

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

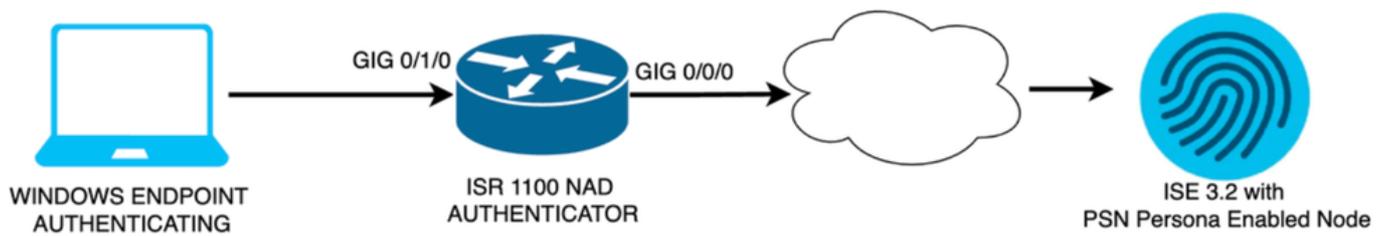


Diagramme du réseau

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>
```

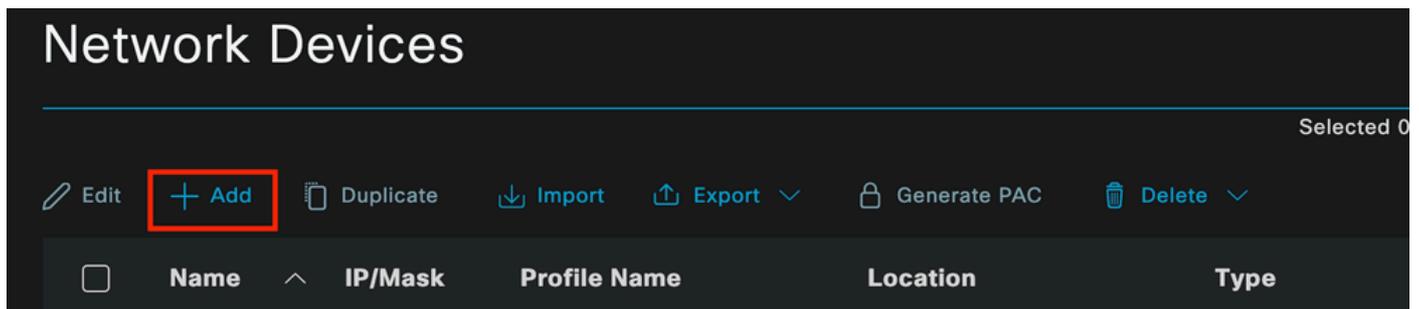
