# Dépannage des problèmes Wired Dot1x dans ISE 3.2 et Windows

## Table des matières


Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Diagramme du réseau


## Introduction

Ce document décrit comment configurer une authentification PEAP 802.1X de base pour Identity Services Engine (ISE) 3.2 et le demandeur natif Windows.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- PEAP (Protected Extensible Authentication Protocol)
- PEAP 802.1x

### Composants utilisés

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

- Version de Cisco Identity Services Engine (ISE)
- Logiciel Cisco IOS® XE C117, version 17.12.02
- Ordinateur portable utilisant Windows 10

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.

## Configurer

### Diagramme du réseau

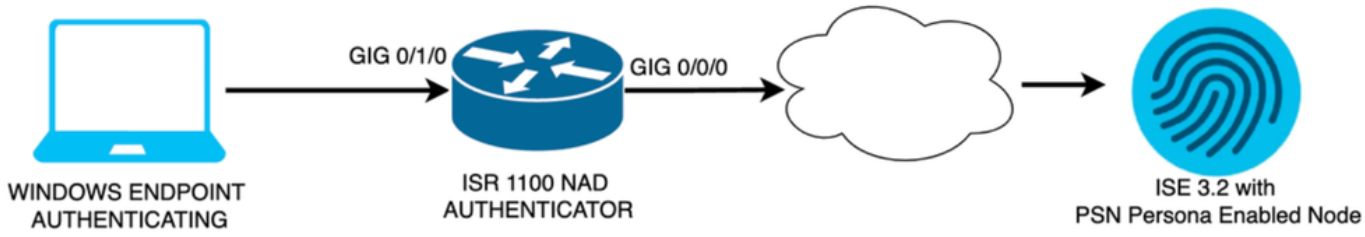



Diagramme du réseau

## Configurations

Procédez comme suit pour configurer :

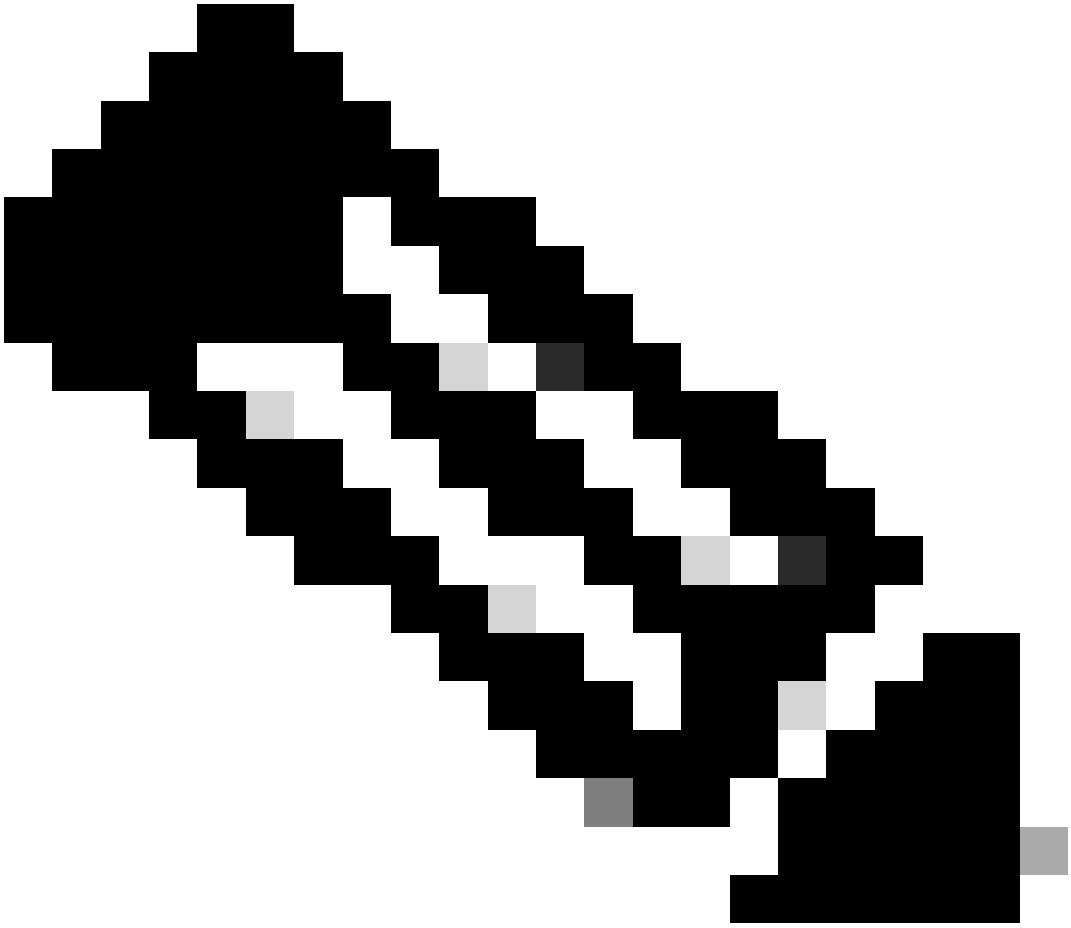
Étape 1. configuration du routeur ISR 1100

Étape 2. Configurez Identity Service Engine 3.2.

Étape 3. Configurez le demandeur natif Windows.

Étape 1. Configuration du routeur ISR 1100

Cette section explique la configuration de base qu'au moins le NAD doit avoir pour que dot1x fonctionne.



