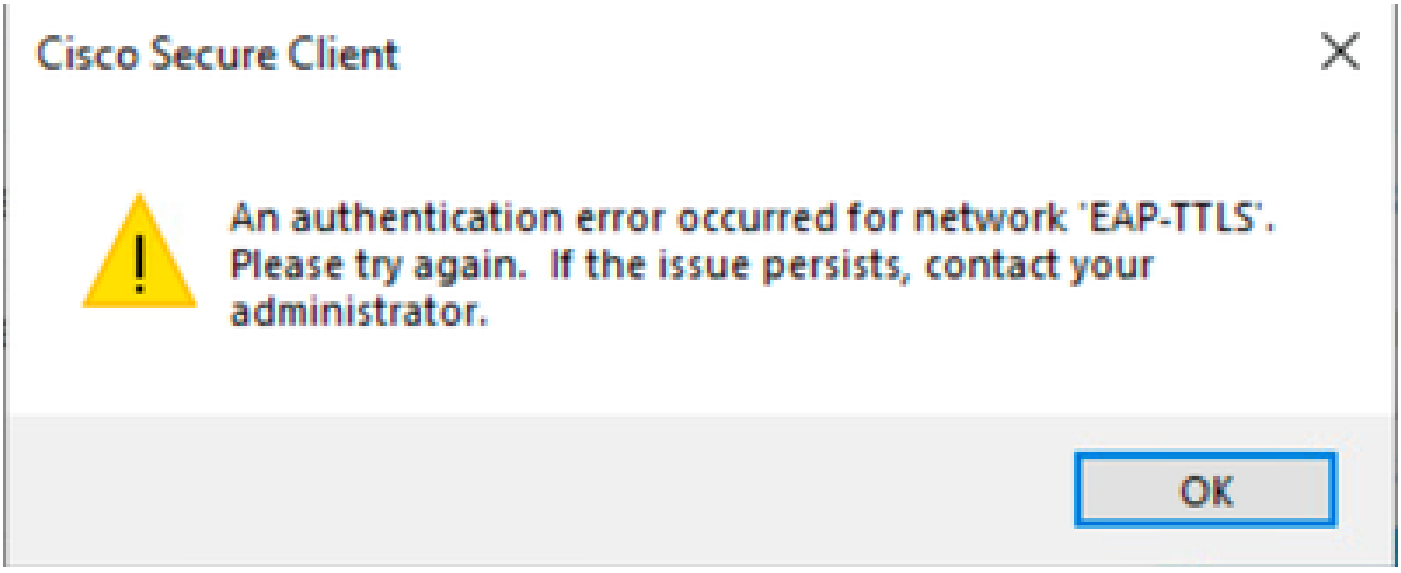
Échec de l'authentification utilisateur en raison de références incorrectes

Lorsqu'un utilisateur entre des informations d'identification incorrectes, Secure Client affiche un mot de passe générique incorrect pour le réseau : message EAP-TTLS. L'erreur à l'écran ne spécifie pas si le problème est dû à un nom d'utilisateur ou un mot de passe non valide.



Erreur de mot de passe incorrect

Si l'authentification échoue deux fois de suite, Secure Client affiche le message suivant : Une erreur d'authentification s'est produite pour le réseau « EAP-TTLS ». Veuillez réessayer. Si le problème persiste, contactez votre administrateur.



Problème d'authentification utilisateur

Pour identifier la cause, consultez les journaux NAM.

1. Mot de passe incorrect :

Lorsqu'un utilisateur saisit un mot de passe incorrect, les journaux NAM affichent des entrées similaires à ce résultat :

```
3775: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3776: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3777: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.922 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
```

Dans les journaux en direct de Cisco ISE, l'événement correspondant apparaît comme suit :

Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password

Mot de passe incorrect

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity 10 **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 0** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 0 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 0 **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - varshaah-ad 0 24430 Authenticating user against Active Directory - varshaah-ad 0 24325 Resolving identity - labuser@varshaah.local 4 24313 Search for matching accounts at join point - varshaah.local 0 24319 Single matching account found in forest - varshaah.local 0 24323 Identity resolution detected single matching account 0 **24344 RPC Logon request failed - STATUS_WRONG_PASSWORD, ERROR_INVALID_PASSWORD, labuser@varshaah.local 20 24408 User authentication against Active Directory failed since user has entered the wrong password - varshaah-ad 1** ... ... 11823 EAP-MSCHAP authentication attempt failed ... ... 11815 Inner EAP-MSCHAP authentication failed 0 ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11003 Returned RADIUS Access-Reject

2. Nom d'utilisateur incorrect :

Lorsqu'un utilisateur saisit un nom d'utilisateur incorrect, les journaux NAM affichent des entrées similaires à ce résultat :

```
3788: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3789: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300]: EAP-CB: EAP
```

Dans les journaux en direct de Cisco ISE, l'événement correspondant apparaît comme suit :

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resoultion settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).

Nom d'utilisateur incorrect

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - All_AD_Join_Points 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - user@varshaah.local 24313 Search for matching accounts at join point - varshaah.local ... ... 24352 Identity resolution failed - ERROR_NO_SUCH_USER **24412 User not found in Active Directory - varshaah-ad** ... ... 15013 Selected Identity Source - Internal Users 24210 Looking up User in Internal Users IDStore - user **24216 The user is not found in the internal users identity store** ... ... 22056 Subject not found in the applicable identity store(s) 22058 The advanced option that is configured for an unknown user is used 22061 The 'Reject' advanced option is configured in case of a failed authentication request **11823 EAP-MSCHAP authentication attempt failed** ... ... **11815 Inner EAP-MSCHAP authentication failed** ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11504 Prepared EAP-Failure 1 **11003 Returned RADIUS Access-Reject**

Défauts connus

ID de bogue	Description
ID de bogue Cisco 63395	ISE 3.0 ne peut pas localiser le magasin d'ID REST après le redémarrage des services

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.