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication 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.

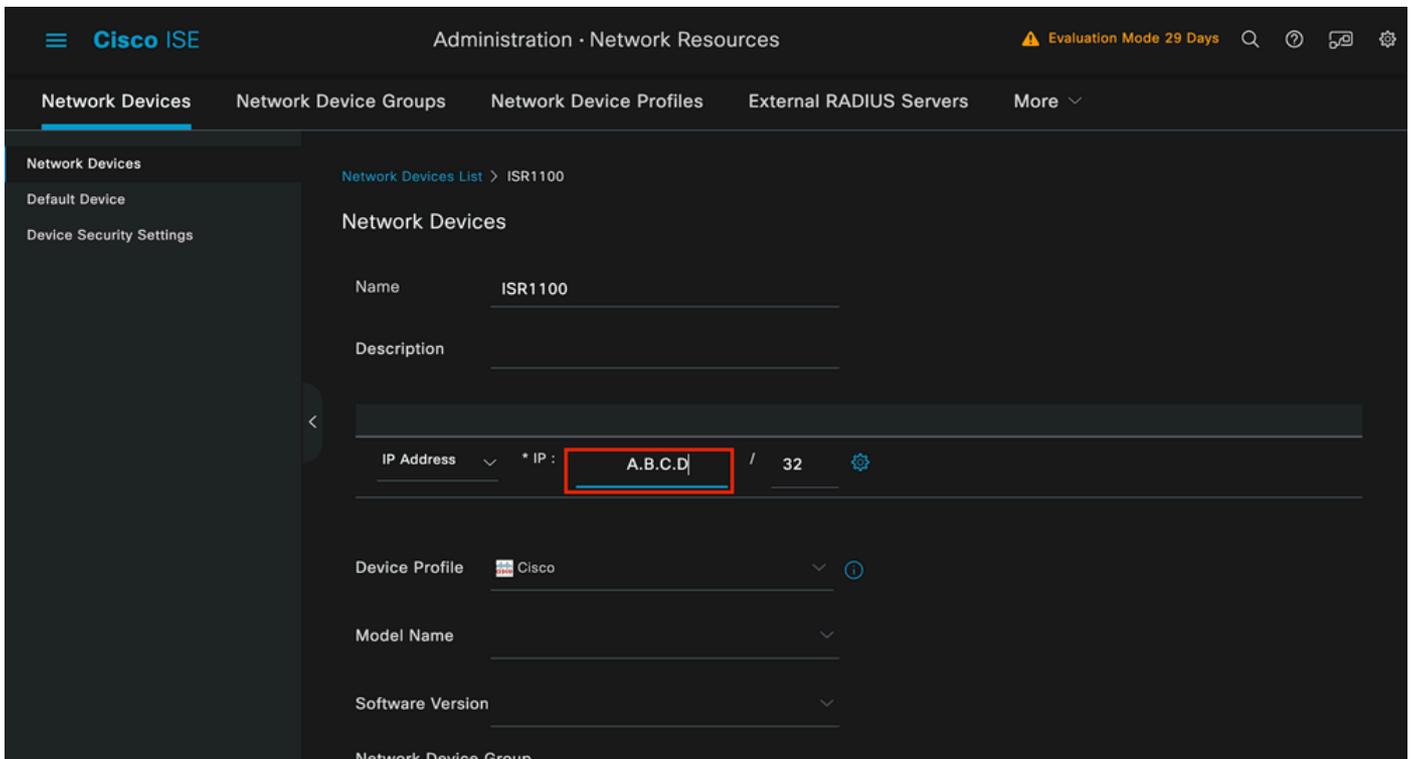
Ajoutez la section Network Device to ISE Network Devices.

Cliquez sur le bouton Add pour démarrer.