Remarque : pour un déploiement ISE multinoeud, configurez l'adresse IP du noeud sur lequel le personnage PSN est activé. Vous pouvez l'activer si vous accédez 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>
```

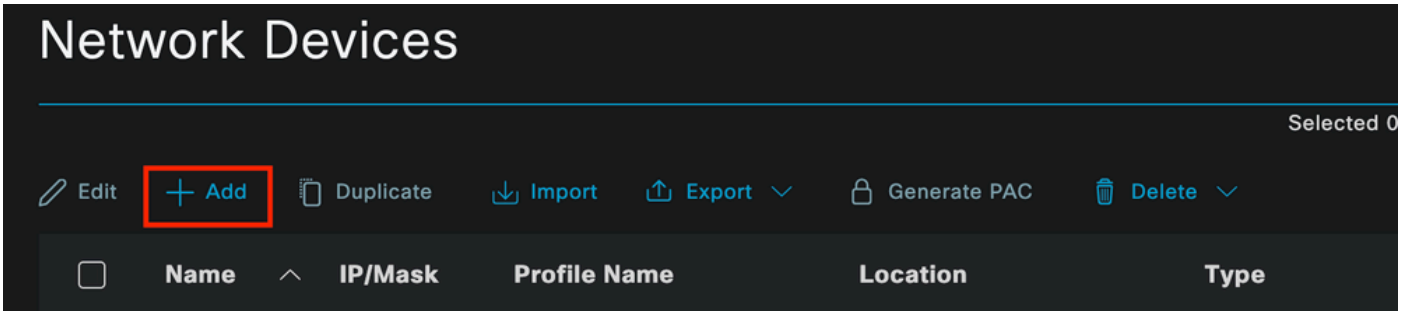
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication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

Étape 2. Configurez Identity Service Engine 3.2.

2. a. Configurez et ajoutez le périphérique réseau à utiliser pour l'authentification.

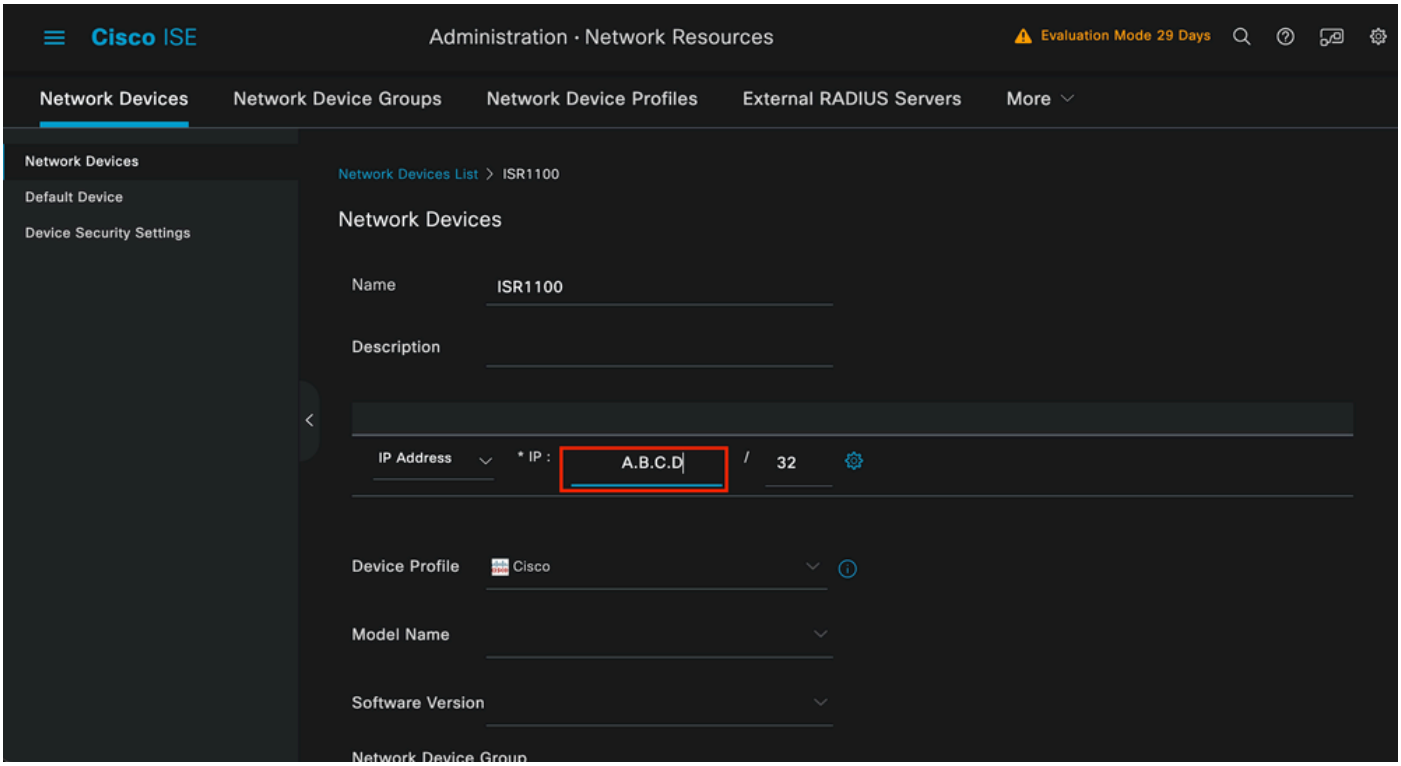
Ajoutez la section Network Device to ISE Network Devices.

Cliquez sur le bouton Add pour démarrer.




Périphériques réseau ISE

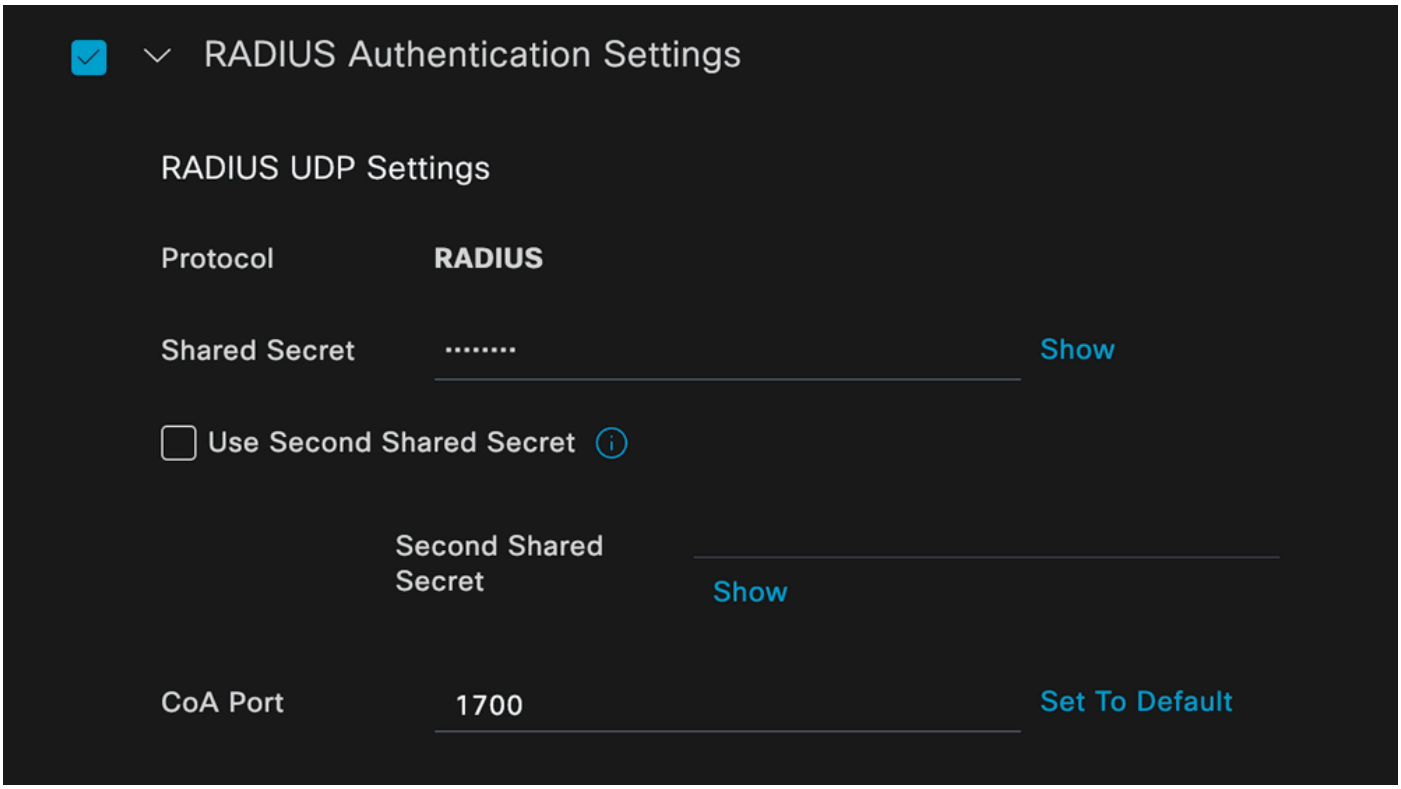
Entrez les valeurs, attribuez un nom au NAD que vous créez et ajoutez également l'adresse IP que le périphérique réseau utilise pour contacter ISE.




*Page Network Device Creation*

Sur cette même page, faites défiler vers le bas pour rechercher les paramètres d'authentification Radius. Comme l'illustre l'image suivante.

Ajoutez le secret partagé que vous avez utilisé dans votre configuration NAD.

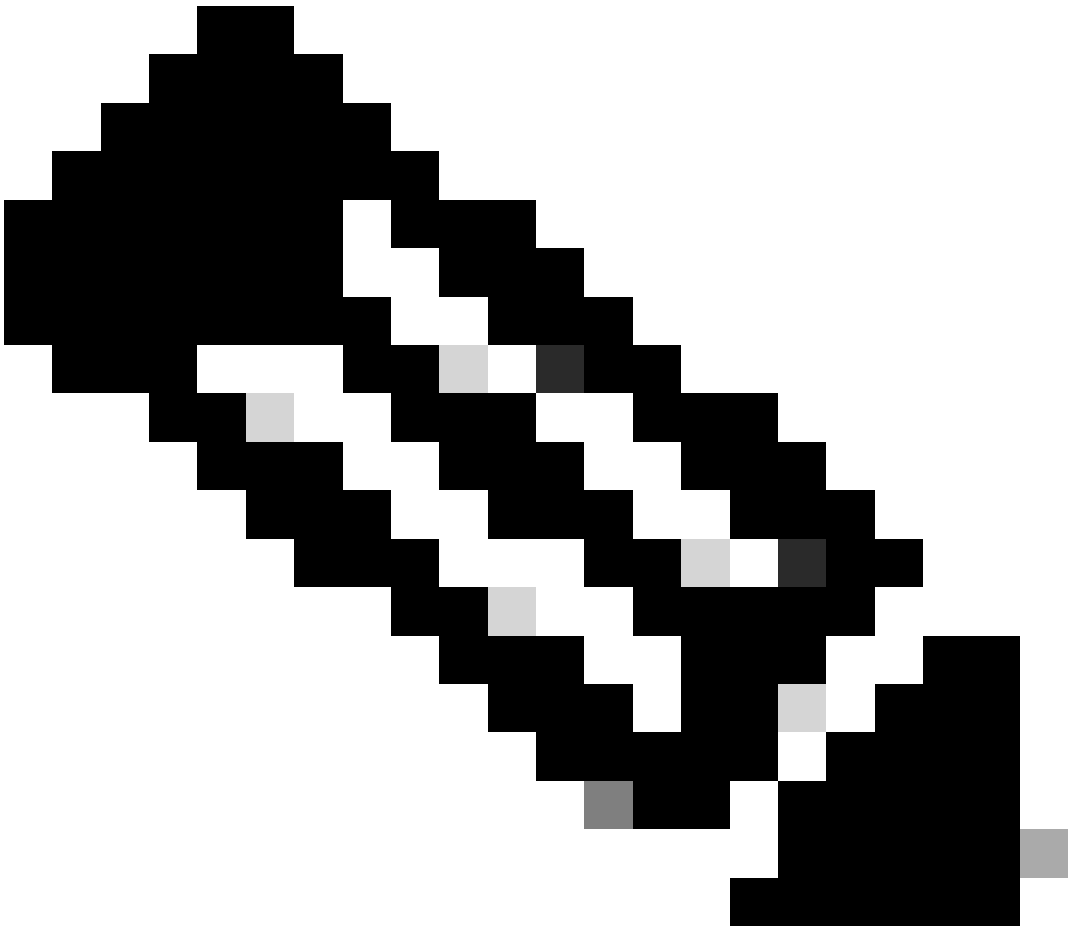



*Configuration RADIUS*

Enregistrez les modifications.

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

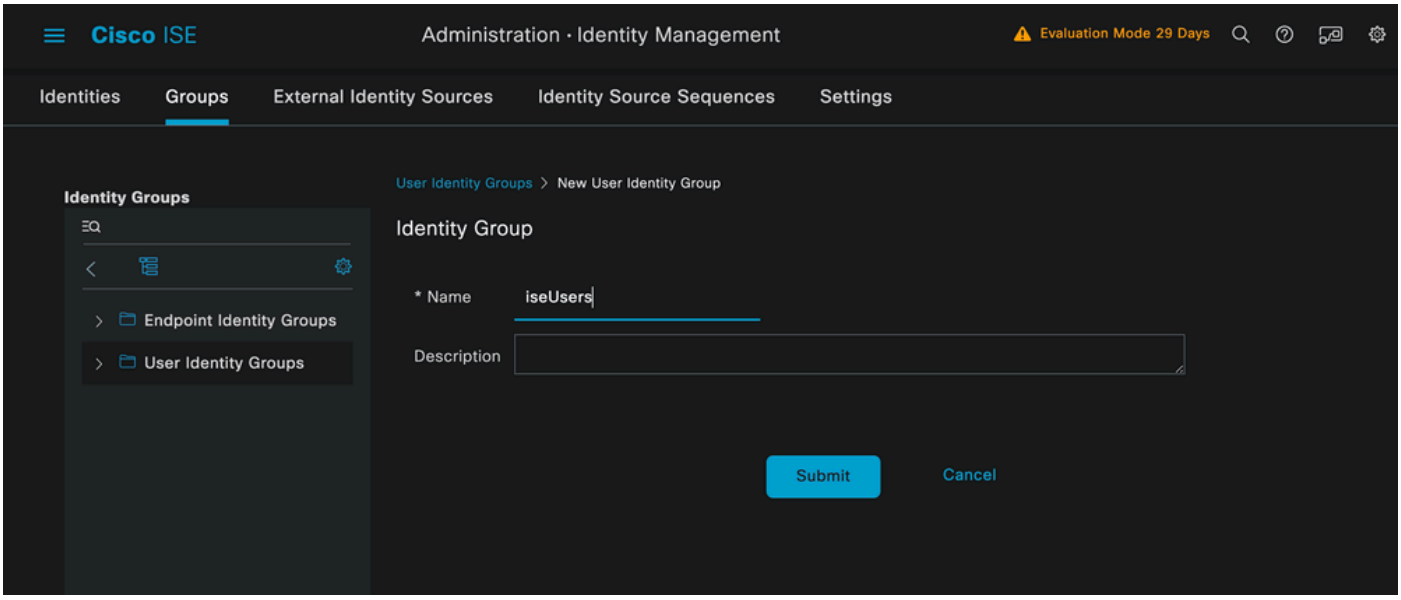
---



> Remarque : l'objectif de ce guide de configuration est d'utiliser une authentification locale ISE simple.

---

Accédez à l'onglet Administration > Gestion des identités > Groupes. Créez le groupe et l'identité, le groupe créé pour cette démonstration est iseUsers.

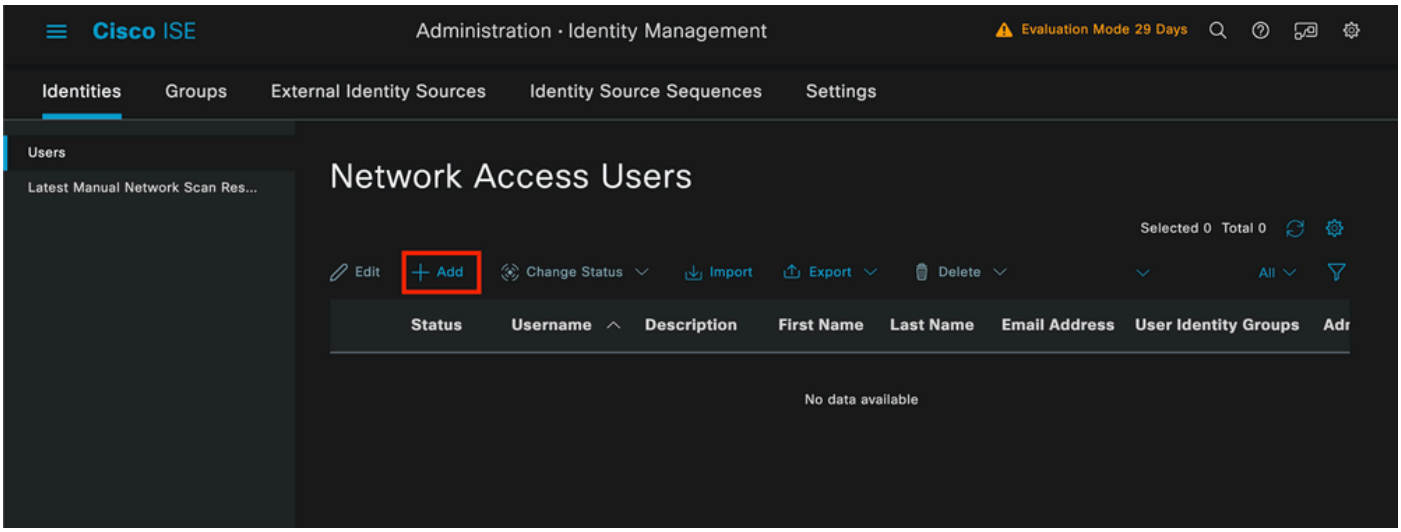



*Page Identity Group Creation*

Cliquez sur le bouton Envoyer.

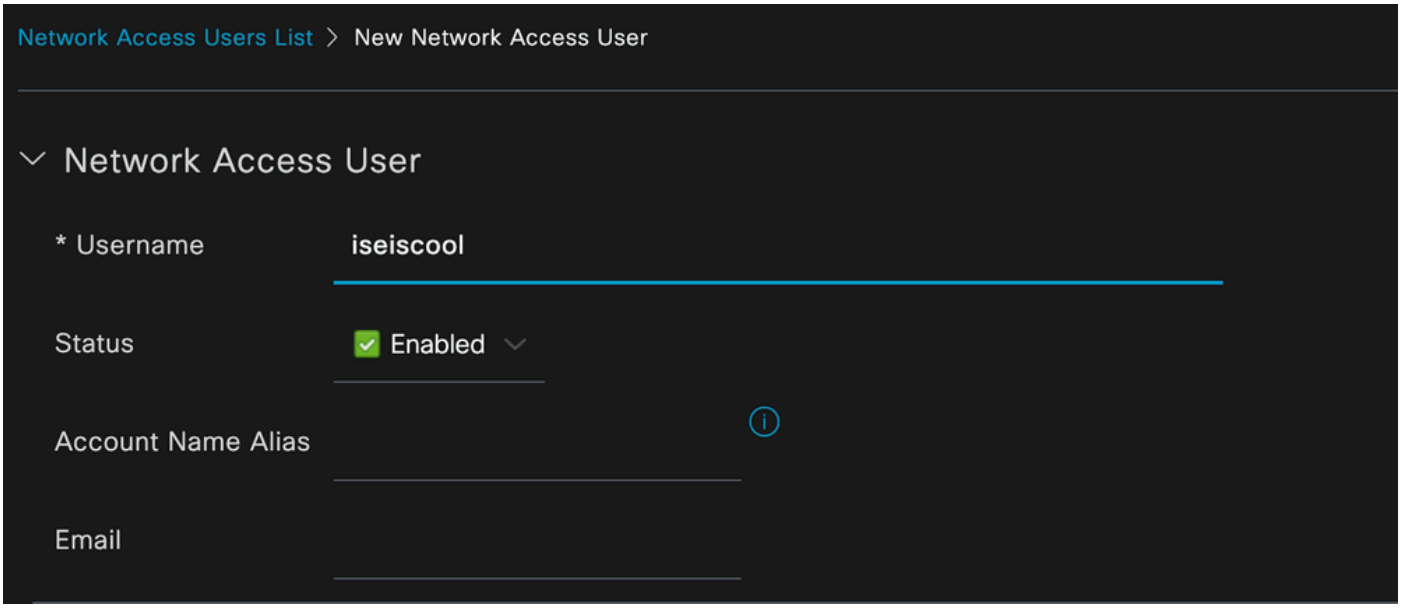
Accédez ensuite à Administration > Identity Management > Identity tab.

Cliquez sur Ajouter.



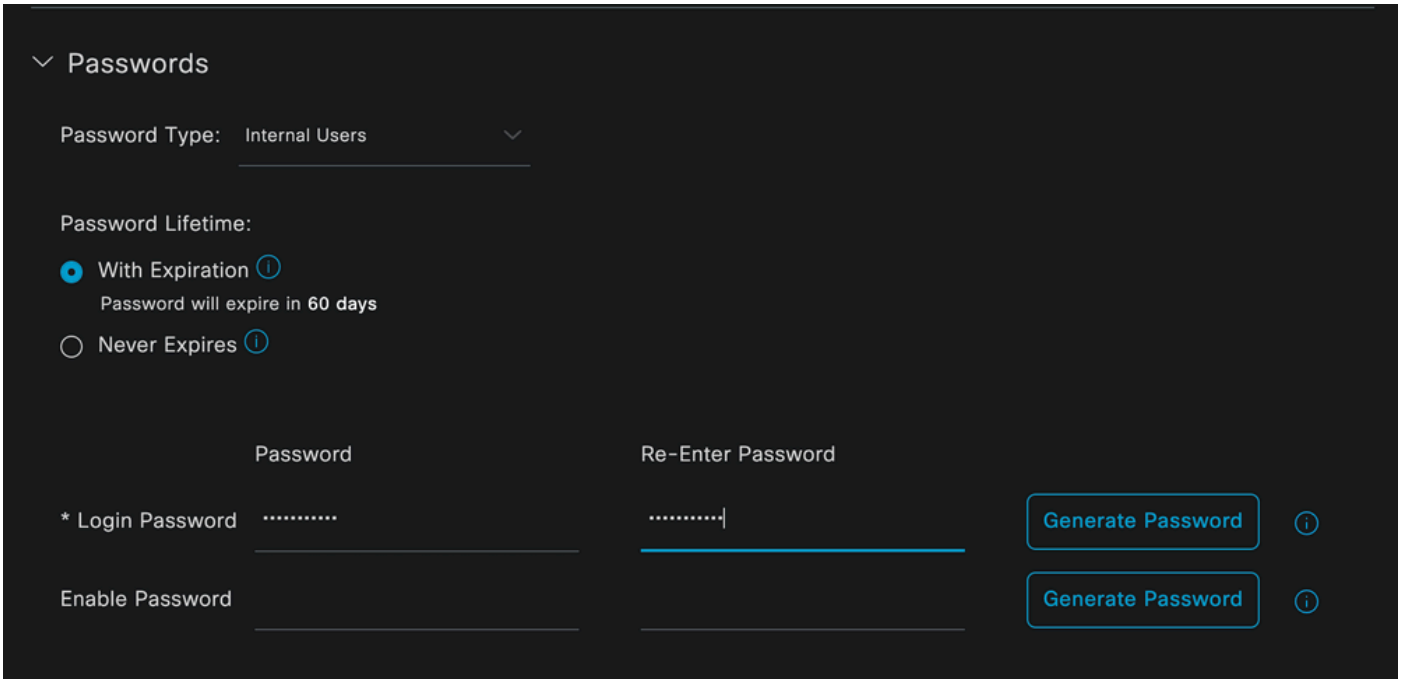

*Page Création d'utilisateur*

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



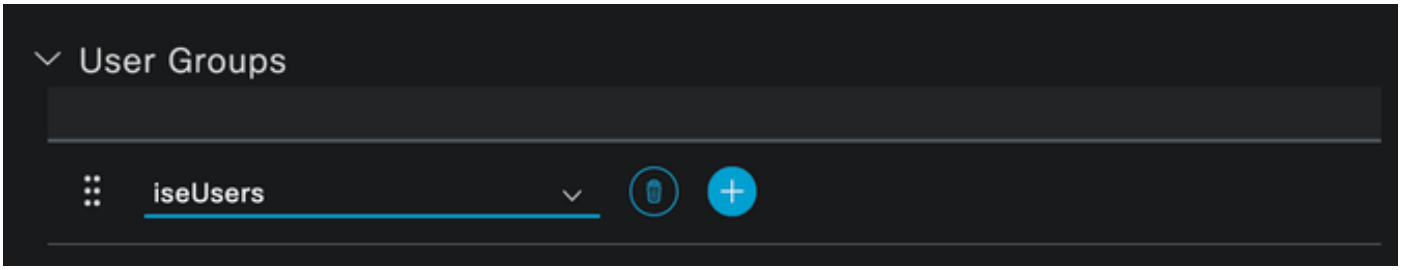

*Nom attribué au nom d'utilisateur*

L'étape suivante consiste à attribuer un mot de passe au nom d'utilisateur créé. VainillaISE97 est utilisé dans cette démonstration.




*Création de mot de passe*

Affectez l'utilisateur au groupe iseUsers.



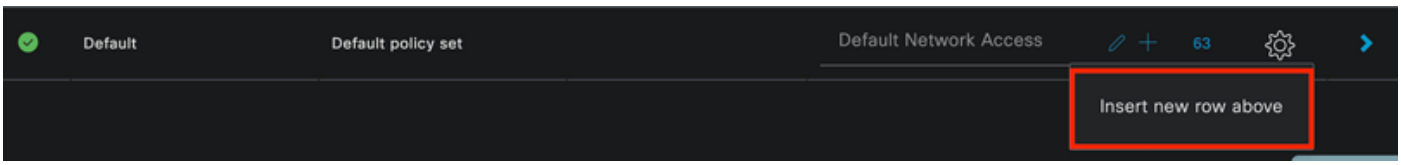

*Attribution du groupe d'utilisateurs*

2. c. Configurer l'ensemble de stratégies

Accédez au menu ISE > Policy > Policy Sets.

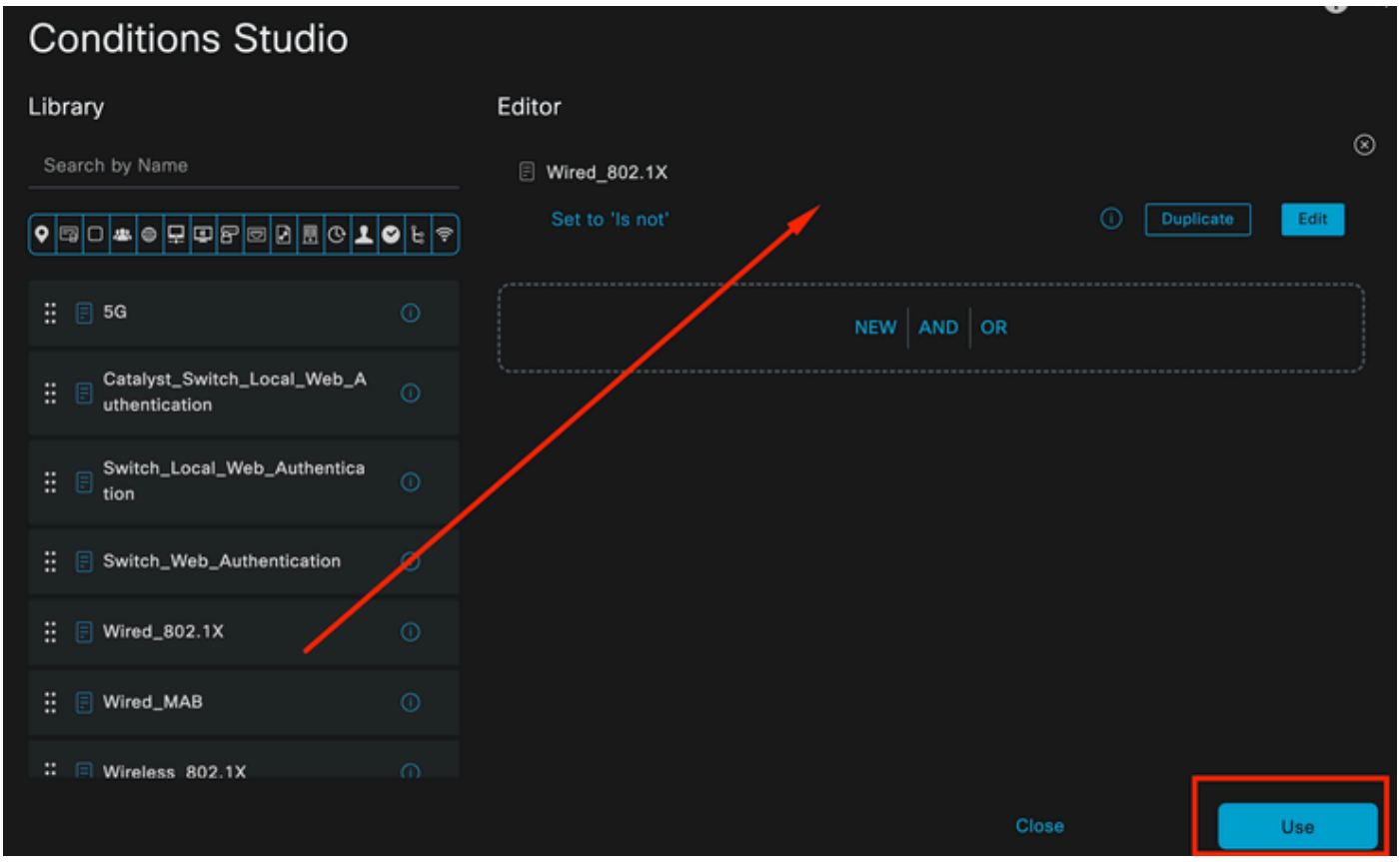
Le jeu de stratégies par défaut peut être utilisé. Cependant, dans cet exemple, un jeu de stratégies est créé et il est appelé Wired. La classification et la différenciation des ensembles de stratégies facilitent le dépannage,

Si l'icône Ajouter ou Plus n'est pas visible, vous pouvez cliquer sur l'icône d'engrenage de n'importe quel jeu de stratégies. Sélectionnez l'icône d'engrenage, puis Insérer une nouvelle ligne au-dessus.