Périphériques réseau ISE

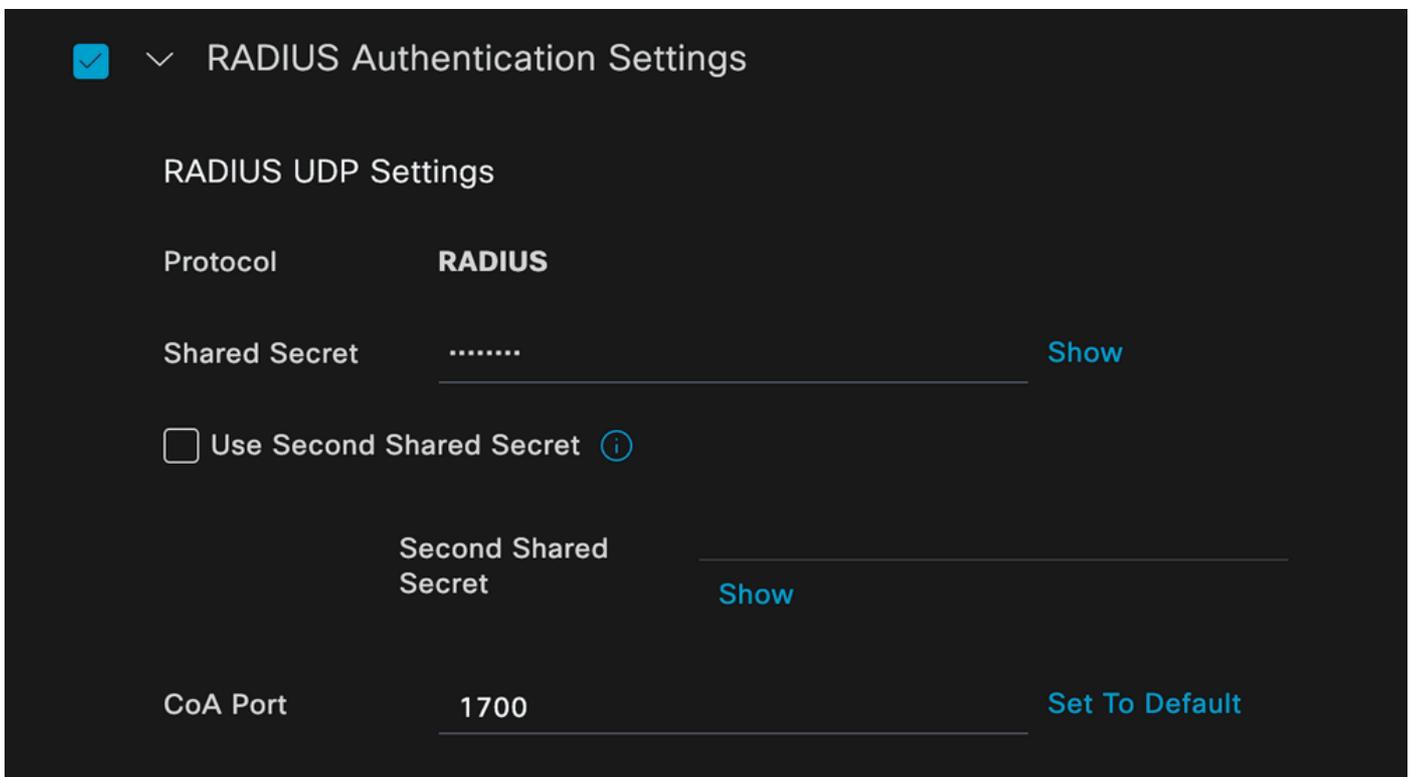
Entrez les valeurs, attribuez un nom au NAD que vous créez et ajoutez également l'adresse IP que le périphérique réseau utilise pour contacter ISE.



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.