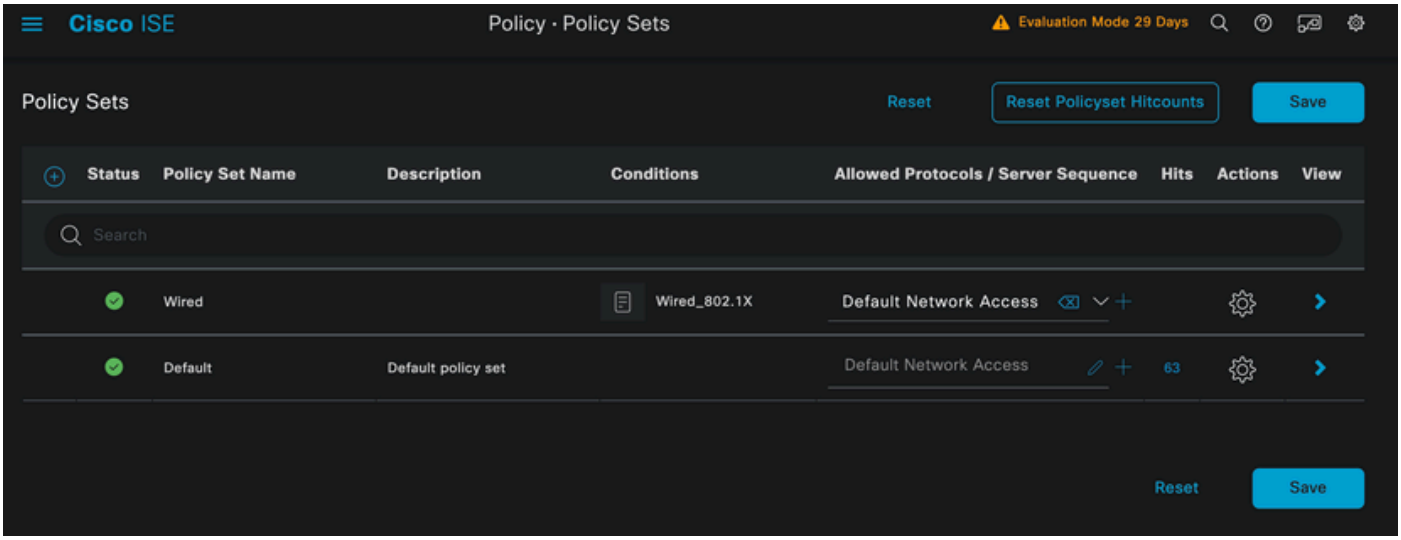

*Création de politiques*

La condition configurée dans cet exemple est Wired 8021x qui est une condition préconfigurée dans les nouveaux déploiements ISE. Faites-le glisser, puis cliquez sur Utiliser.




*Studio de condition*

Enfin, sélectionnez Default Network Access service de protocoles autorisés préconfigurés.

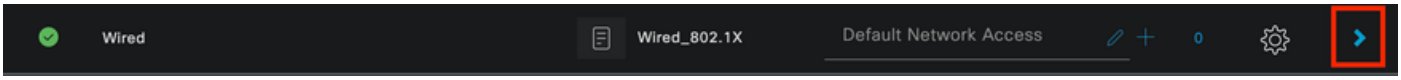



*Vue Jeu de stratégies*

Cliquez sur Save.

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

Cliquez sur la flèche située à droite de l'ensemble de stratégies que vous venez de créer.




*Ensemble de stratégies câblées*

Développer la stratégie d'authentification

Cliquez sur l'icône +.

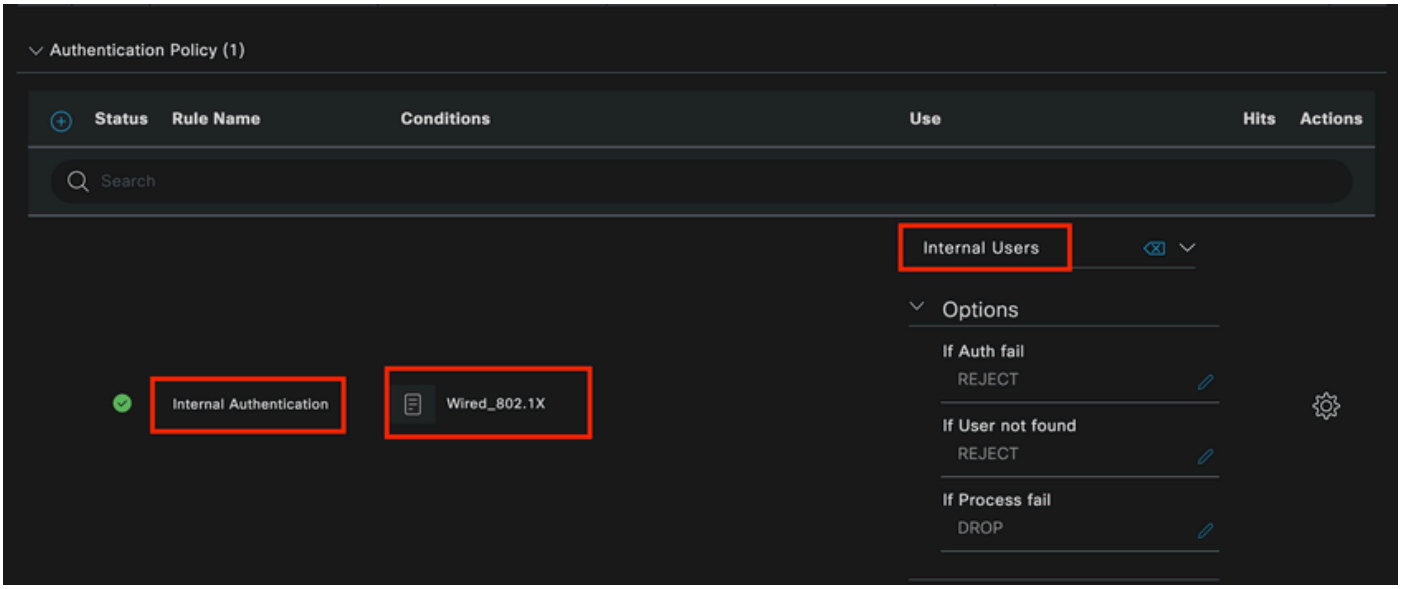

*Ajouter une stratégie d'authentification*

Attribuez un nom à la stratégie d'authentification. Dans cet exemple, l'authentification interne est utilisée.

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

La condition préconfigurée Wired Dot1x ISE est fournie avec peut être utilisée.

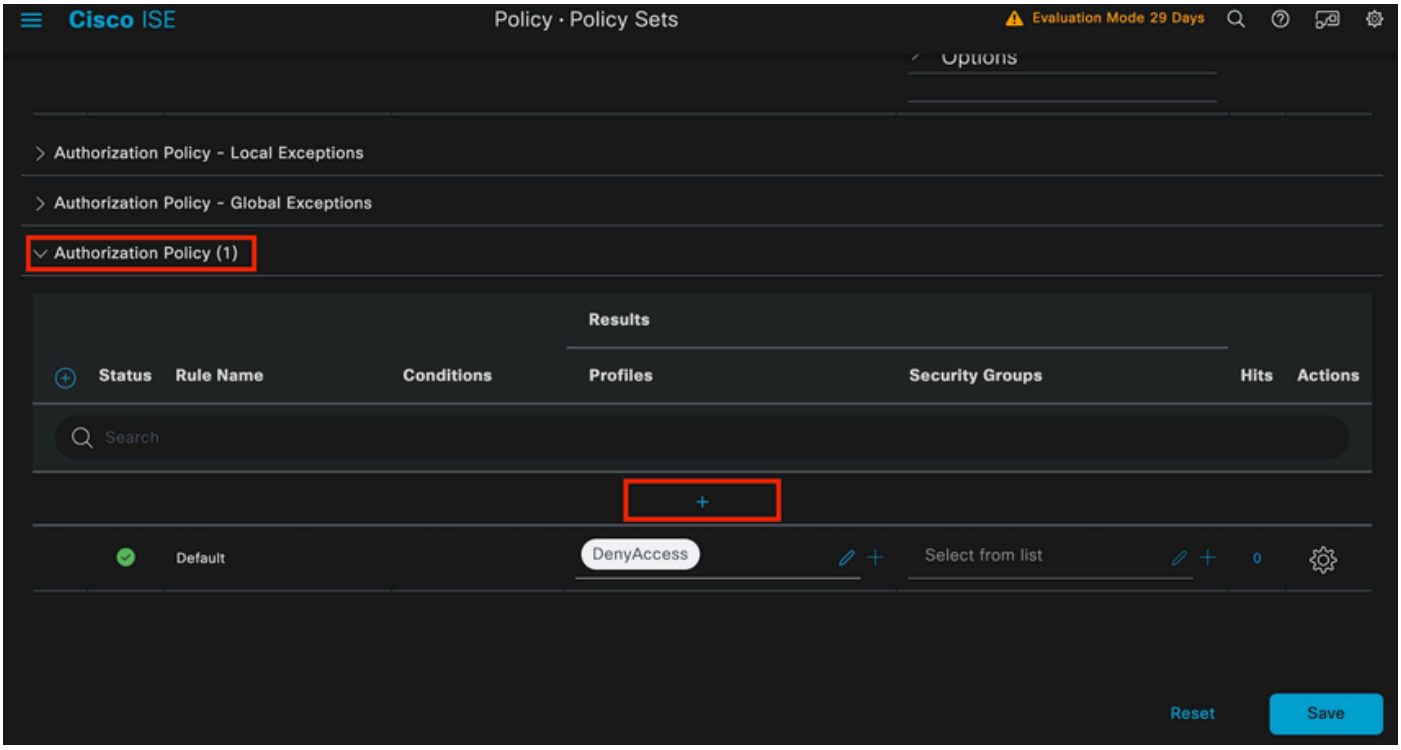
Enfin, dans la colonne Use, sélectionnez Internal Users dans la liste déroulante.




*Stratégie d'authentification*

## Politique d'autorisation

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




Politique d'autorisation

Attribuez un nom à la stratégie d'autorisation que vous venez d'ajouter, dans cet exemple de configuration, le nom Internal ISE Users est utilisé.

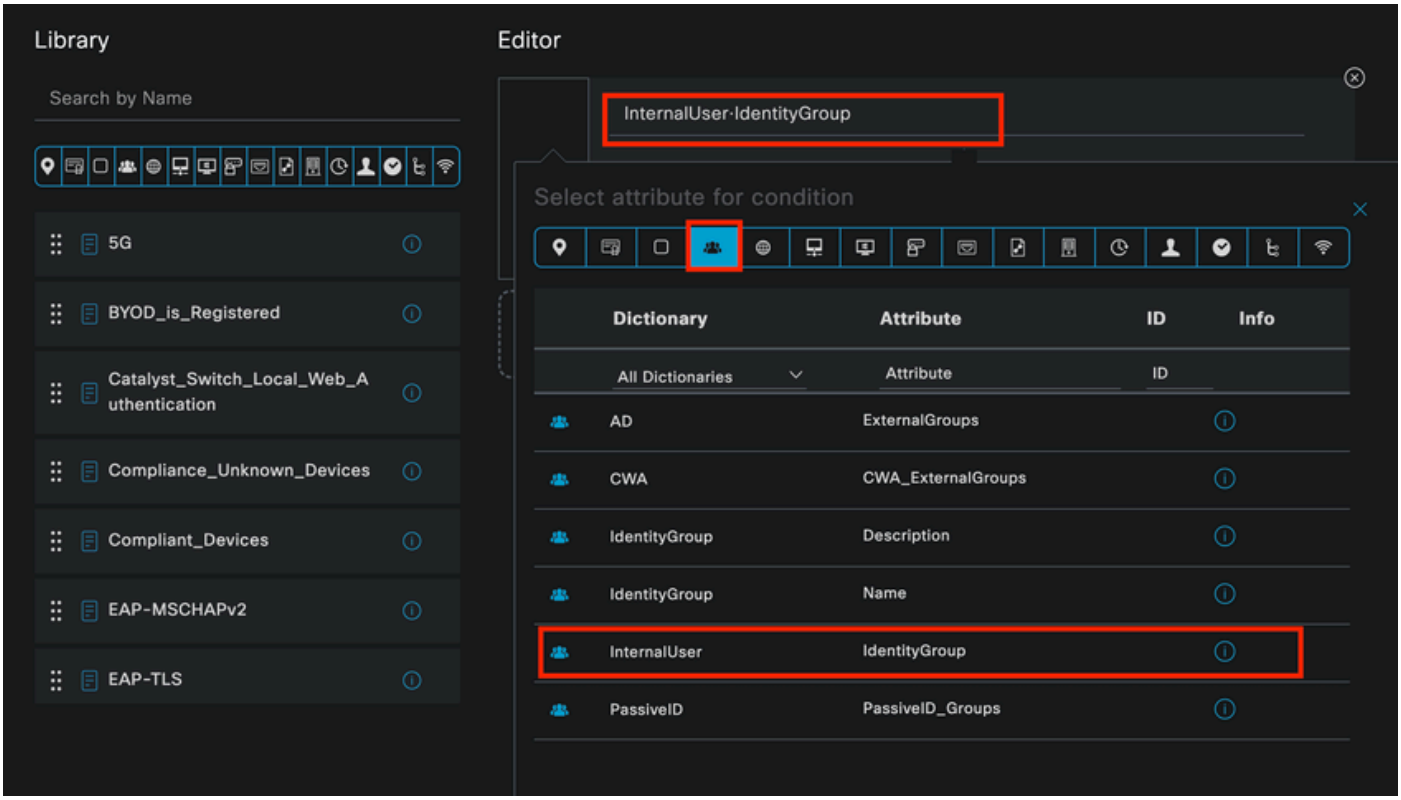
Pour créer une condition pour cette stratégie d'autorisation, cliquez sur l'icône + dans la colonne Conditions.

L'utilisateur précédemment créé fait partie du groupe IseUsers.

Une fois dans l'éditeur, cliquez sur la section Cliquez pour ajouter un attribut.

Sélectionnez l'icône Groupe d'identités.

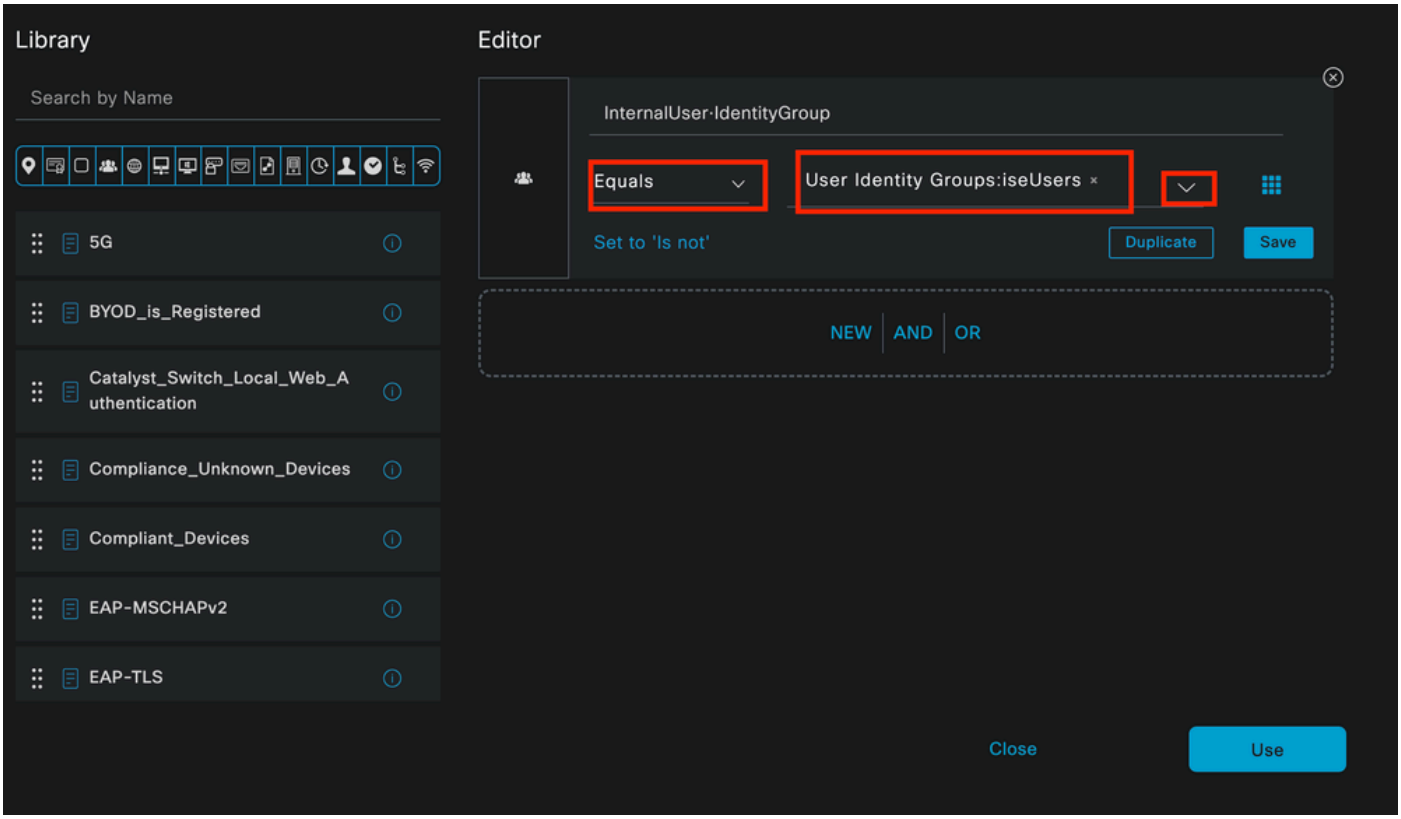
Dans le dictionnaire, sélectionnez le dictionnaire InternalUser fourni avec l'attribut Identity Group.




Studio de condition pour la stratégie d'autorisation

Sélectionnez l'opérateur Est égal à.

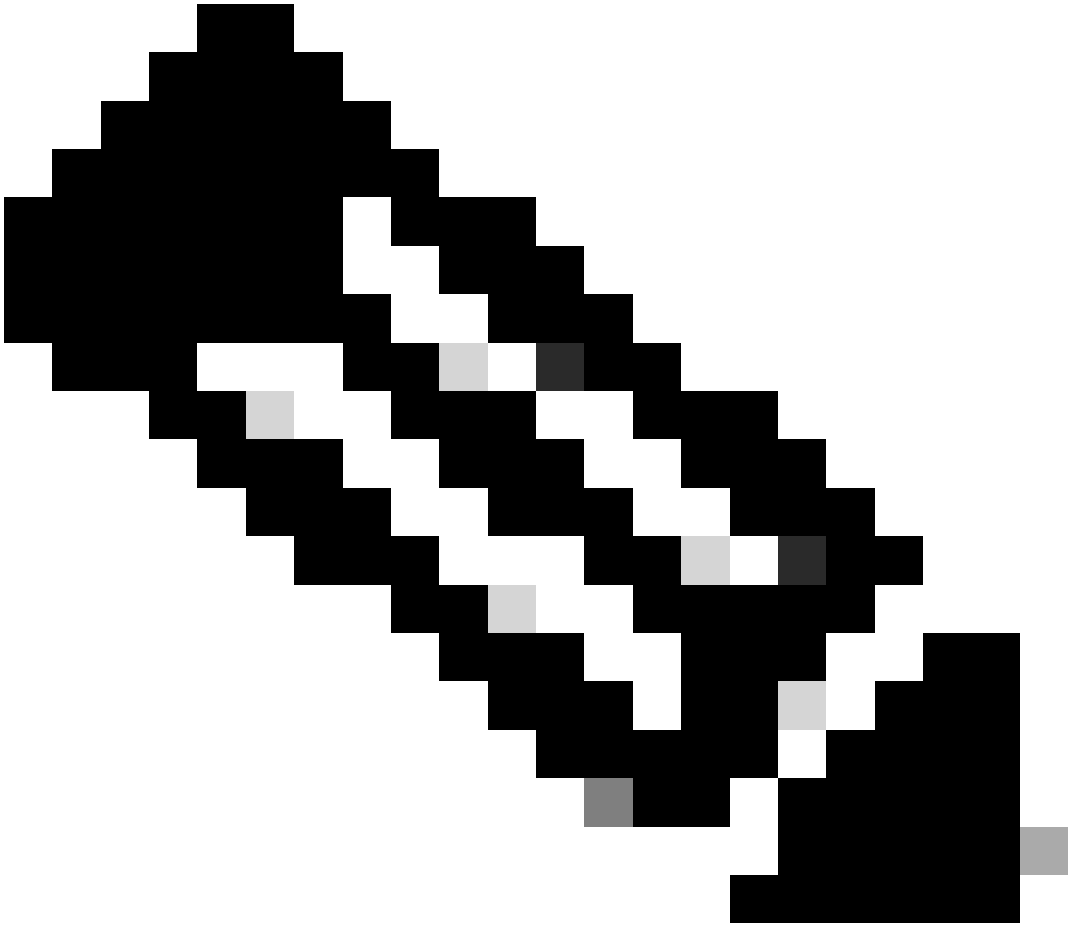
Dans la liste déroulante User Identity Groups, sélectionnez le groupe IseUsers.




*Condition de la stratégie d'autorisation terminée*

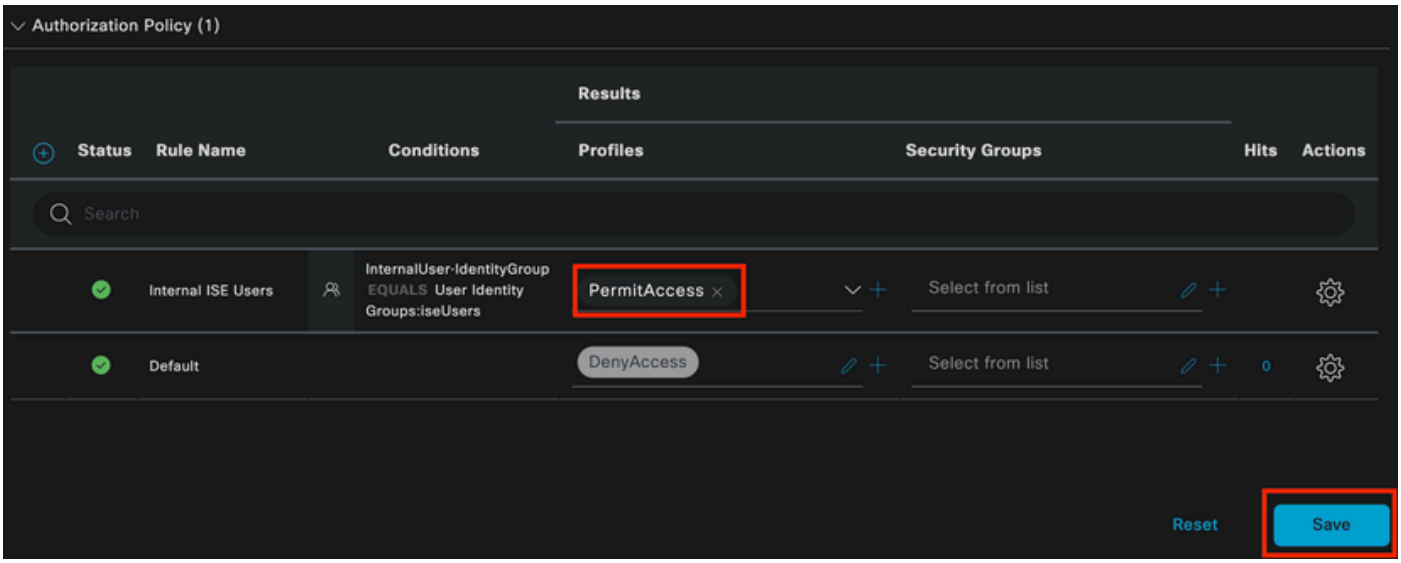
Cliquez sur Utiliser.

Enfin, sélectionnez le profil d'autorisation de résultat qui reçoit la partie authentifications de ce groupe d'identités.



Remarque : notez que les authentifications arrivant sur ISE et accédant à cet ensemble de stratégies Wired Dot1x qui ne font pas partie des utilisateurs ISEUsers du groupe d'identité des utilisateurs, accèdent maintenant à la stratégie d'autorisation par défaut. Le résultat du profil est DenyAccess.

ISE est préconfiguré avec le profil Permit Access. Sélectionnez-le.