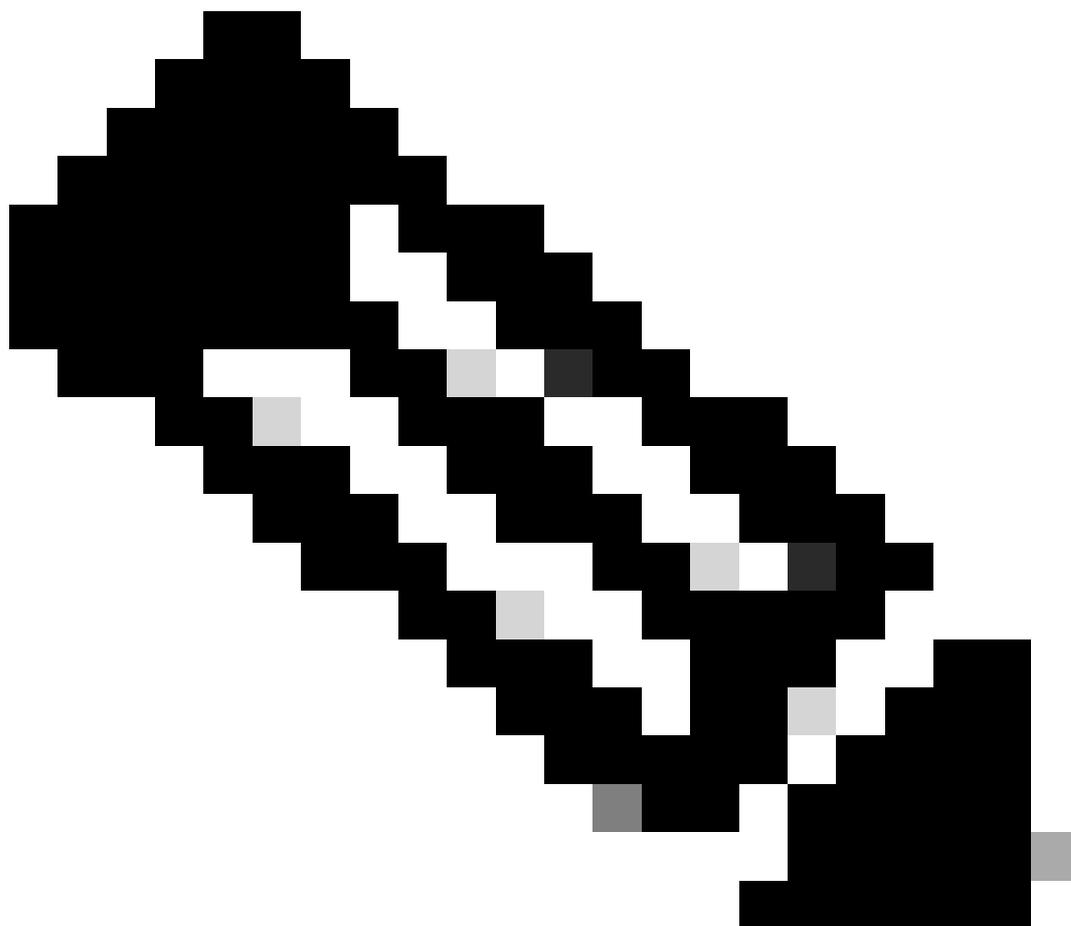
Ajoutez le secret partagé que vous avez utilisé dans votre configuration NAD.



Configuration RADIUS

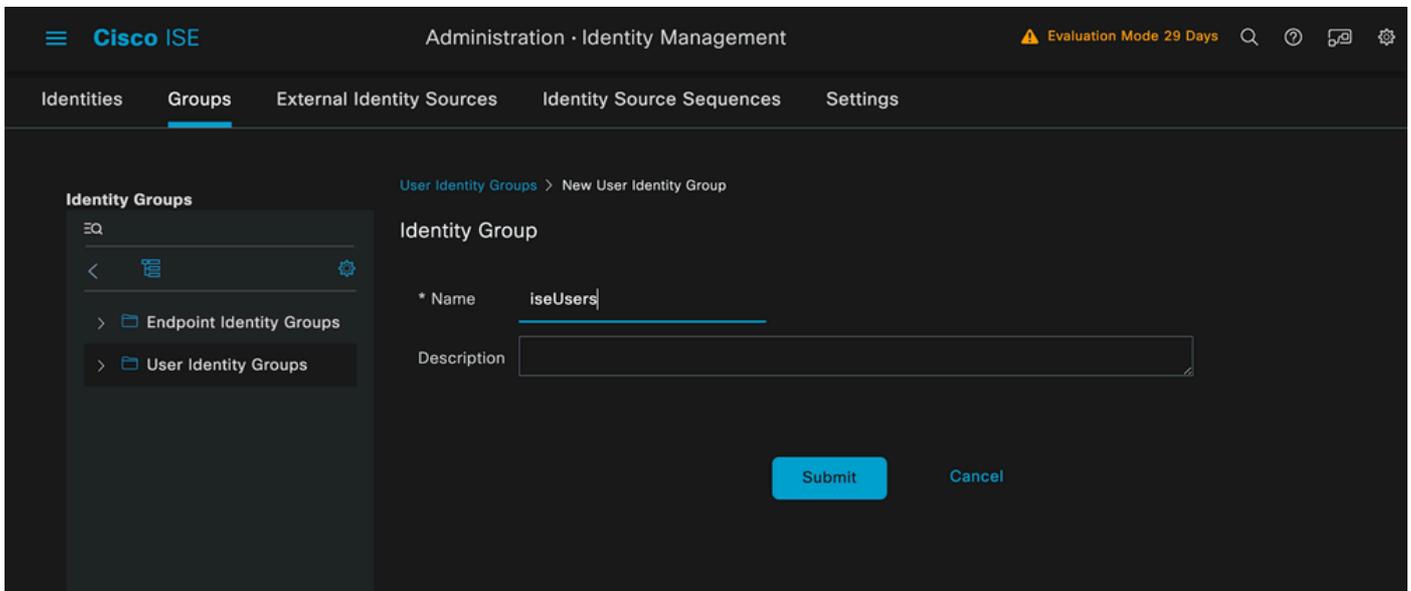
Enregistrez les modifications.