Stratégie d'autorisation terminée

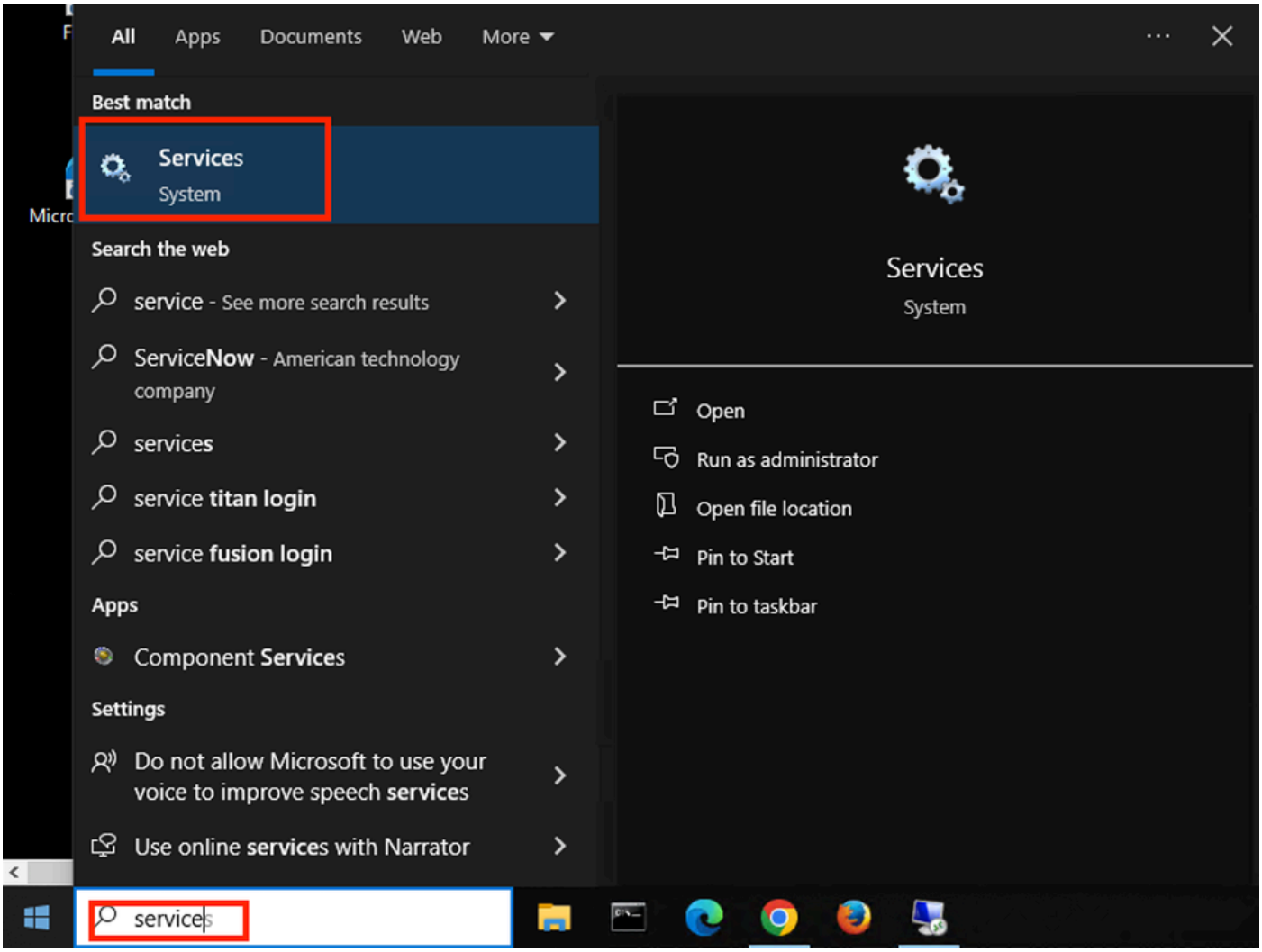
Cliquez sur Save.

La configuration d'ISE est terminée.

Étape 3. Configuration du demandeur natif Windows

3. a. Activez Wired dot1x sous Windows.

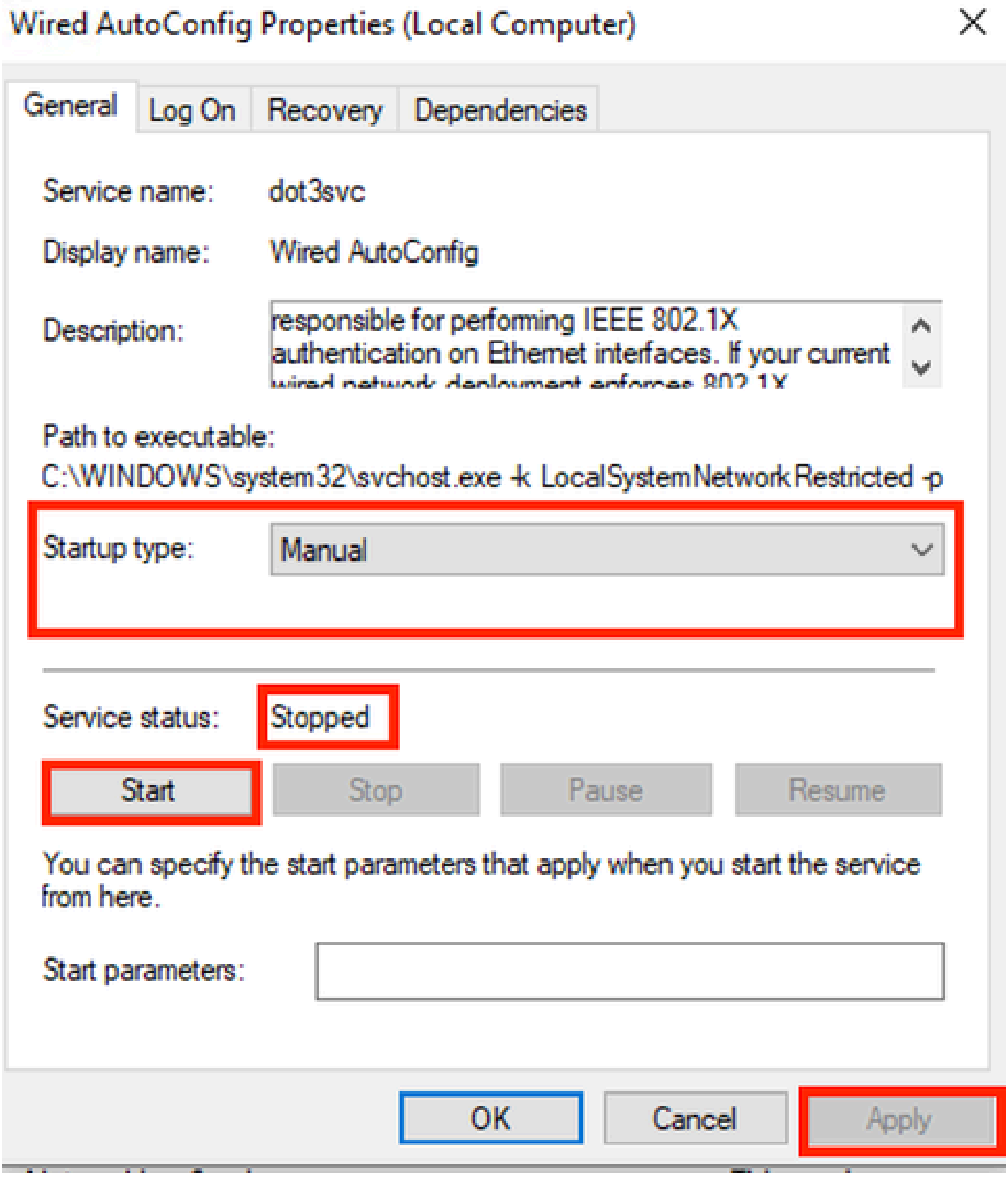
Dans la barre de recherche Windows, ouvrez Services.



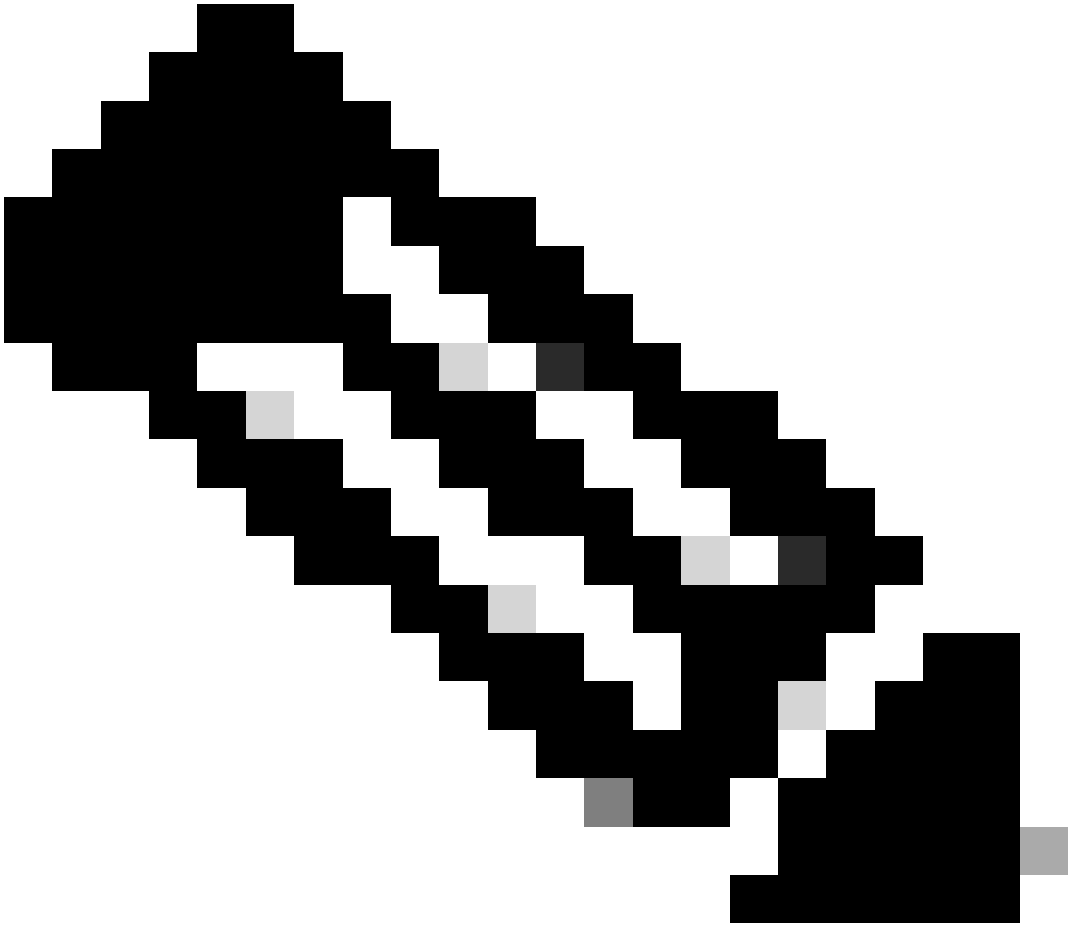

*Barre de recherche Windows*

Au bas de la liste des services, localisez Wired Autoconfig.

Cliquez avec le bouton droit sur Wired AutoConfig et sélectionnez Propriétés.



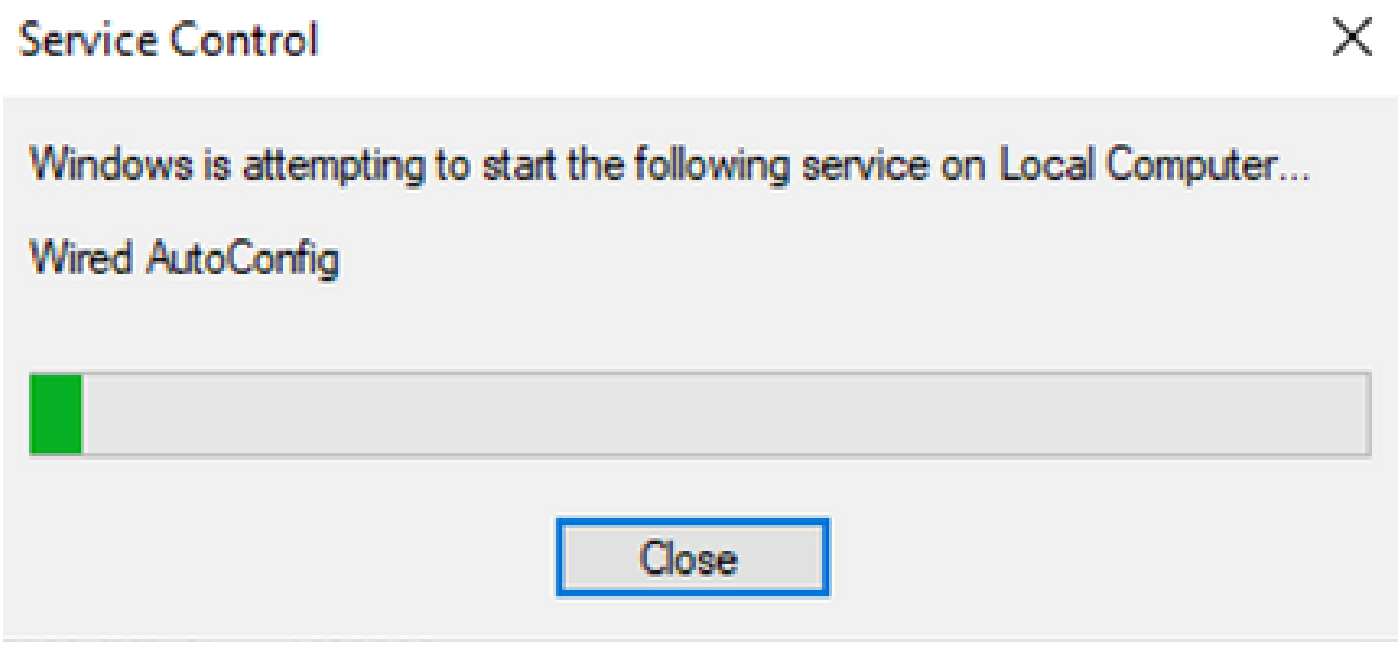

*Fenêtre Propriétés*



Remarque : le service de configuration automatique câblée (DOT3SVC) est chargé d'effectuer l'authentification IEEE 802.1X sur les interfaces Ethernet.

Le type de démarrage Manuel est sélectionné.

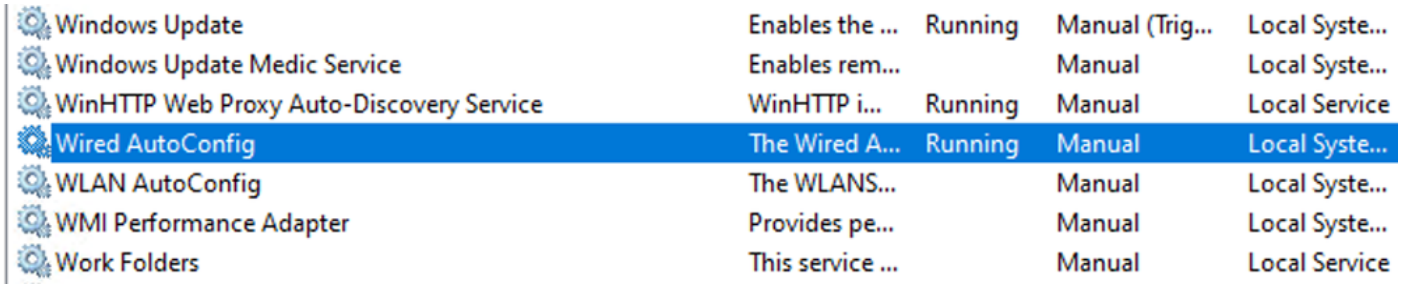
Puisque l'état du service est Arrêté. Cliquez sur Démarrer.




*Contrôle des services*

Cliquez ensuite sur OK.

Le service s'exécute ensuite.



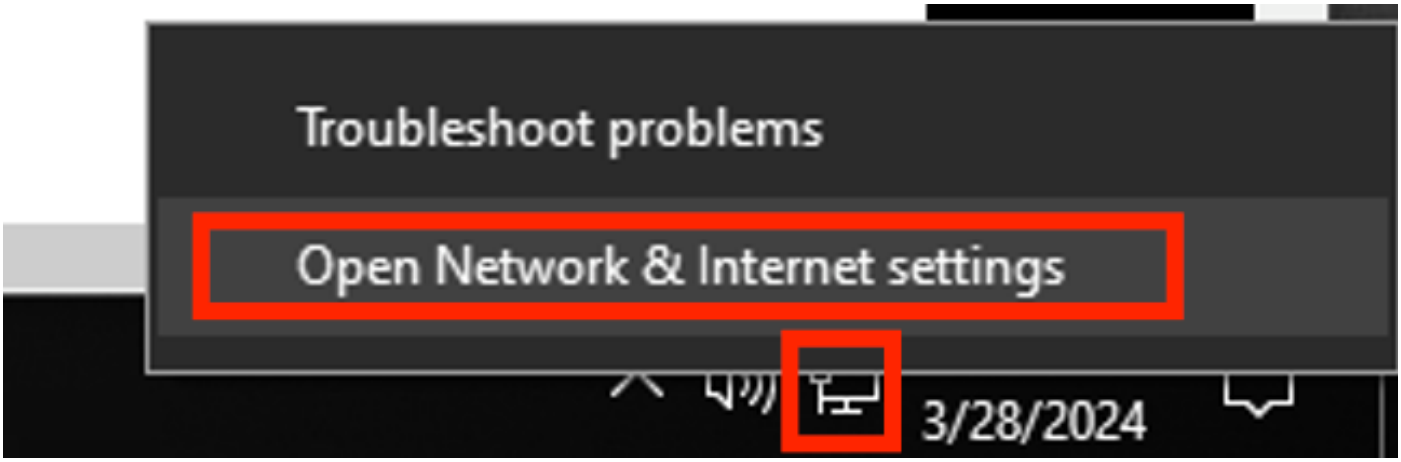

*Service de configuration automatique filaire*

3. b. Configurez l'interface de l'ordinateur portable Windows connectée à l'authentificateur NAD (ISR 1100).

Dans la barre des tâches, localisez le coin droit, puis utilisez l'icône de l'ordinateur.

Double-cliquez sur l'icône de l'ordinateur.

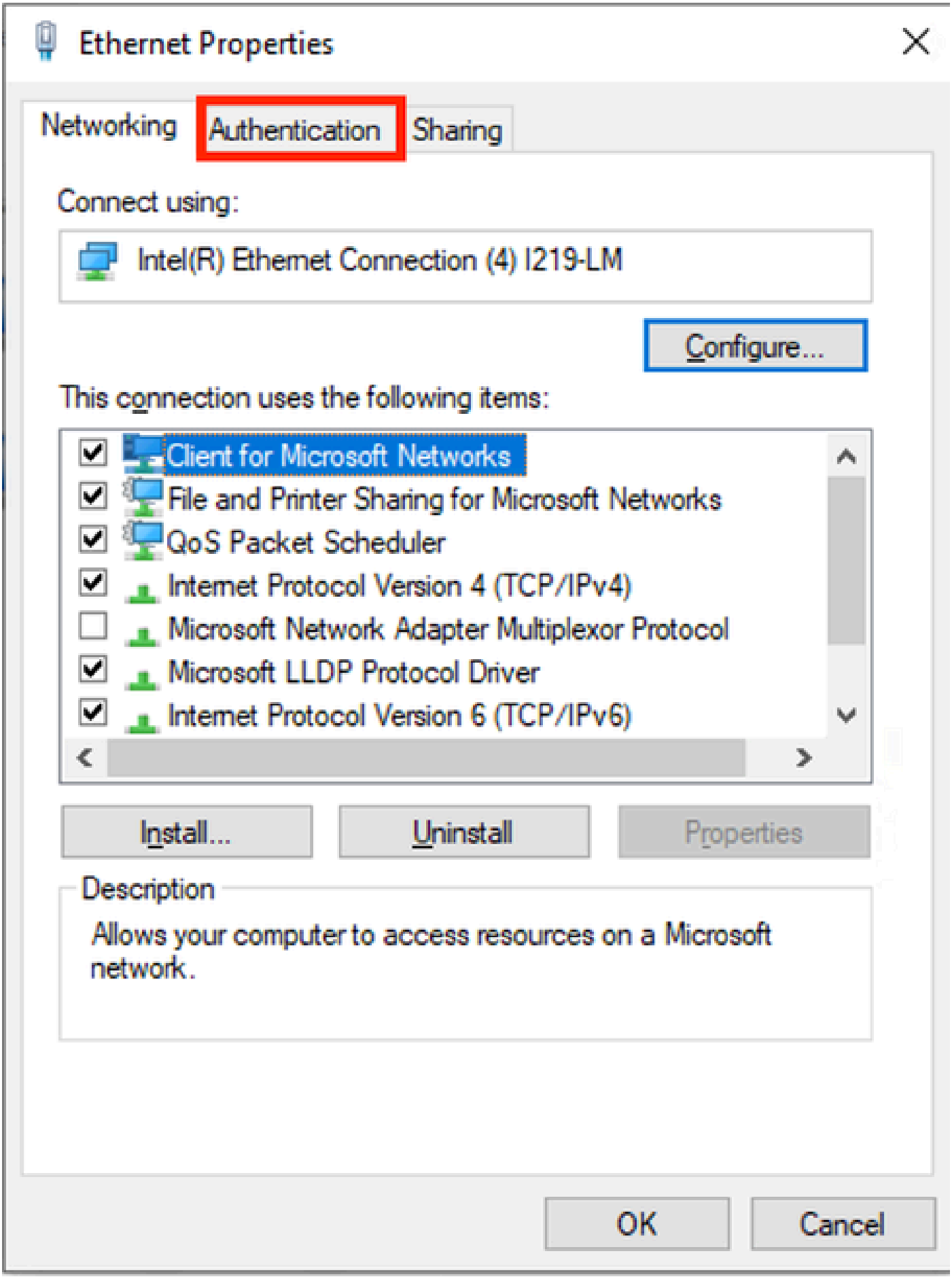
Sélectionnez Ouvrir les paramètres réseau et Internet.




*Barre des tâches Windows*

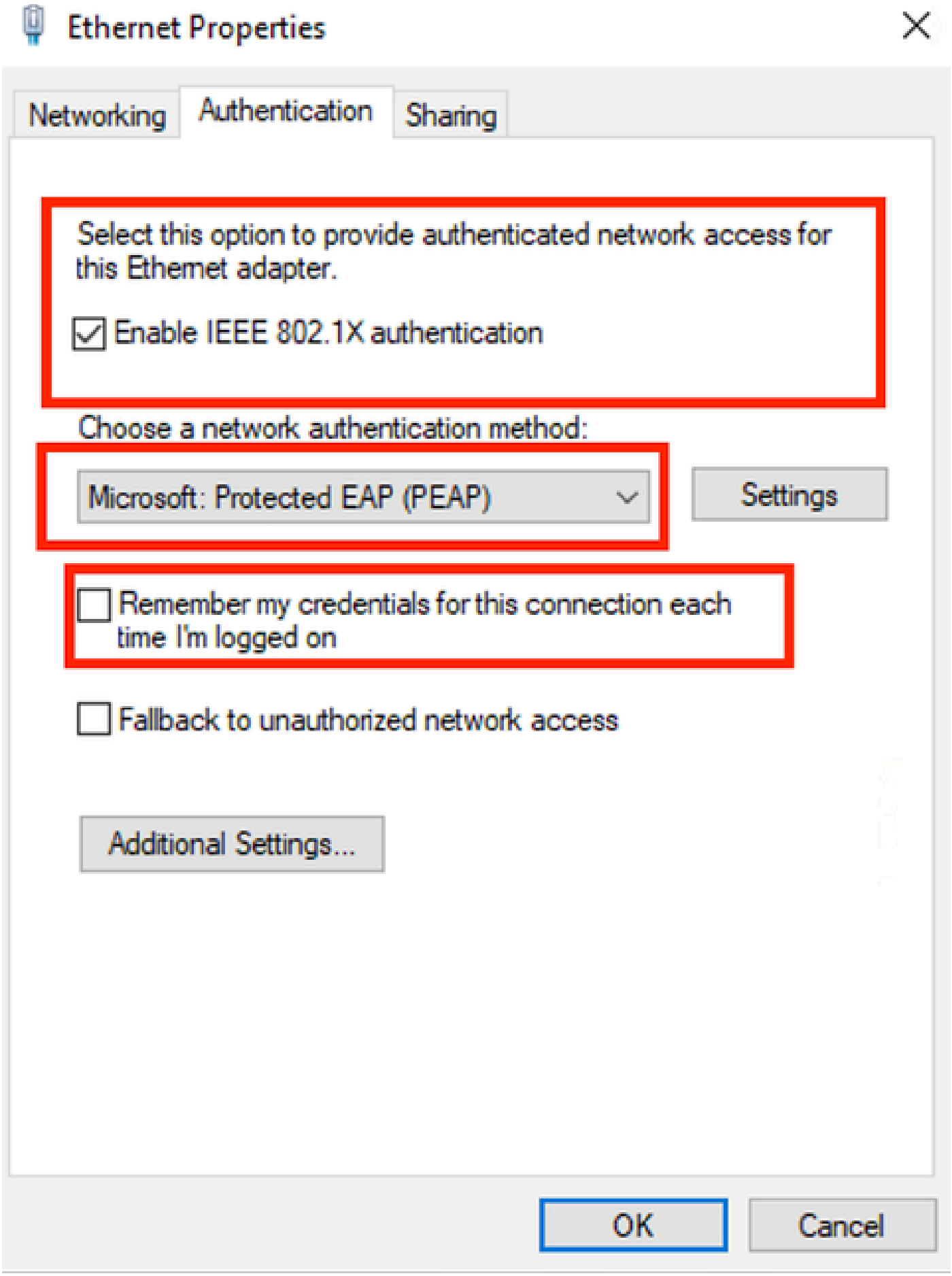
Une fois la fenêtre Connexions réseau ouverte, cliquez avec le bouton droit de la souris sur l'interface Ethernet connectée à l'ISR Gig 0/1/0. Cliquez sur l'option Propriétés.

Cliquez sur l'onglet Authentification.




*Propriétés Ethernet d'interface*

Cochez la case Enable IEEE 802.1X authentication.

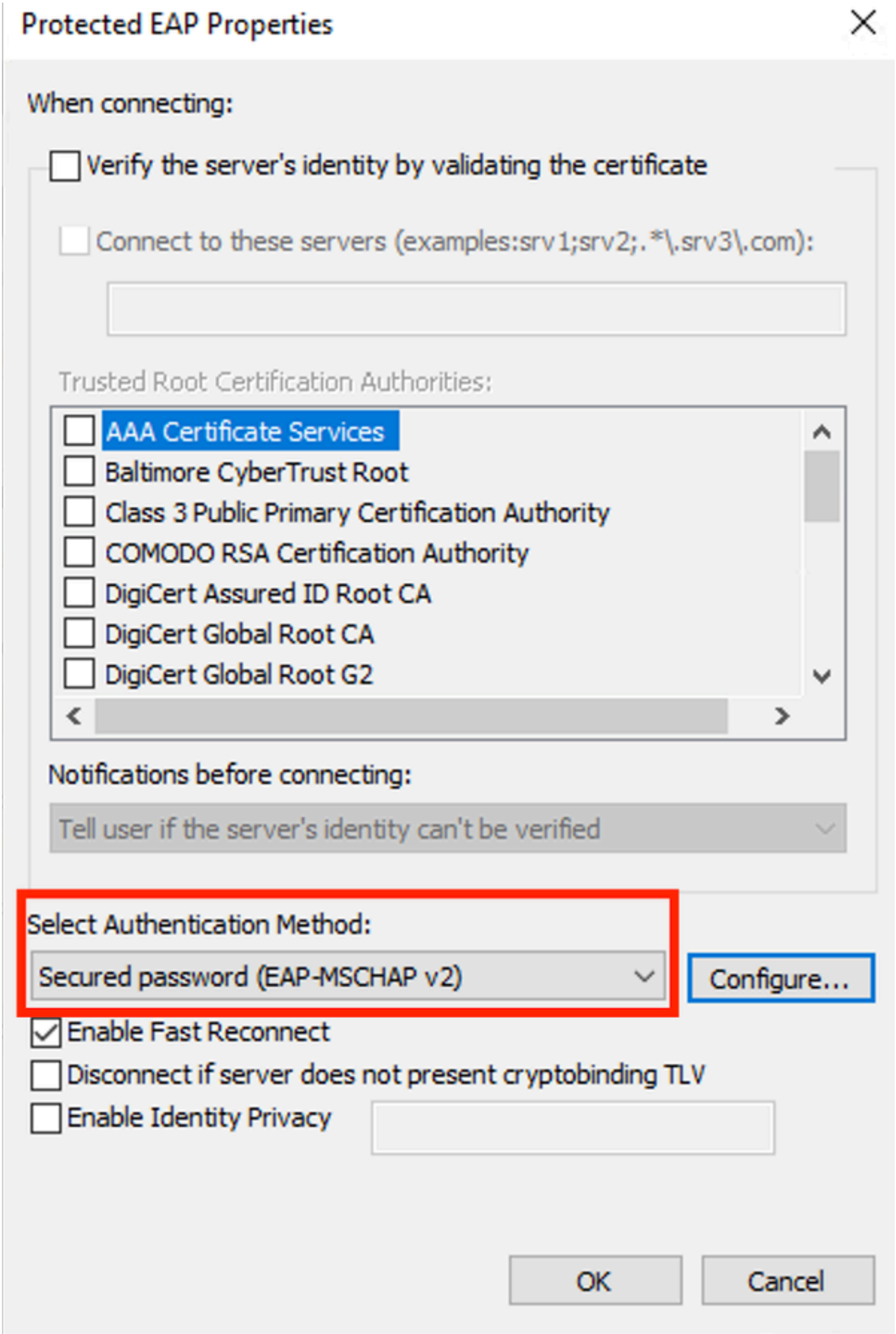



*Authentification Propriétés Ethernet*

Sélectionnez Protected EAP (PEAP).

Désactivez l'option Mémoriser mes informations d'identification pour cette connexion chaque fois que je suis connecté.

Cliquez sur Paramètres.




*Propriétés PEAP*

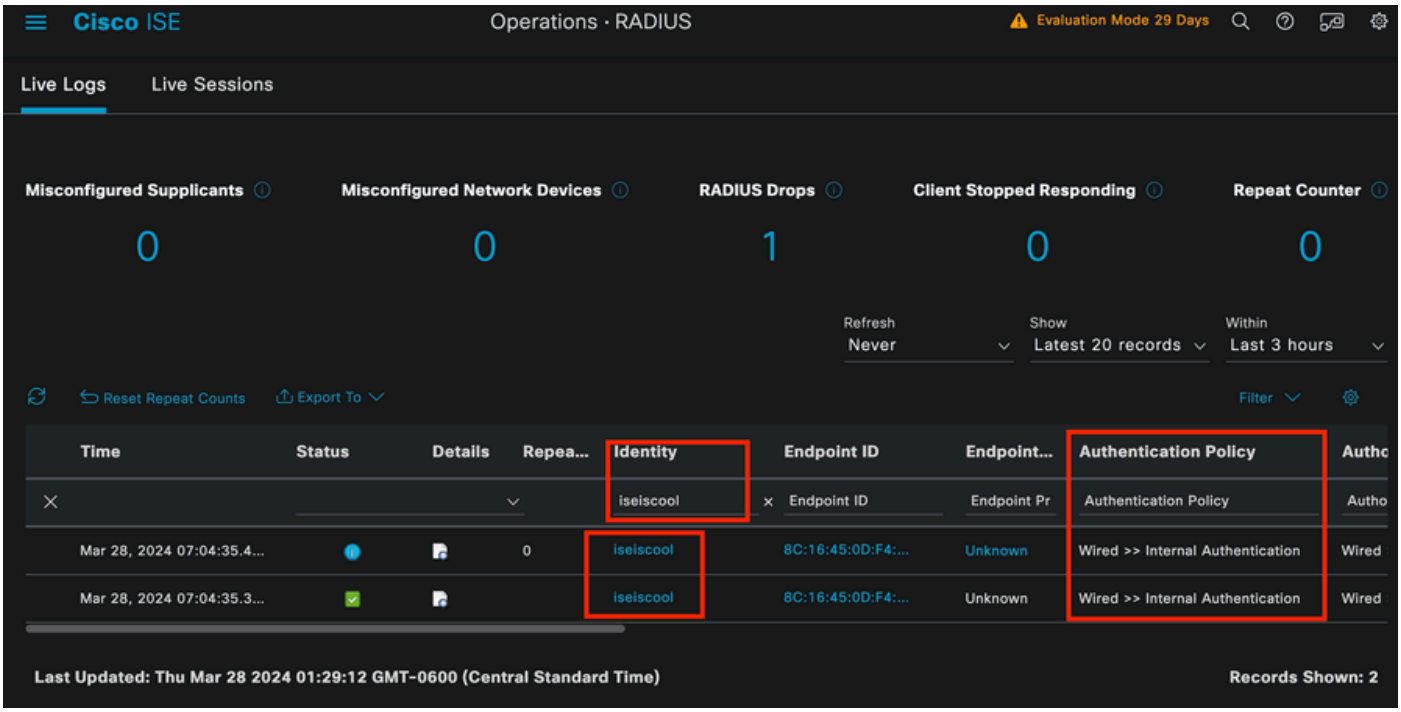
```
            Interface:  GigabitEthernet0/1/0
                IIF-ID:  0x08767C0D
           MAC Address:  8c16.450d.f42b
          IPv6 Address:  Unknown
          IPv4 Address:  Unknown
             User-Name:  iseiscool <--------- The username configured for Windows Native Supplicant
                Status:  Authorized <--------- An indication that this session was authorized by the PSN
                Domain:  DATA
        Oper host mode:  multi-auth
      Oper control dir:  both
       Session timeout:  N/A
     Common Session ID:  22781F0A0000000C83E28461
       Acct Session ID:  0x00000003
                Handle:  0xc6000002
        Current Policy:  POLICY_Gi0/1/0

Local Policies:
         Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
       Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
         dot1x          Authc Success <--------- An indication that dot1x is used for this authenticati
```

```
Router#
```

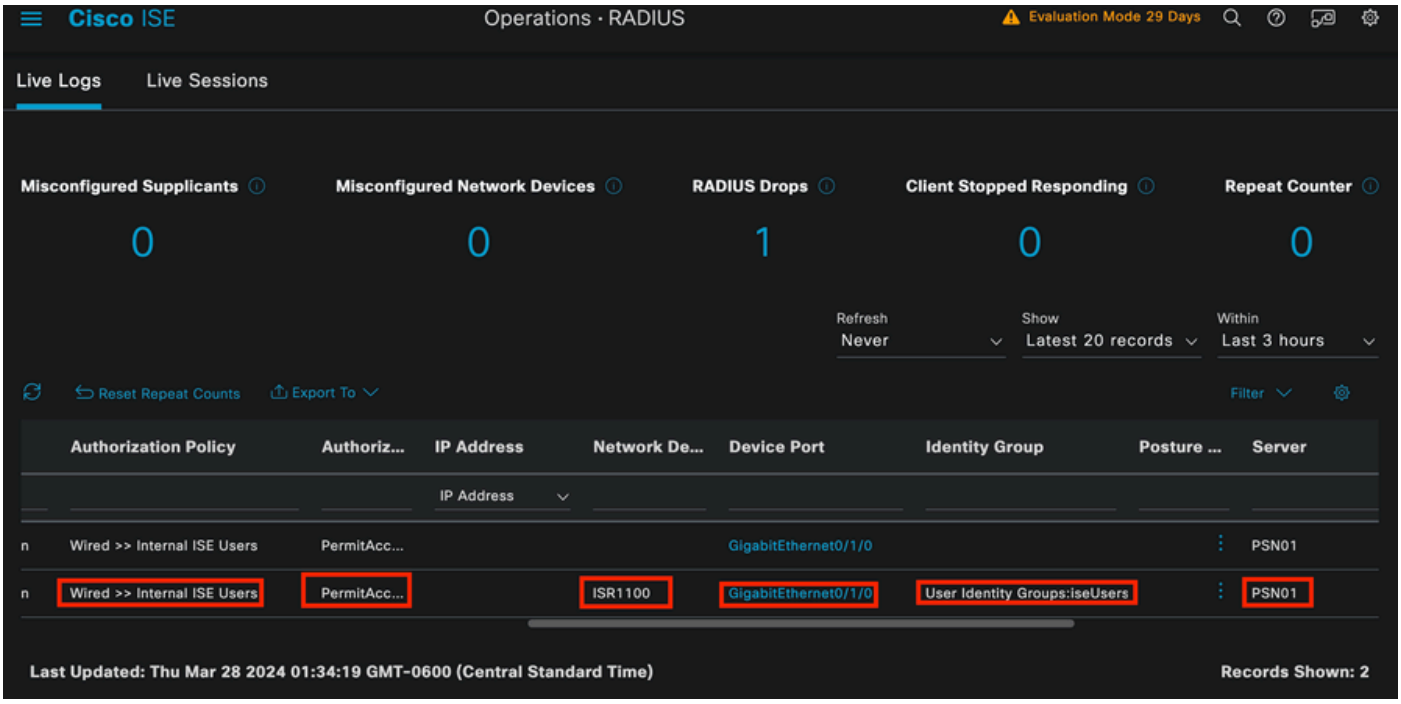
Journaux ISE

Accédez à Operations > Radius > Live logs tab.

Filtrez par l'identité du nom d'utilisateur. Dans cet exemple, le nom d'utilisateur iseiscool est utilisé.




*ISE Livelogs*




*ISE Livelogs*

Notez que dans cette vue rapide, les journaux en direct fournissent des informations clés :

- Horodatage de l'authentification.
- Identité utilisée.
- Adresse MAC du terminal.
- Ensemble de stratégies et stratégie d'authentification qui a été atteinte.
- Ensemble de stratégies et stratégie d'autorisation qui a été atteinte.
- Résultat du profil d'autorisation.
- Périphérique réseau qui envoie la requête Radius à ISE.
- Interface à laquelle le point d'extrémité est connecté.
- Groupe d'identités de l'utilisateur authentifié.
- Noeud de serveur de stratégie (PSN) qui a géré l'authentification.

# Dépannage

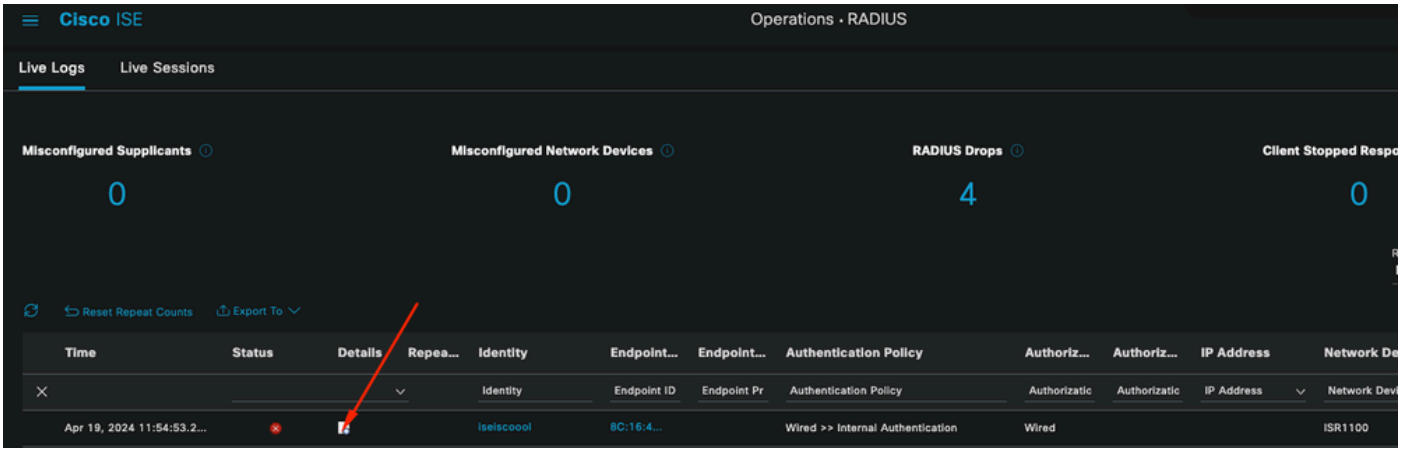
1 - Lecture des détails du journal en direct ISE

Accédez à Operations > Radius > Live logs tab, filtrez par Auth status : Failed OU par le nom d'utilisateur utilisé OU par l'adresse MAC OU par le périphérique d'accès réseau utilisé.

Accédez à Operations > Radius > Live logs > Desired authentication > Live log details.

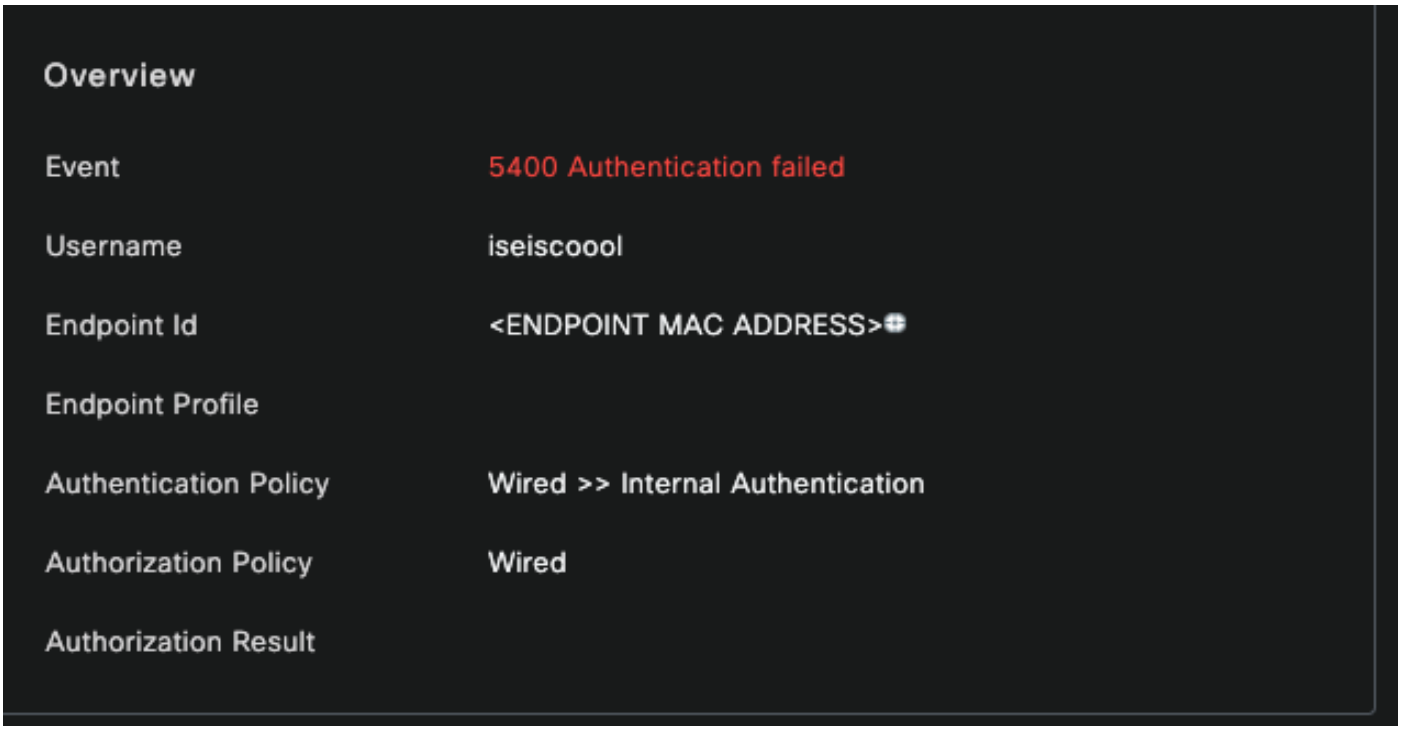
Sur la même page, une fois l'authentification filtrée, cliquez sur l'icône Search.

Premier scénario : l'utilisateur saisit son nom d'utilisateur avec une faute de frappe.



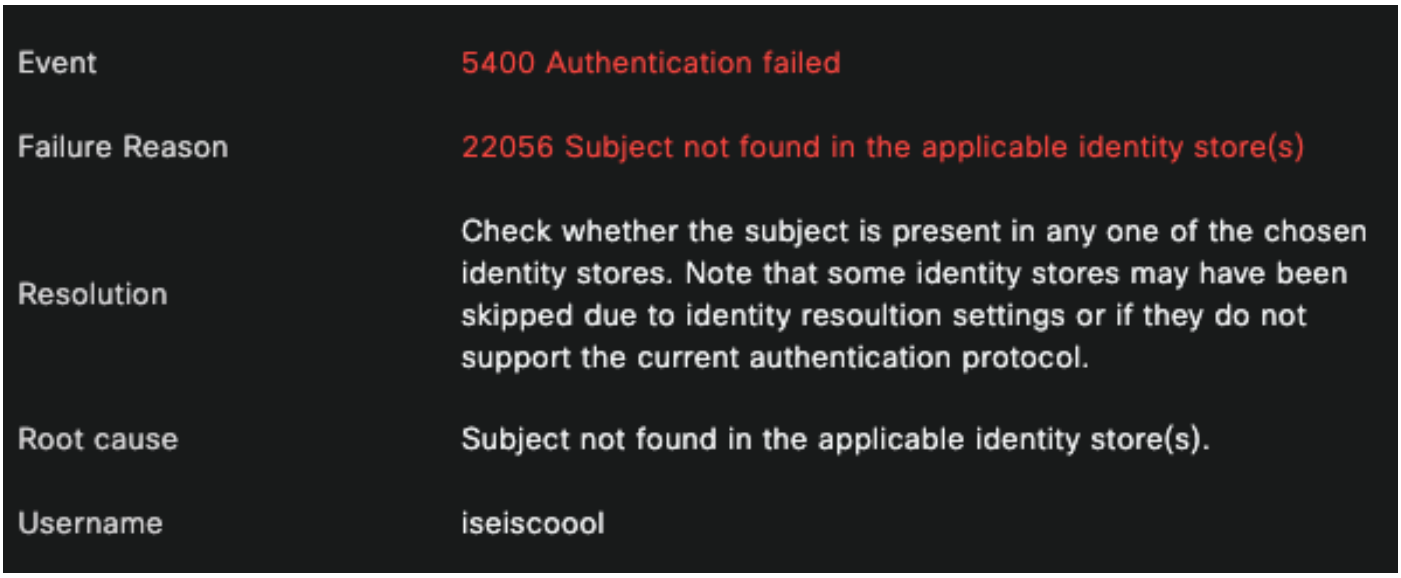

Ouverture des détails du journal dynamique

Une fois les détails du journal en direct ouverts, vous pouvez voir que l'authentification a échoué et que le nom d'utilisateur utilisé est également répertorié.




Section Présentation

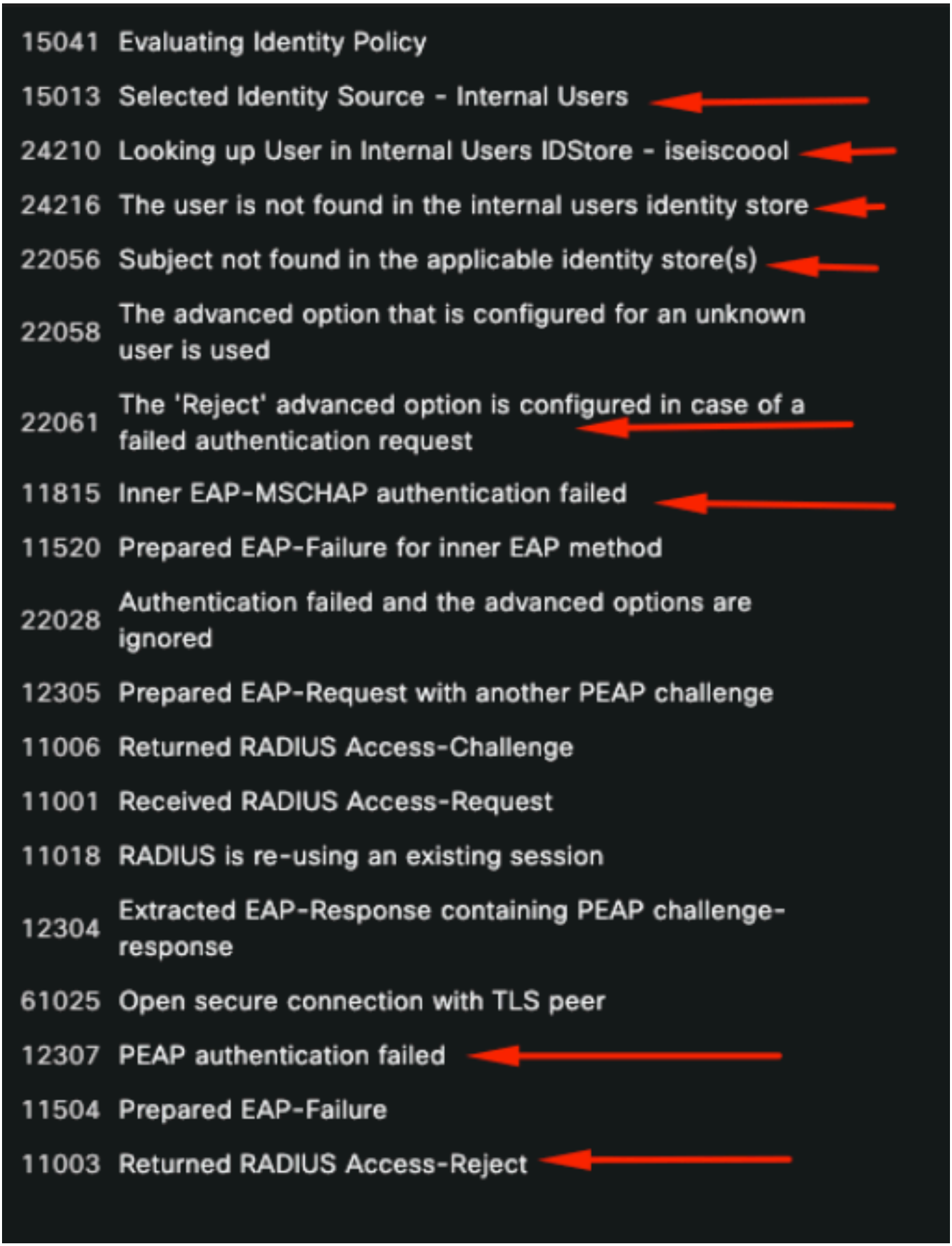
Ensuite, sur le même détail de journal en direct, dans la section Détails d'authentification, il peut être trouvé la raison de l'échec, la cause première, et la résolution de l'erreur.




Détails d'authentification

Dans ce scénario, la raison de l'échec de l'authentification est que le nom d'utilisateur a une faute de frappe. Toutefois, cette même erreur serait présentée si l'utilisateur n'est pas créé dans ISE ou si ISE n'a pas pu valider que l'utilisateur existe dans d'autres magasins d'identité, par exemple, LDAP ou AD.

Section Étapes




Section Étape Détails du journal en direct

La section des étapes décrit en détail le processus exécuté par ISE au cours de la conversation

RADIUS.

Vous pouvez trouver des informations ici comme :

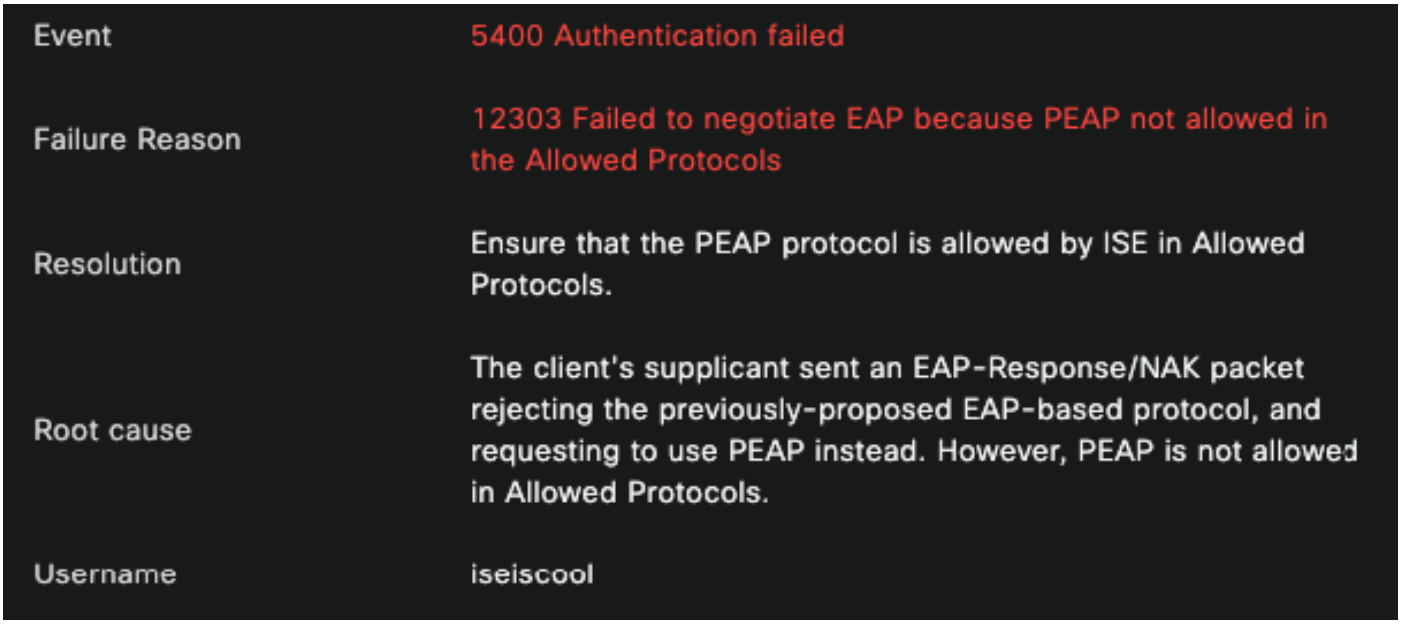
- Comment la conversation a commencé.
- Processus de connexion SSL.
- La méthode EAP négociée.
- Processus de méthode EAP.

Dans cet exemple, on peut voir qu'ISE vient de vérifier les identités internes pour cette authentification. L'utilisateur est introuvable et, pour cette raison, ISE a envoyé une réponse Access-Reject.

Deuxième scénario : l'administrateur ISE a désactivé le protocole PEAP dans les protocoles Policy Set Allowed.

2 - PEAP désactivé

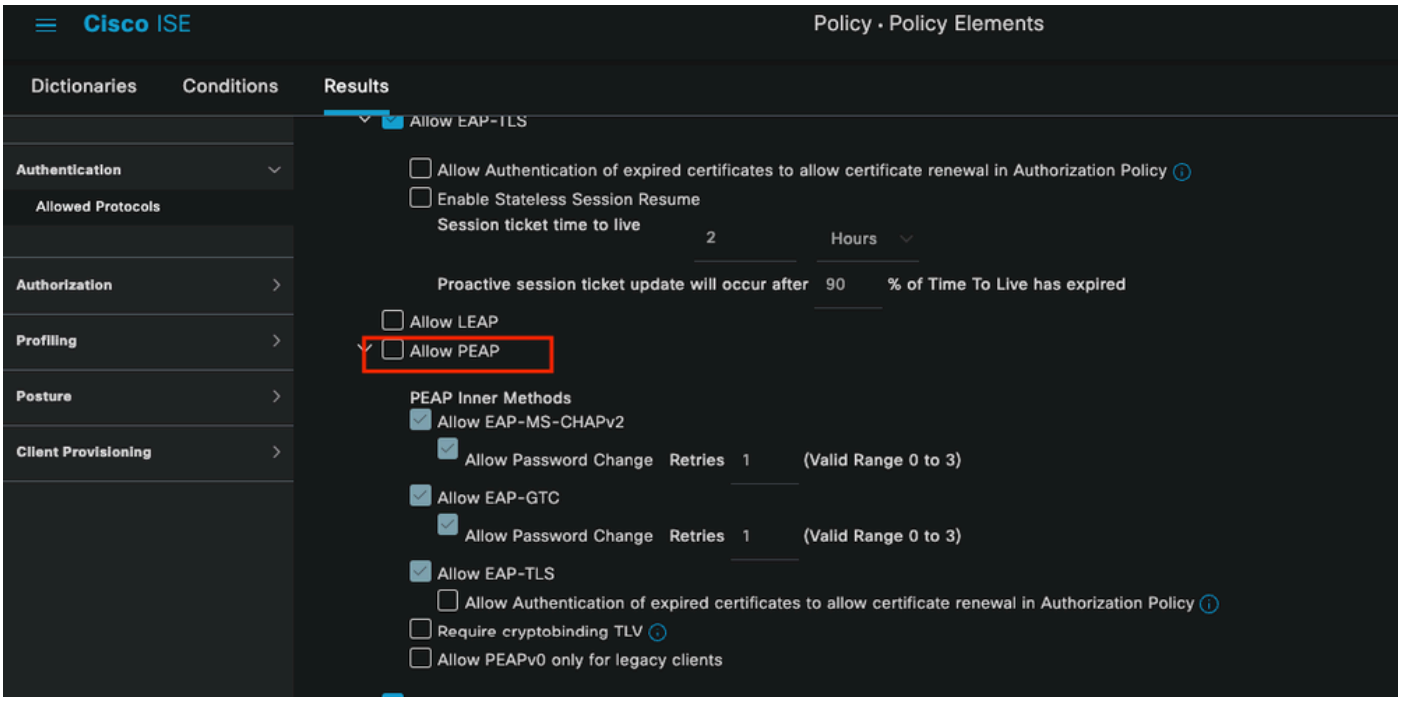
Une fois que les détails du journal en direct de la session défaillante sont ouverts, le message d'erreur « PEAP is not allowed in the Allowed Protocols » s'affiche.



| | |
|---|---|
| Event | 5400 Authentication failed |
| Failure Reason | 12303 Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols |
| Resolution | Ensure that the PEAP protocol is allowed by ISE in Allowed Protocols. |
| Root cause | The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead. However, PEAP is not allowed in Allowed Protocols. |
| Username | iseiscool |

Rapport détaillé du journal en direct

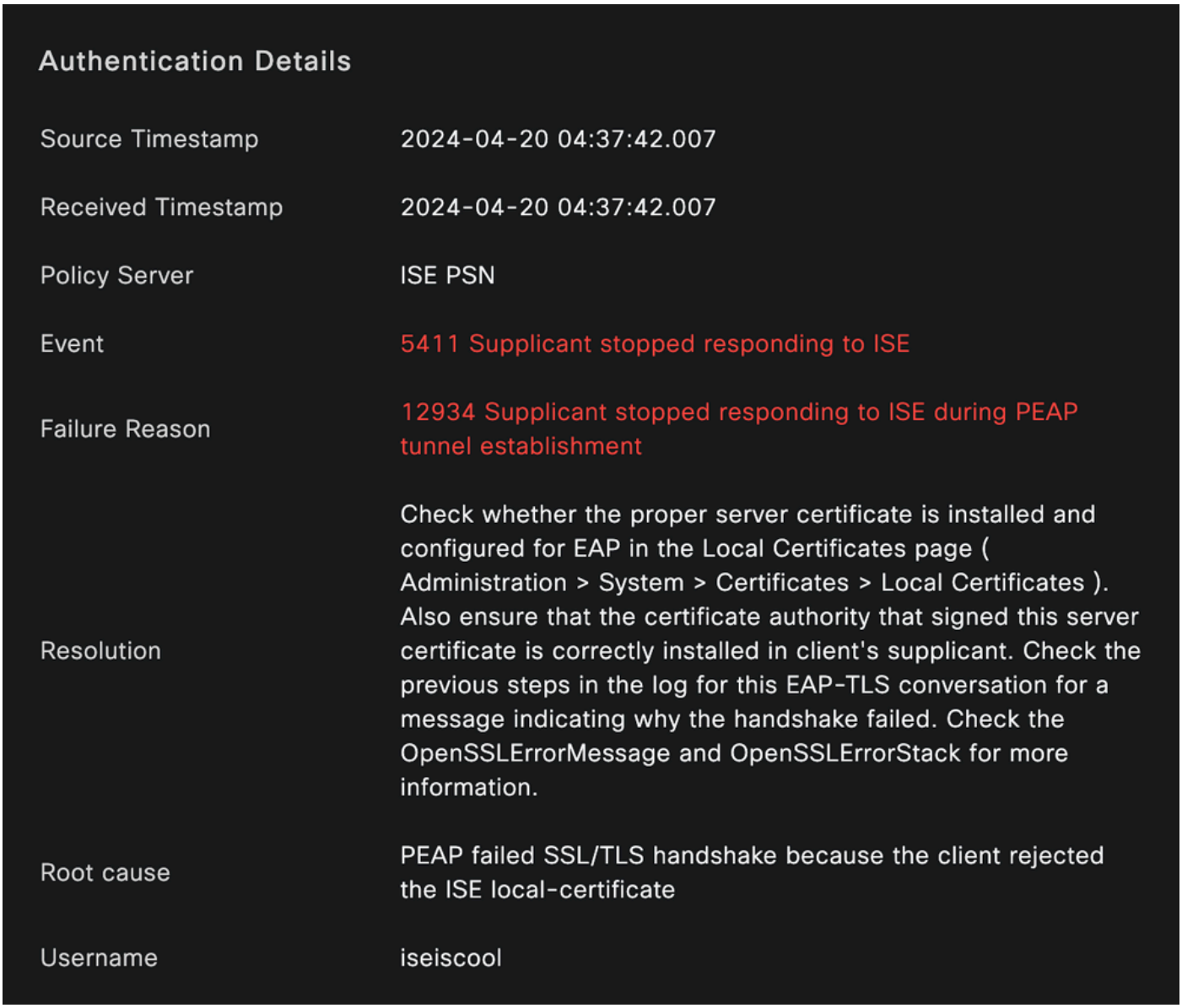
Cette erreur est facile à résoudre, la résolution est de naviguer vers Policy > Policy Elements > Authentication > Allowed Protocols. Vérifiez si l'option Allow PEAP est désactivée.




Section Protocoles autorisés

Troisième scénario : l'authentification échoue car le point d'extrémité n'approuve pas le certificat ISE.

Accédez aux détails du journal en direct. Recherchez l'enregistrement correspondant à l'échec de l'authentification et vérifiez les détails du journal en direct.

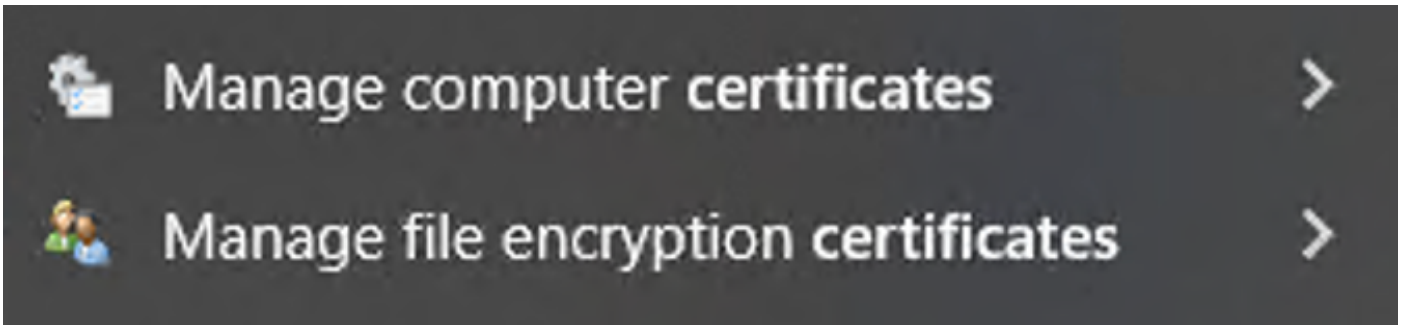



Détails du journal en direct

Le point d'extrémité rejette le certificat utilisé pour l'établissement du tunnel PEAP.