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.

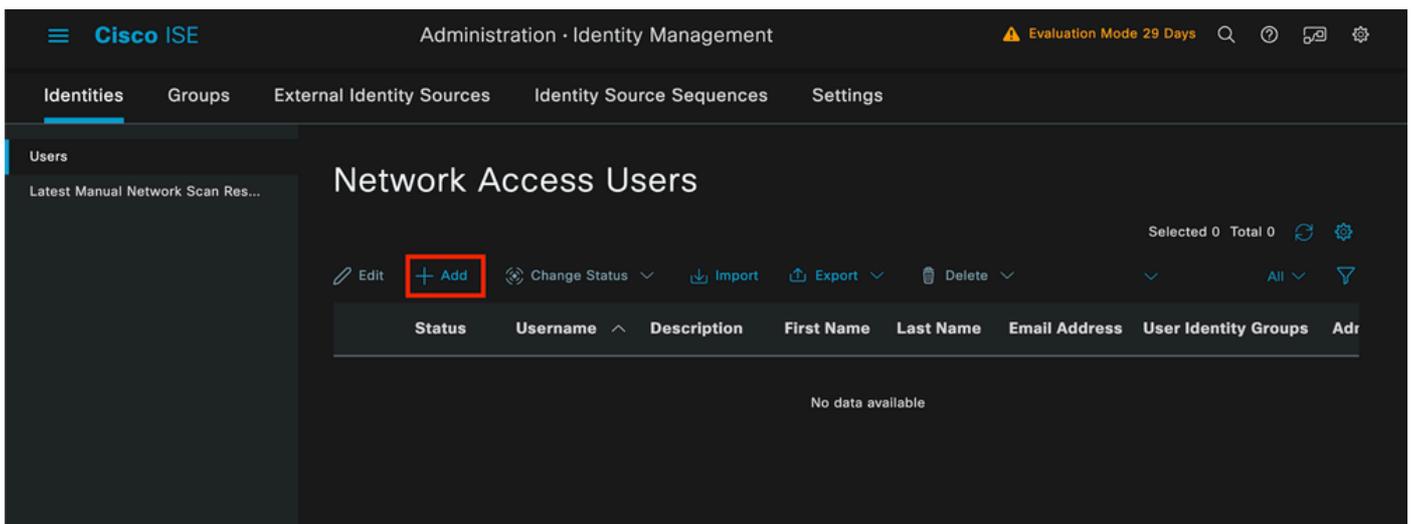


Page Identity Group Creation

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.

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Nom attribué au nom d'utilisateur

L'étape suivante consiste à attribuer un mot de passe au nom d'utilisateur créé. VainillaSE97 est utilisé dans cette démonstration.

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 ⓘ

Création de mot de passe

Affectez l'utilisateur au groupe iseUsers.

User Groups



▼



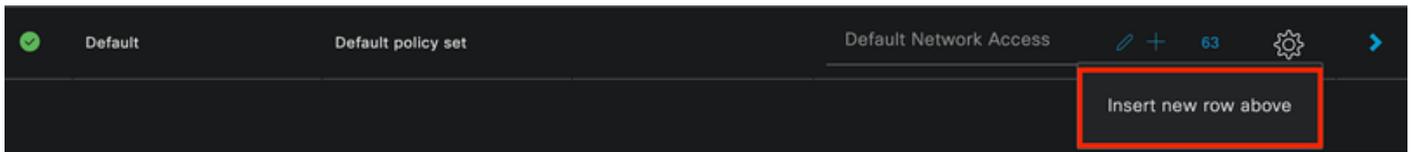
Attribution du groupe d'utilisateurs

2. c. Configurer l'ensemble de stratégies

Accédez au menu ISE > Policy > Policy Sets.