Pour résoudre ce problème, dans le point de terminaison Windows où vous avez le problème, vérifiez que la chaîne de l'autorité de certification qui a signé le certificat ISE se trouve dans la section Windows Manage User Certificates > Trusted Root Certification Authorities OU Manage Computer Certificates > Trusted Root Certification Authorities.

Vous pouvez accéder à cette section de configuration sur votre périphérique Windows en effectuant une recherche dans la barre de recherche Windows.

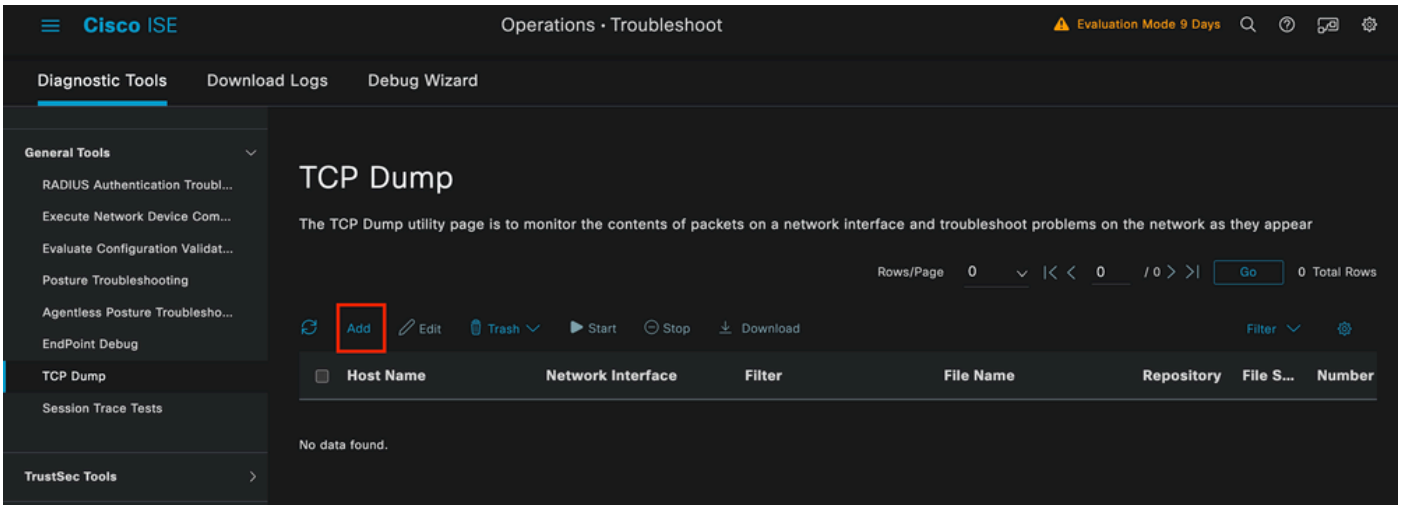



Résultats de la barre de recherche Windows

3 - Outil de vidage TCP ISE (capture de paquets)

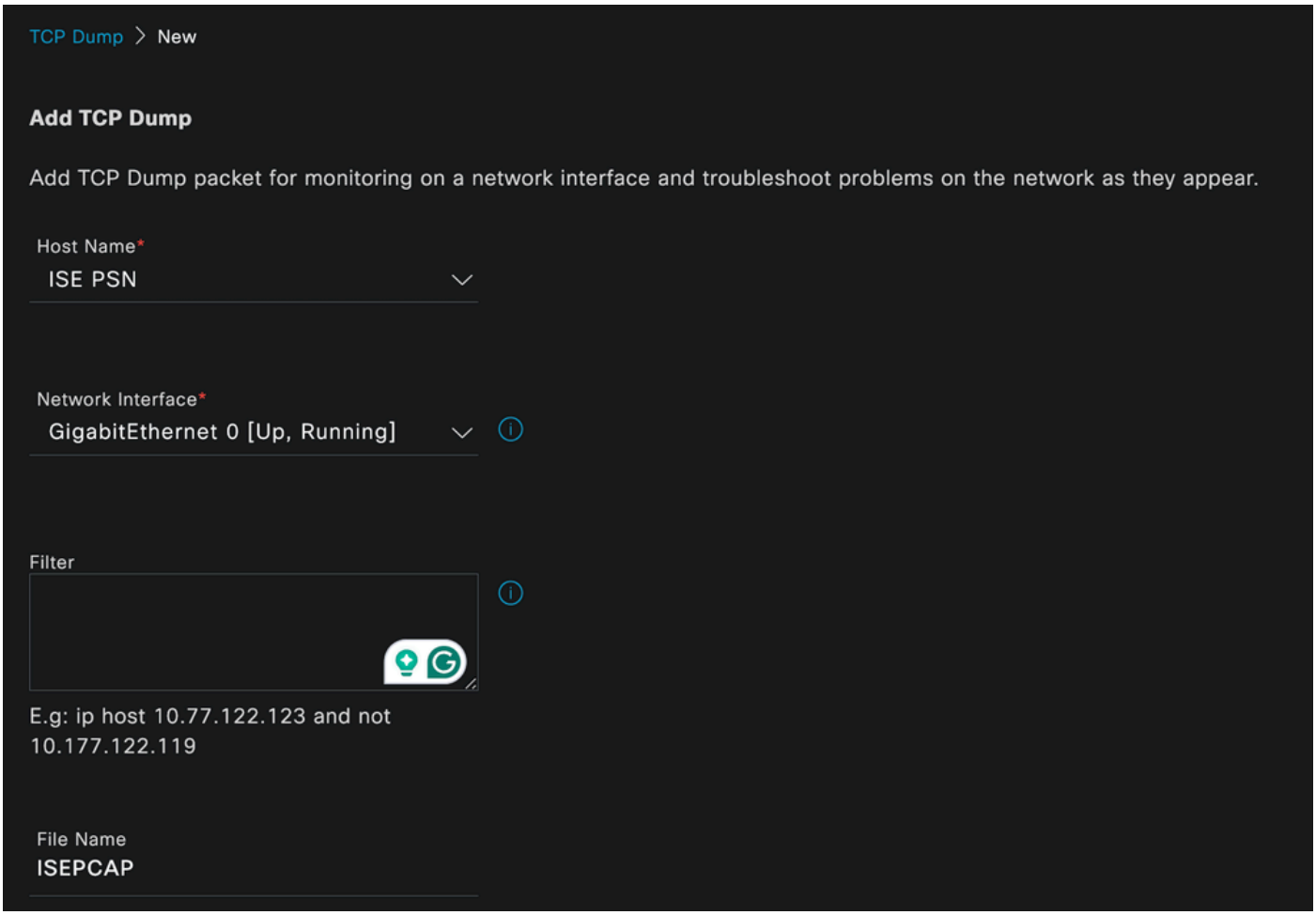
L'analyse de la capture de paquets est essentielle lors du dépannage. Les captures de paquets ISE peuvent être effectuées directement sur tous les noeuds et sur toutes les interfaces des noeuds.

Pour accéder à cet outil, accédez à Opérations > Outils de diagnostic > Outils généraux > Dépôt TCP.

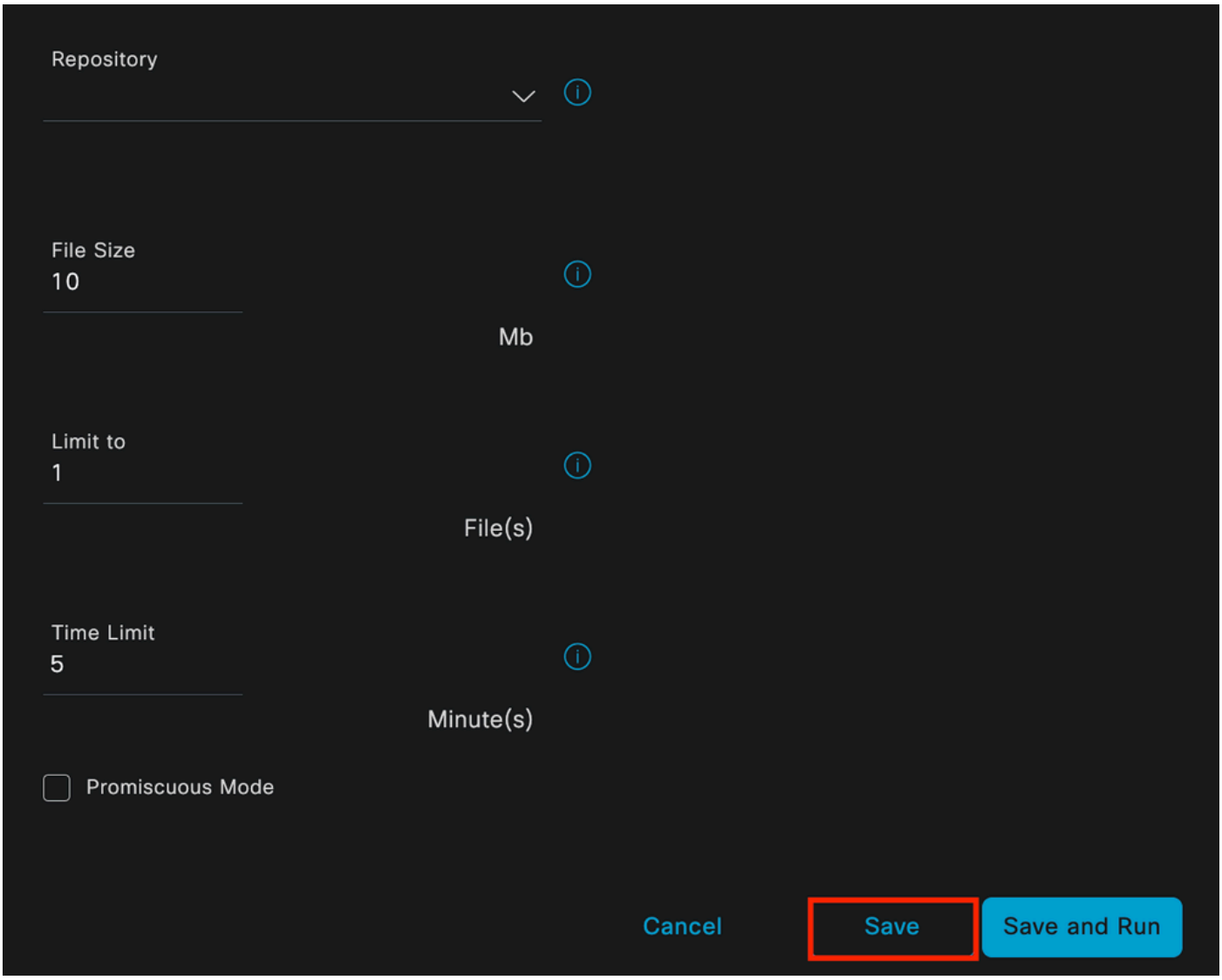



Section Dépôt TCP

Cliquez sur le bouton Add, pour commencer à configurer un pcap.




Création de vidage TCP

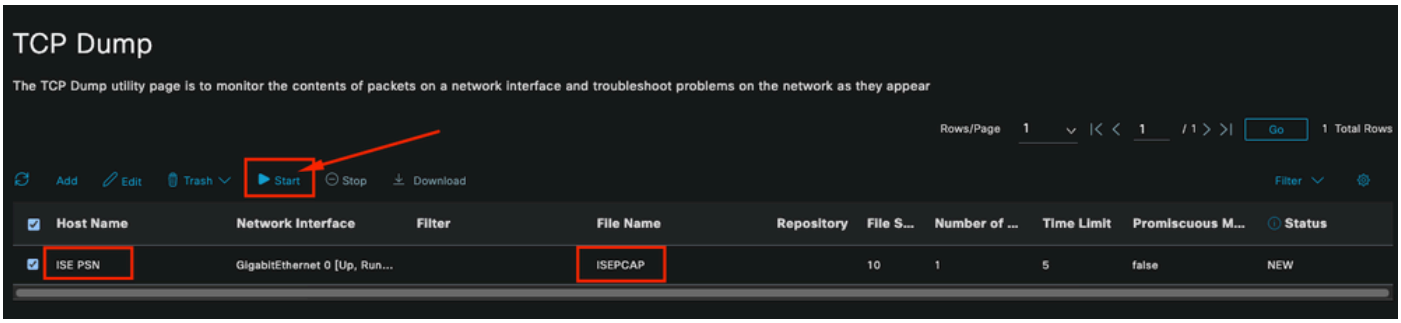



Section Dépôt TCP

Pour créer un pcap dans ISE, voici les données que vous devez saisir :

- Sélectionnez le noeud dans lequel vous devez prendre le pcap.
- Sélectionnez l'interface de noeud ISE utilisée pour le pcap.
- Si vous avez besoin de capturer un certain trafic, utilisez les filtres, ISE vous fournit quelques exemples.
- Nommez le pcap. Dans ce scénario, nous avons utilisé ISEPCAP.
- Sélectionnez le référentiel, si aucun référentiel n'est sélectionné, la capture est enregistrée sur le disque local ISE et peut être téléchargée depuis l'interface utilisateur graphique.
- En outre, si nécessaire, modifiez la taille du fichier pcap.
- Si nécessaire, utilisez plus d'1 fichier, de sorte que si la pcap dépasse la taille du fichier, un nouveau fichier est créé par la suite.
- Prolongez le temps de capture du trafic pour le pcap si nécessaire.

Enfin, cliquez sur le bouton Save.

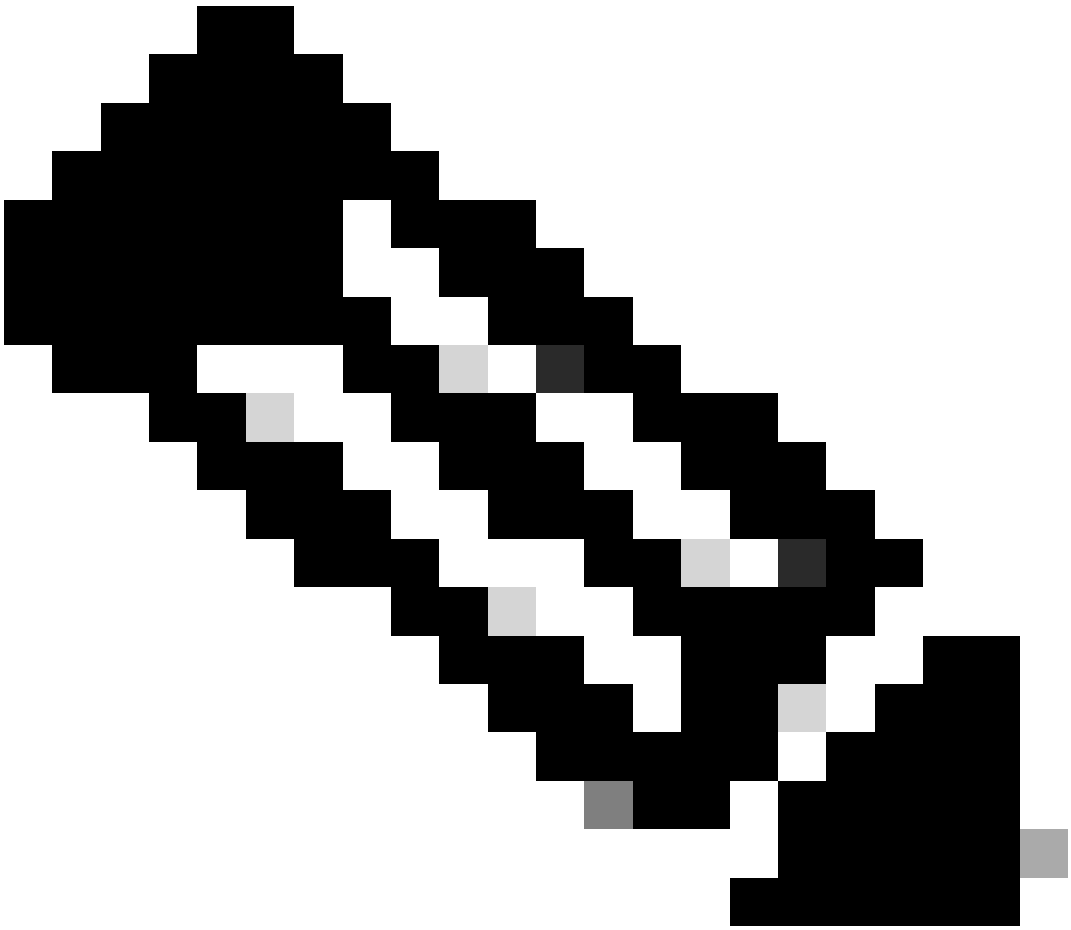



Section Dépôt TCP

Une fois prêt, sélectionnez le pcap, puis cliquez sur le bouton Start.

Une fois que vous avez cliqué sur Start, la colonne Status passe à l'état RUNNING.

---



Remarque : lorsque le PCAP est à l'état EN COURS D'EXÉCUTION, répliquez le scénario défaillant ou le comportement à capturer. Une fois terminé, les détails de la conversation RADIUS, sont visibles dans le PCAP.

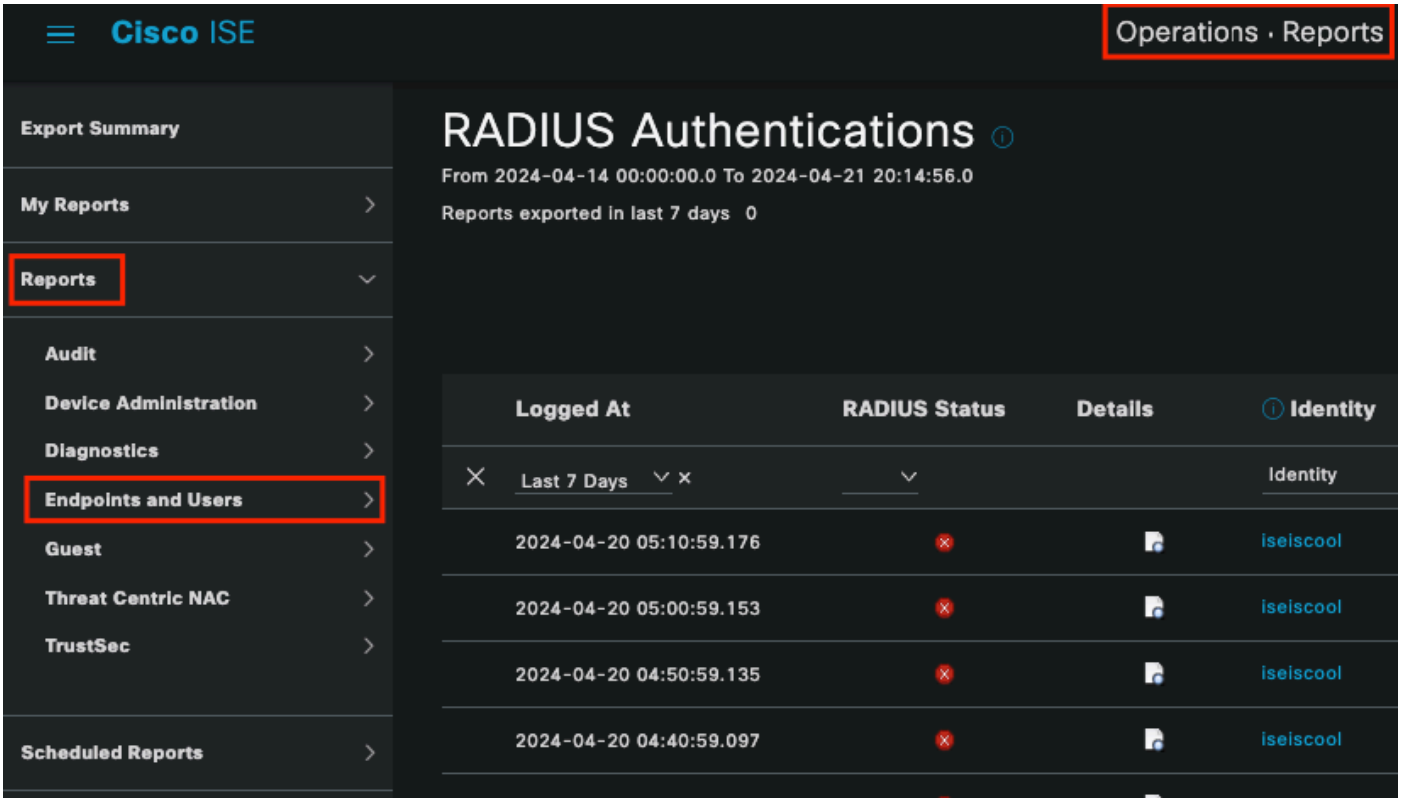
---

Une fois que les données dont vous avez besoin sont capturées pendant que le PCAP est en cours d'exécution, terminez la collecte pcap. Sélectionnez-la à nouveau et cliquez sur Stop.

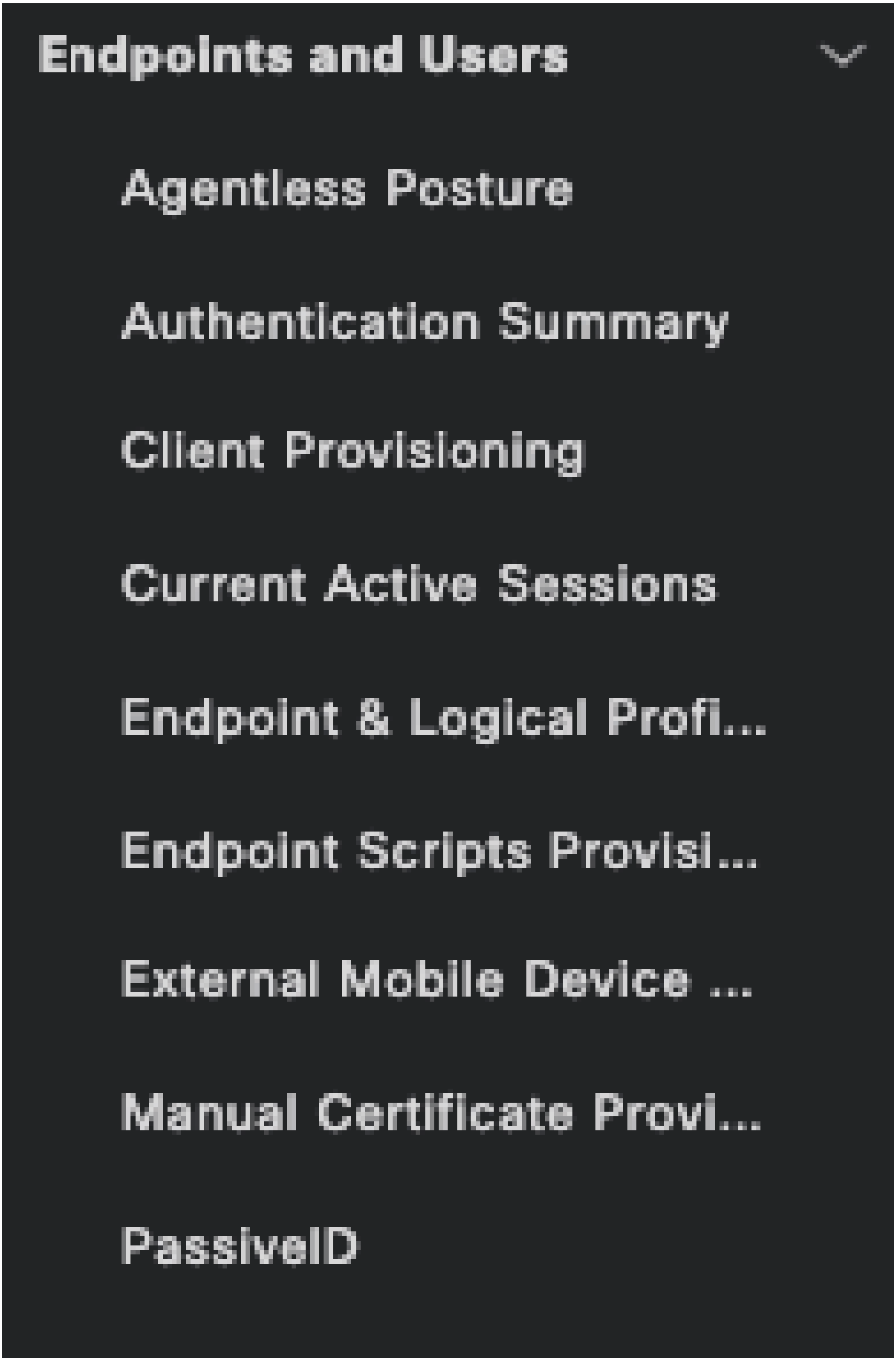
3 - 1 rapports ISE

Si une analyse plus approfondie est nécessaire, ISE propose des rapports utiles pour analyser les événements passés.

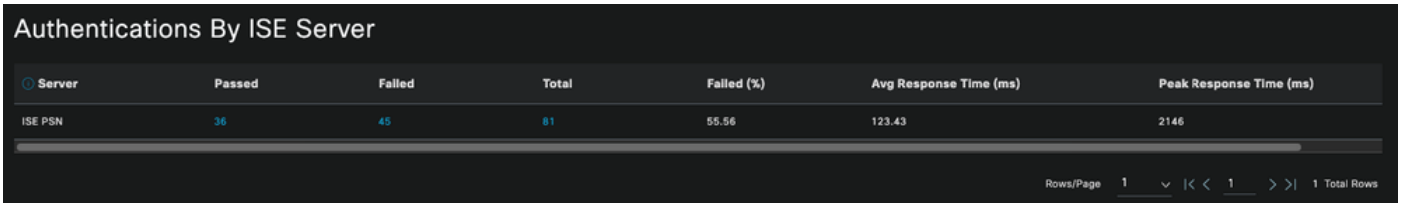
Pour les trouver, accédez à Operations > Reports > Reports > Endpoints and Users




Section Rapports ISE


Endpoints and Users
Agentless Posture
Authentication Summary
Client Provisioning
Current Active Sessions
Endpoint & Logical Profi...
Endpoint Scripts Provisi...
External Mobile Device ...
Manual Certificate Provi...
PassiveID

: dans le déploiement utilisé pour ce document, un seul PSN a été utilisé ; toutefois, pour les déploiements plus importants, ces données sont utiles pour voir si l'équilibrage de charge est nécessaire.



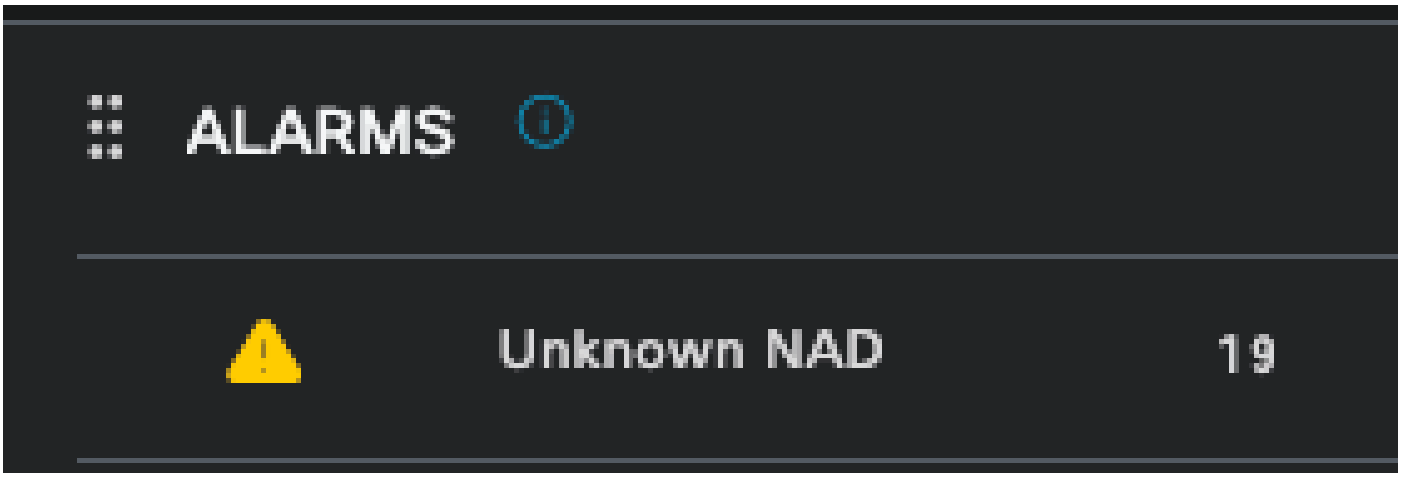

Authentifications par serveur ISE

4 - Alarmes ISE

Sous le tableau de bord ISE, la section Alarmes affiche les problèmes de déploiement.

Voici plusieurs alarmes ISE qui facilitent le dépannage.

NAD inconnu - Cette alarme est affichée lorsqu'un périphérique réseau authentifie un point d'extrémité et atteint ISE. Mais ISE ne lui fait pas confiance et il abandonne la connexion RADIUS. Les raisons les plus courantes sont que le périphérique réseau n'est pas créé ou que l'adresse IP utilisée par le périphérique réseau n'est pas la même que celle enregistrée par ISE.

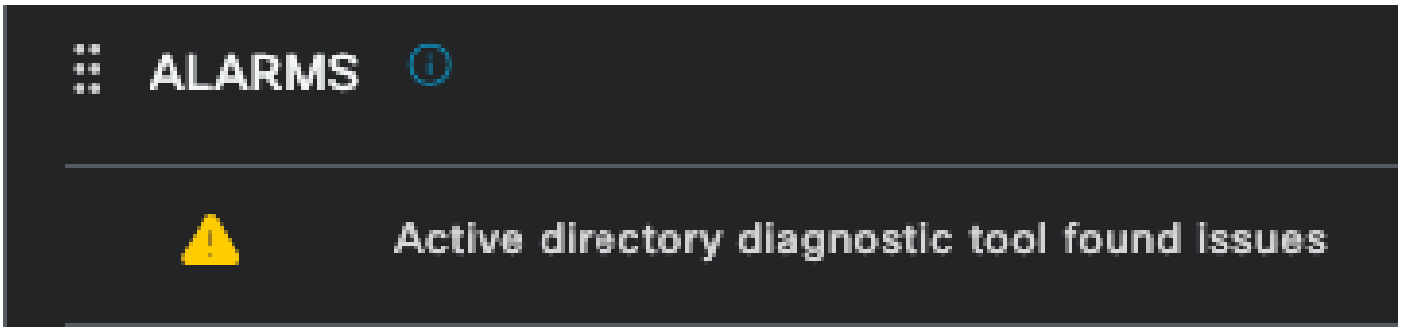



NAD inconnu

Le demandeur a cessé de répondre — Cette alarme se produit lorsqu'il y a un problème avec la communication du demandeur, la plupart du temps est due à une mauvaise configuration dans le demandeur qui doit être vérifiée et examinée du côté du point d'extrémité.


Le demandeur ne répond plus

Problèmes détectés par l'outil de diagnostic Active Directory — Lorsqu'Active Directory est utilisé pour valider l'identité de l'utilisateur, s'il commence à rencontrer des problèmes avec le processus de communication ou si la connexion est interrompue, cette alarme s'affiche. Ensuite, vous réaliserez pourquoi les authentifications indiquant que l'identité existe sur AD échouent.




Échec des diagnostics AD

Échec du COA (changement d'autorisation) — Plusieurs flux dans ISE utilisent CoA, cette alarme vous informe si des problèmes ont été rencontrés lors de la communication du port CoA à un périphérique réseau.


Échec de Coa

5 - Configuration du débogage ISE et collecte des journaux

Pour continuer avec les détails du processus d'authentification, vous devez activer les composants suivants dans DEBUG pour les problèmes mab et dot1x :

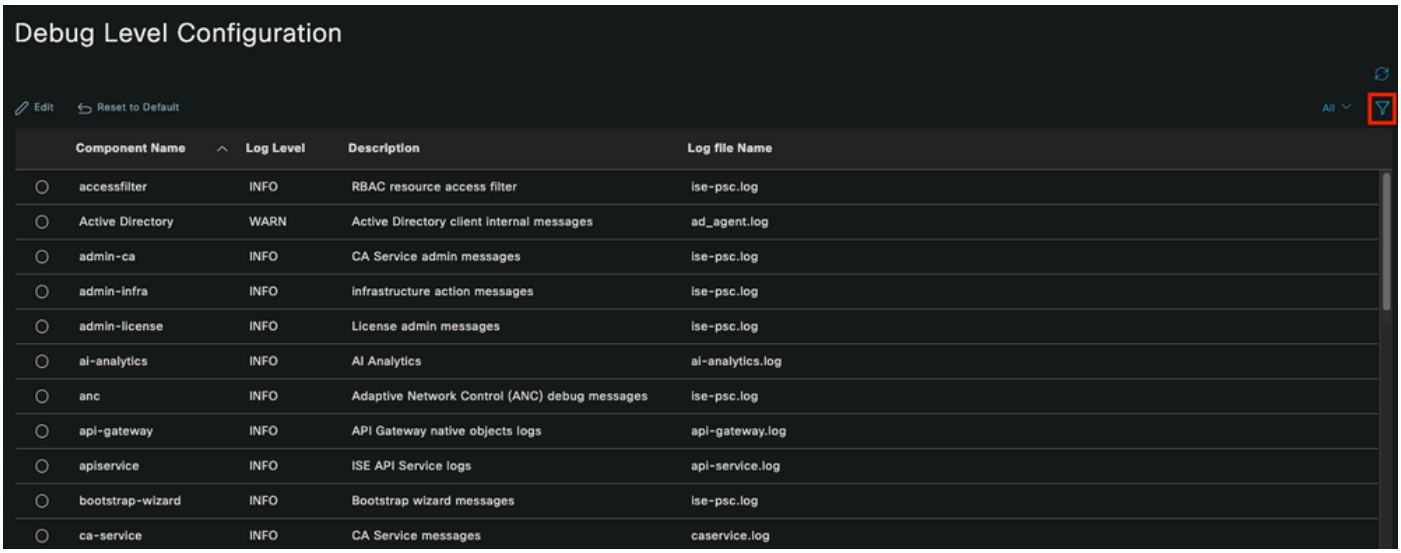
Problème : dot1x/mab

Attributs à définir au niveau de débogage.

- runtime-AAA (prt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

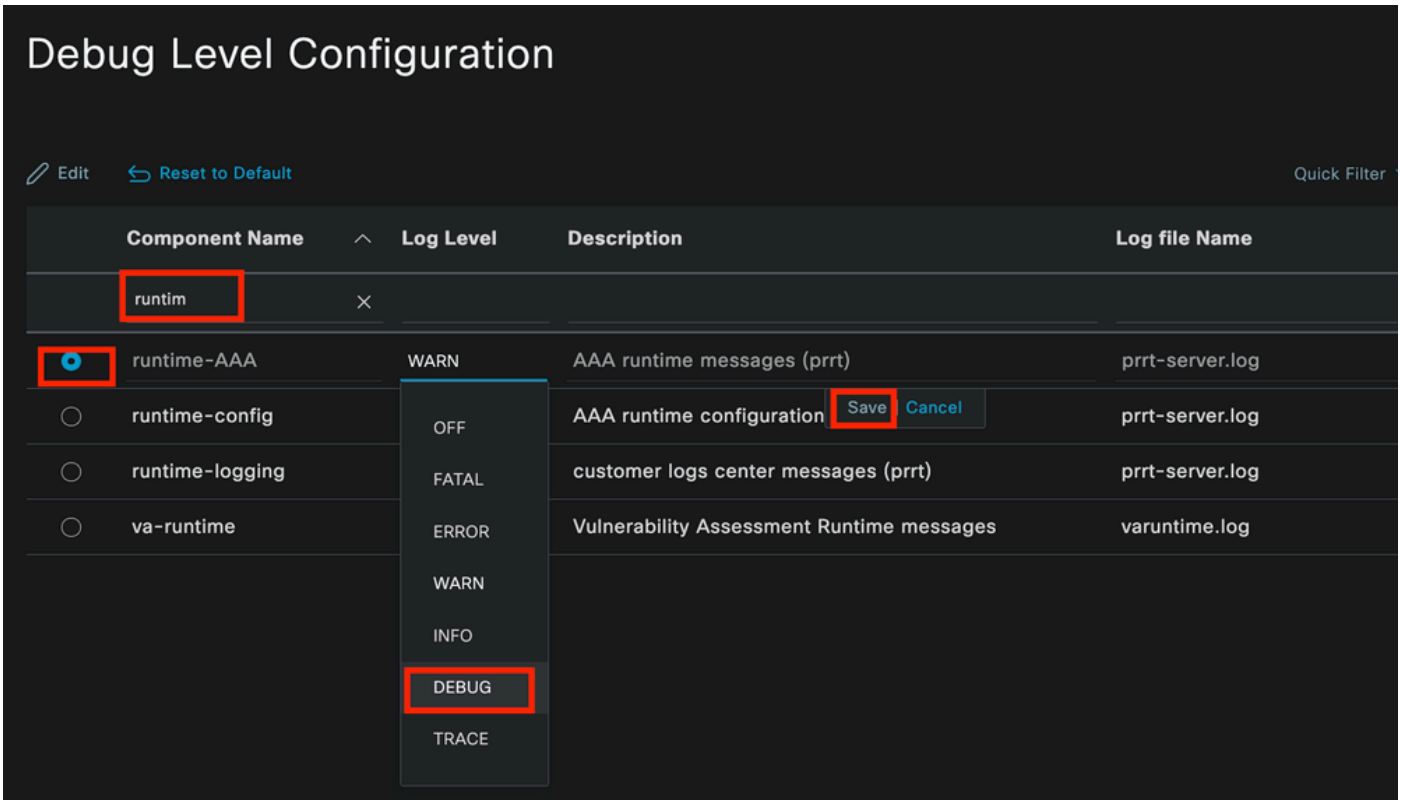
Pour activer les composants au niveau DEBUG, il est d'abord nécessaire d'identifier le PSN qui reçoit l'authentification qui échoue ou qui doit être examiné. Vous pouvez obtenir ces informations à partir des journaux en direct. Ensuite, vous devez accéder au menu ISE > Troubleshoot > Debug Wizard > Debug Log Configuration > Select the PSN > Cliquez sur le bouton Edit.

Le menu suivant s'affiche. Cliquez sur l'icône de filtre :



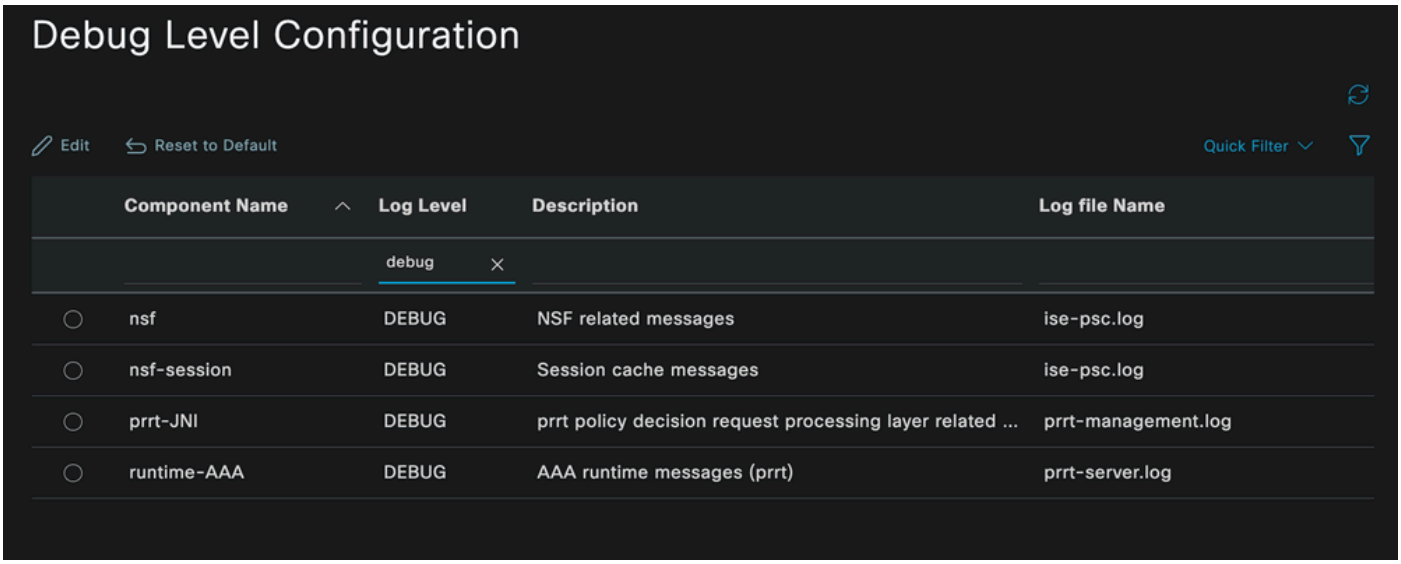

Configuration du journal de débogage

Dans la colonne Nom du composant, recherchez les attributs répertoriés précédemment. Sélectionnez chaque niveau de journal et changez-le en DEBUG. Enregistrez les modifications.




Configuration du composant AAA d'exécution

Une fois que vous avez terminé la configuration de chaque composant, filtrez-les avec DEBUG afin de voir si tous les composants ont été correctement configurés.



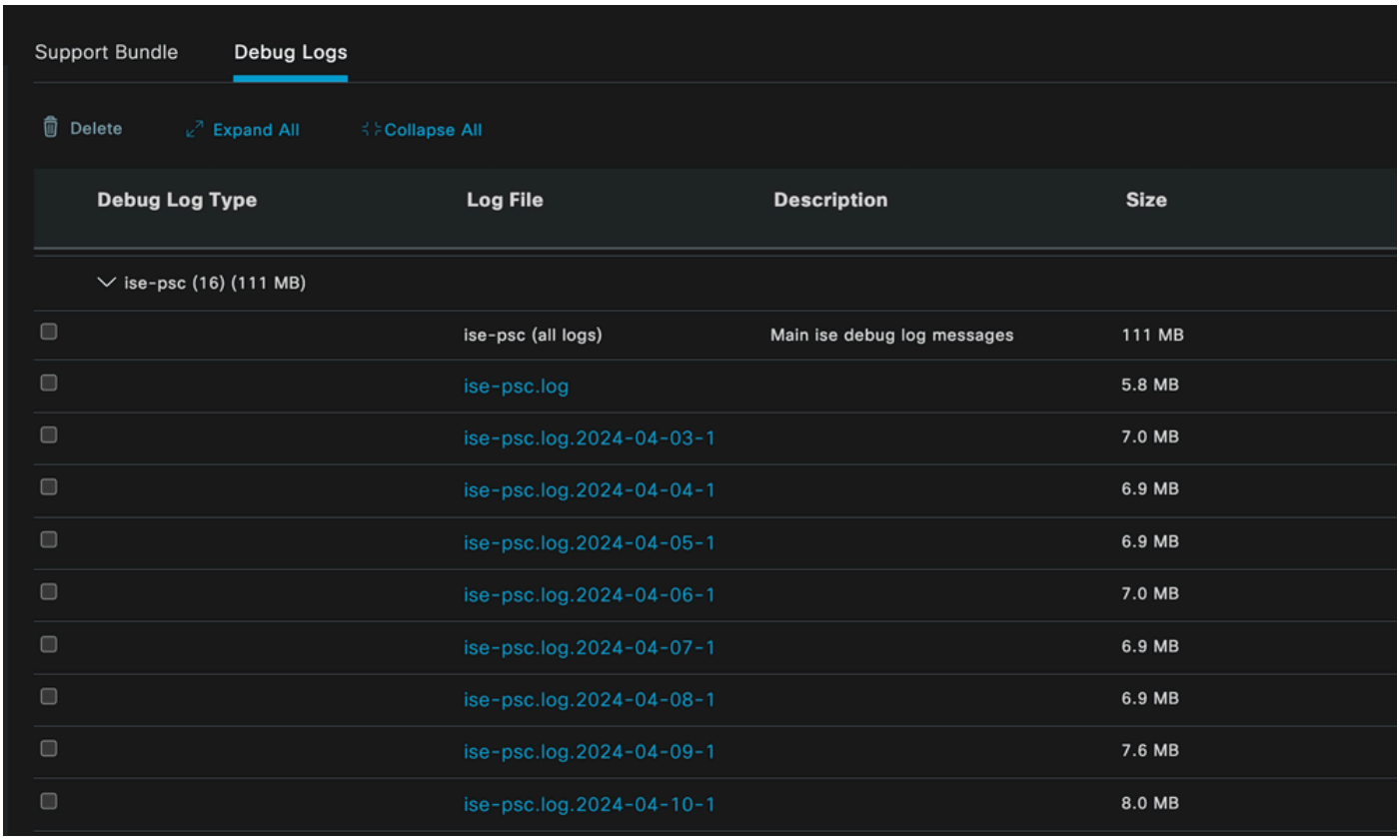

Configuration du journal de débogage

Si vous devez analyser immédiatement les journaux, vous pouvez les télécharger en naviguant vers le chemin ISE Menu > Operations > Troubleshoot > Download Logs > Appliance node list > PSN et en activant DEBUGS > Debug Logs.

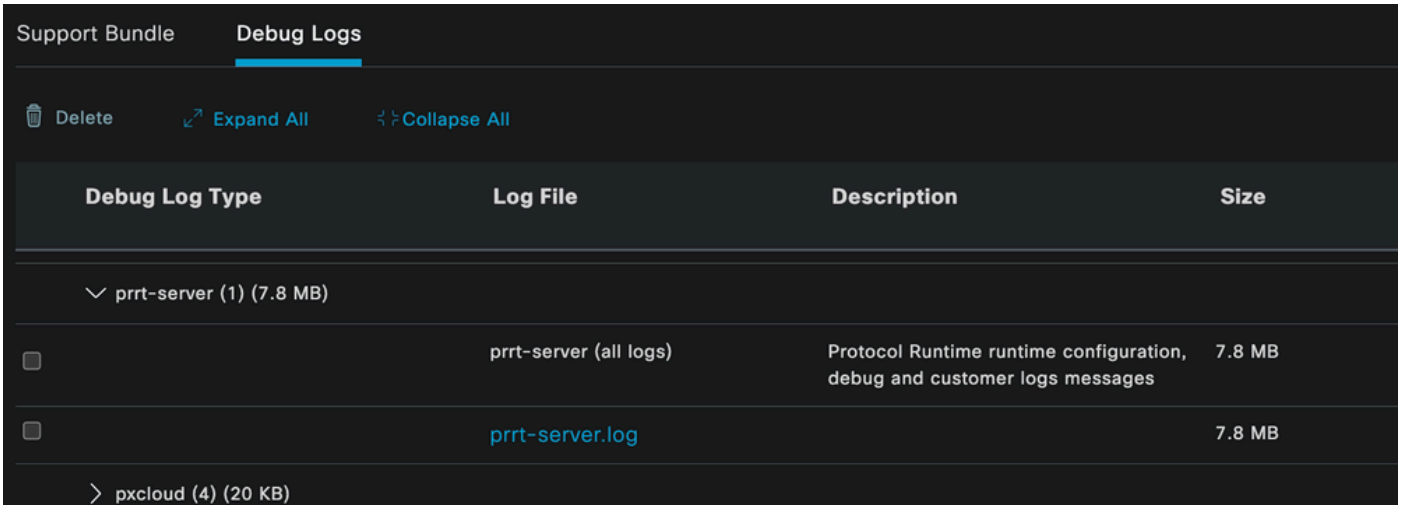
Dans ce cas, vous devez télécharger pour les problèmes dot1x et mab dans prrt-server.log et ise-psc.log. Le journal que vous devez télécharger est celui avec la date de votre dernier test.

Cliquez simplement sur le fichier journal affiché dans cette image et téléchargez-le (affiché en

bleu).




Journaux de débogage du noeud PSN

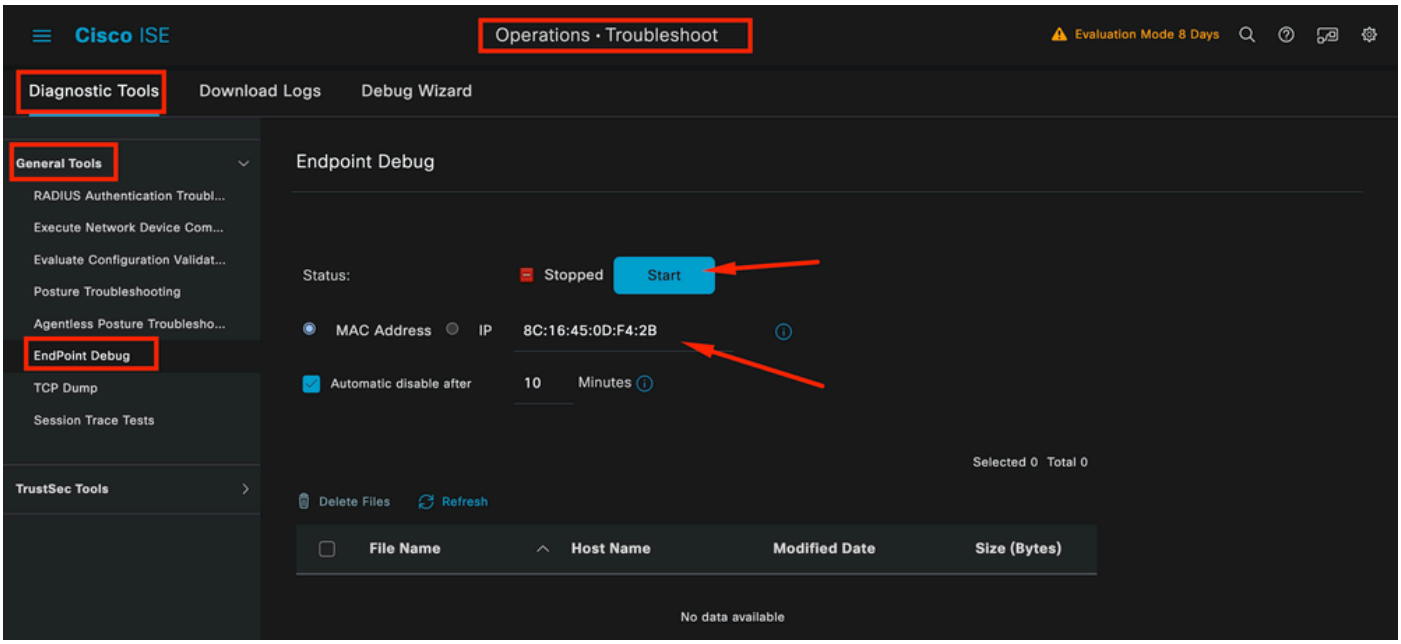



Section Journaux de débogage

## 6 - Débogage ISE par terminal

Il existe également une autre option pour obtenir les journaux DEBUG, par journaux de débogage de point de terminaison basés sur l'adresse MAC ou IP. Vous pouvez utiliser l'outil ISE Endpoint Debug.

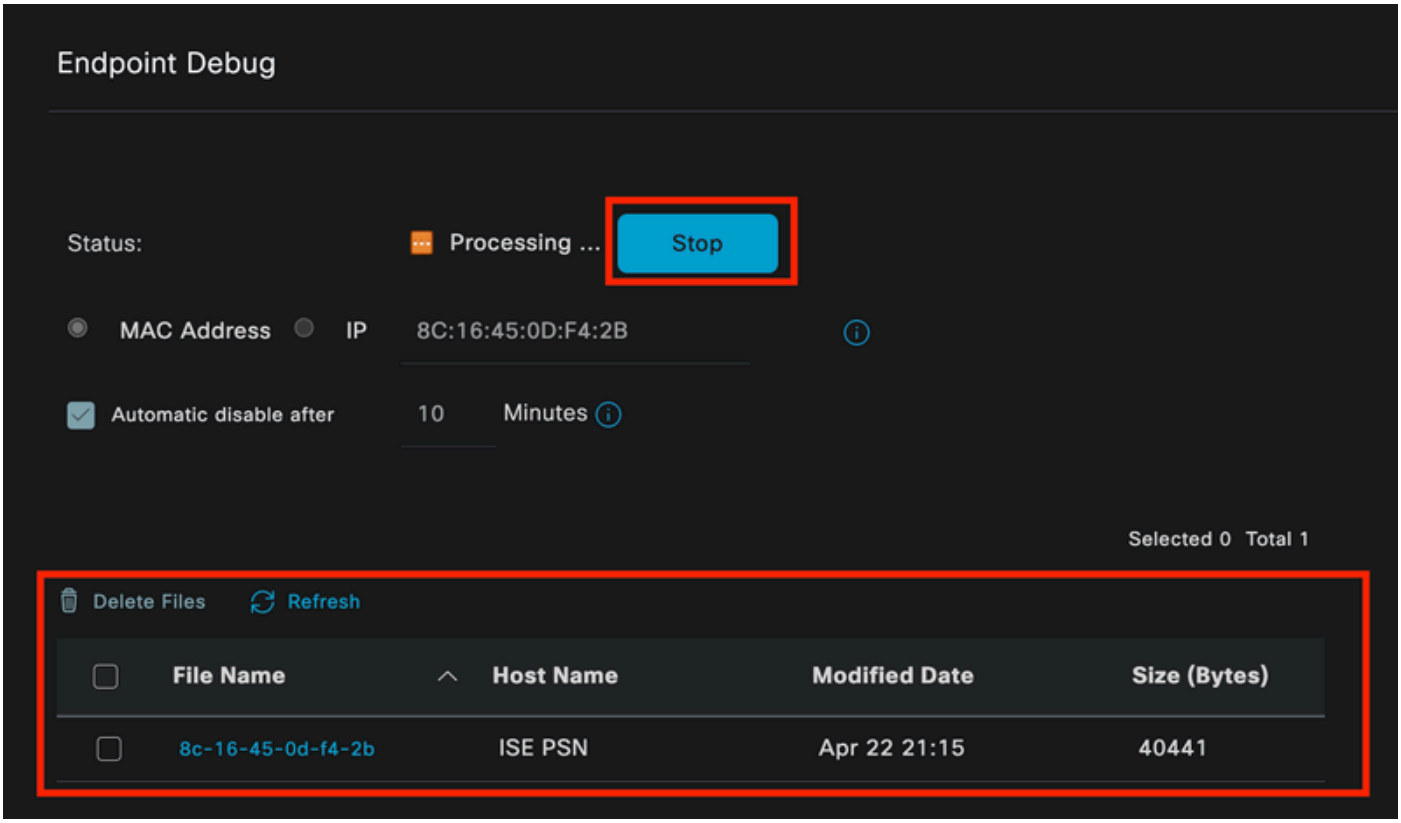
Accédez au menu ISE > Operations > Troubleshoot > Diagnostic Tools > General Tools > Endpoint Debug.




Débogage des terminaux

Saisissez ensuite les informations de point de terminaison souhaitées pour commencer la capture des journaux. Cliquez sur Démarrer.

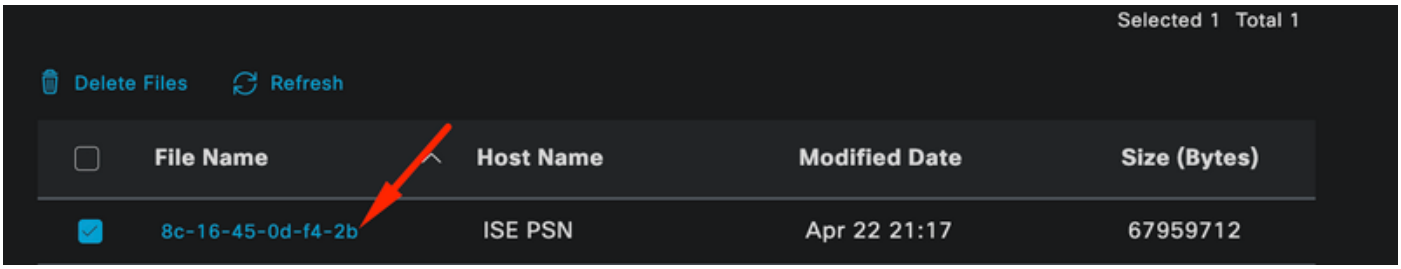
Cliquez ensuite sur Continue dans le message d'avertissement.




Débogage des terminaux

Une fois les informations capturées, cliquez sur Stop.

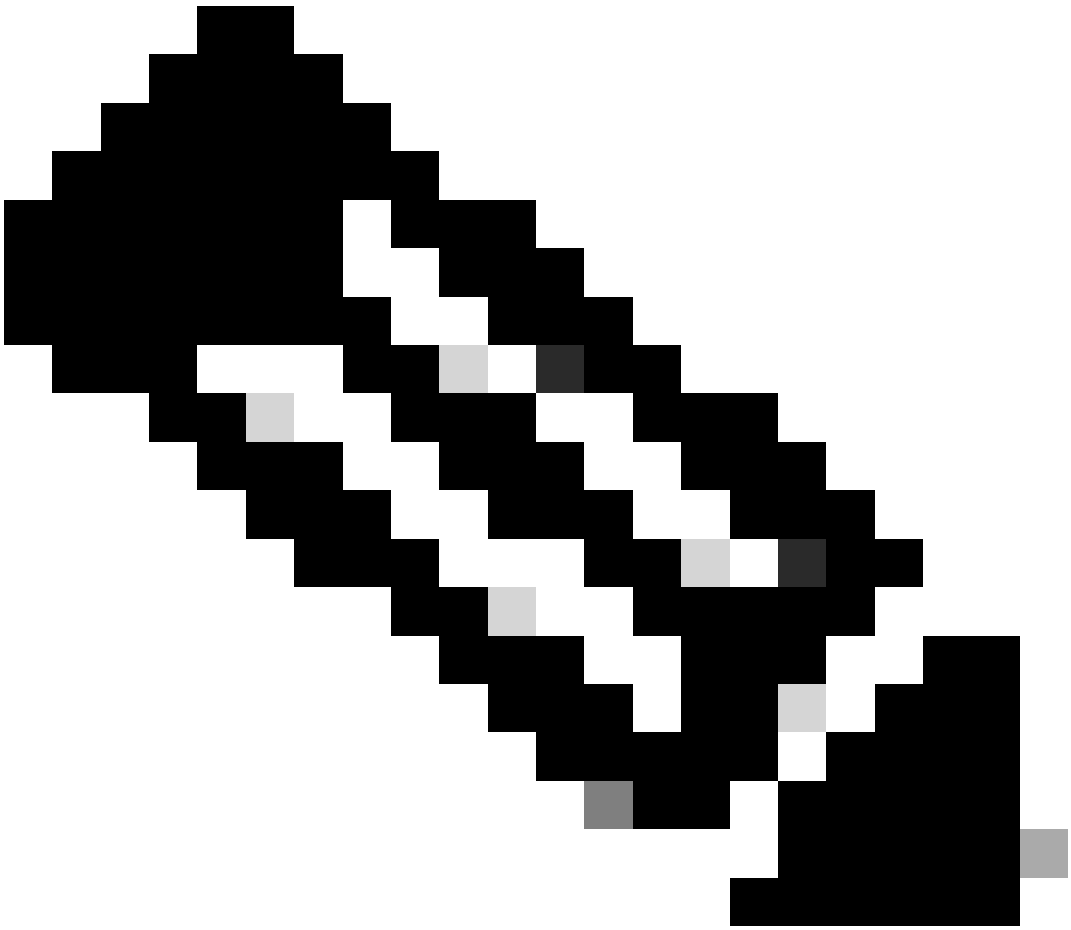
Cliquez sur le nom de fichier affiché en bleu. dans cette image.




Débogage des terminaux

Vous devez pouvoir voir les journaux d'authentification avec les journaux DEBUG sans les activer directement à partir de la configuration du journal de débogage.

---

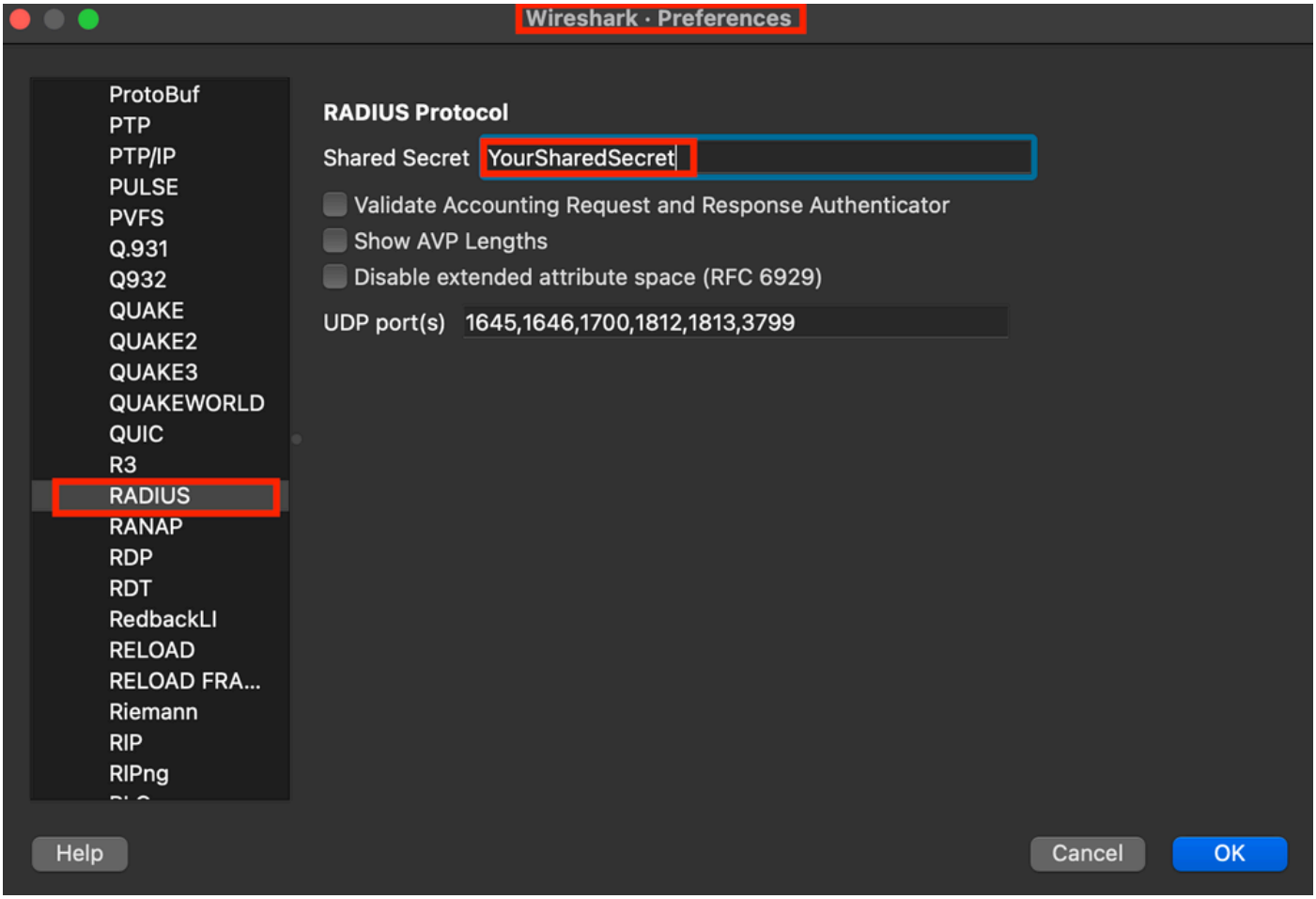


Remarque : comme certains éléments peuvent être omis dans la sortie de débogage du point de terminaison, vous obtiendrez un fichier journal plus complet en le générant avec la configuration du journal de débogage et en téléchargeant tous les journaux requis à partir de n'importe quel fichier dont vous avez besoin. Comme expliqué dans la section précédente Configuration du débogage ISE et collecte de journaux.

---

7 - Déchiffrer les paquets RADIUS

Les paquets Radius ne sont pas chiffrés, sauf pour le champ de mot de passe utilisateur. Cependant, vous devez vérifier le mot de passe envoyé. Vous pouvez voir le paquet envoyé par l'utilisateur en naviguant vers Wireshark > Preferences > Protocols > RADIUS et puis ajoutez la clé partagée RADIUS utilisée par ISE et le périphérique réseau. Ensuite, les paquets RADIUS sont affichés déchiffrés.




Options de rayon Wireshark

8 - Commandes de dépannage des périphériques réseau

La commande suivante vous aide à résoudre les problèmes sur le routeur ISR 1100 ou le périphérique NAD filaire.

8 - 1 Pour voir si le serveur AAA ou ISE est disponible et accessible à partir du périphérique réseau, utilisez la commande show aaa servers.

```
Router>show aaa servers

RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname
     State: current UP, duration 2876s, previous duration 0s
     Dead: total time 0s, count 0

     Platform State from SMD: current UP, duration 2876s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
```

```
Platform State from WNCD (1) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (2) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (3) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (4) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (5) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (6) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (7) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (8) : current UP, duration 3015s, previous duration 0s

WNCD Platform Dead: total time 0s, count 0UP

Quarantined: No

Authen: request 11, timeouts 0, failover 0, retransmission 0

        Response: accept 1, reject 0, challenge 10
        Response: unexpected 0, server error 0, incorrect 0, time 33ms
        Transaction: success 11, failure 0
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        Dot1x transactions:

        Response: total responses: 11, avg response time: 33ms
        Transaction: timeouts 0, failover 0
        Transaction: total 1, success 1, failure 0

        MAC auth transactions:
        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0

        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        MAC author transactions:

        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3
        Request: start 1, interim 0, stop 0
        Response: start 1, interim 0, stop 0

        Response: unexpected 0, server error 0, incorrect 0, time 27ms
        Transaction: success 2, failure 1
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0

Elapsed time since counters last cleared: 47m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

```
     Consecutive Response Failures: total 0
             SMD Platform : max 0, current 0 total 0
             WNCD Platform: max 0, current 0 total 0
             IOSD Platform : max 0, current 0 total 0

     Consecutive Timeouts: total 3
             SMD Platform : max 0, current 0 total 0
             WNCD Platform: max 0, current 0 total 0
             IOSD Platform : max 3, current 0 total 3

     Requests per minute past 24 hours:
             high - 0 hours, 47 minutes ago: 4
             low  - 0 hours, 45 minutes ago: 0
             average: 0

Router>
```

8-2 Pour afficher l'état du port, les détails, les listes de contrôle d'accès appliquées à la session, la méthode d'authentification et des informations plus utiles, utilisez la commande show authentication sessions interface <interface where the laptop is attached> details.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A0000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0


Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Server Policies:


Method status list:
Method State
dot1x Authc Success

Router#
```

8-3 Pour vérifier que vous disposez de toutes les commandes requises pour aaa dans la configuration globale, exécutez la commande show running-config aaa.

```
Router#sh run aaa
!
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 Cisc0123
!
!
radius server COHVSRADISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRADISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#
```

8-4 Une autre commande utile est test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy.

```
Router#test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy
User was successfully authenticated.

Router#
```

9 - Débogages relatifs aux périphériques réseau

- debug dot1x all - Affiche tous les messages EAP dot1x
- debug aaa authentication - Affiche les informations de débogage d'authentification des applications AAA
- debug aaa authorization - Affiche les informations de débogage pour l'autorisation AAA
- debug radius authentication - Fournit des informations détaillées sur les activités au niveau du protocole uniquement pour l'authentification
- debug radius - Fournit des informations détaillées sur les activités au niveau du protocole

# 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.