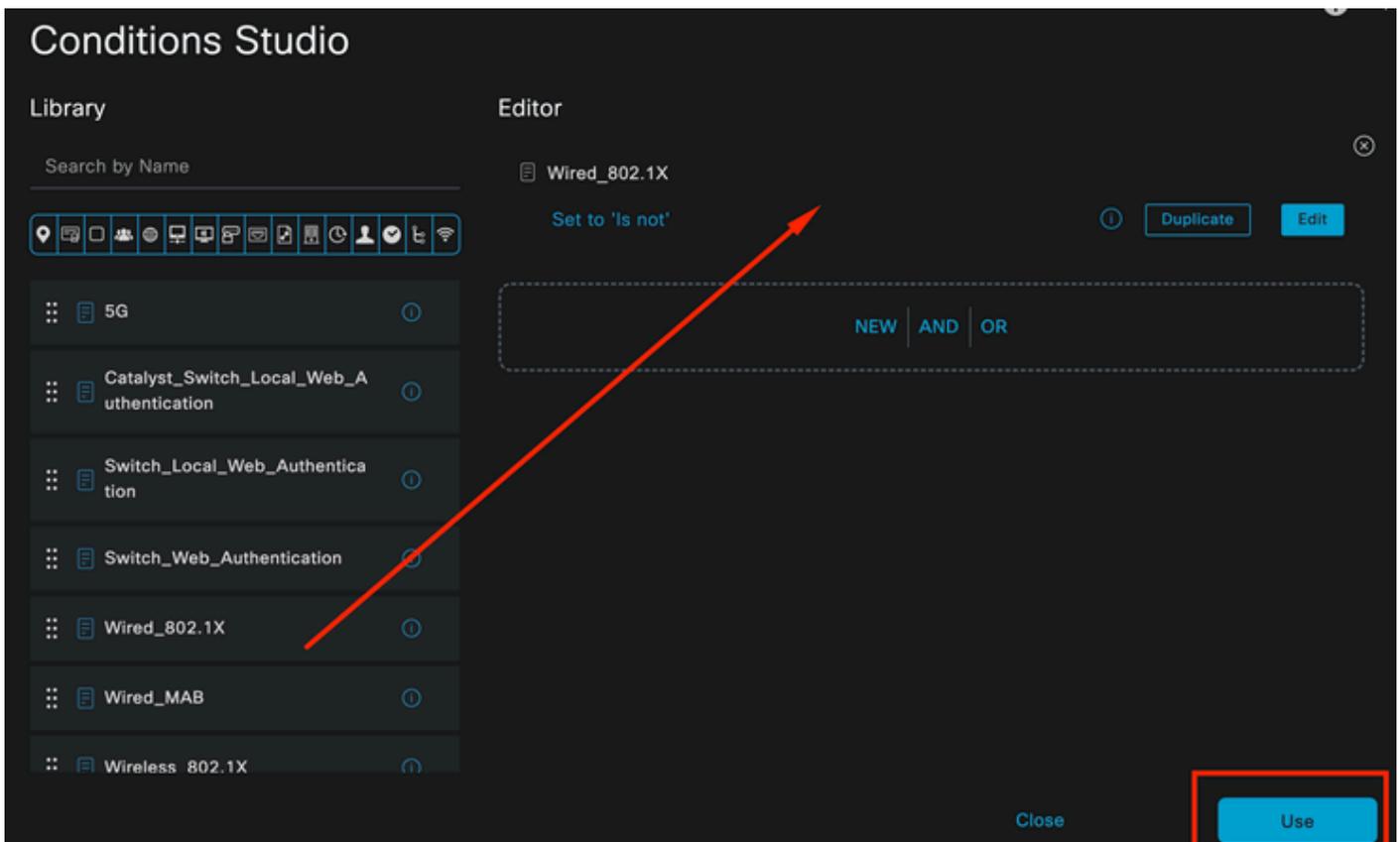
Le jeu de stratégies par défaut peut être utilisé. Cependant, dans cet exemple, un jeu de stratégies est créé et il est appelé Wired. La classification et la différenciation des ensembles de stratégies facilitent le dépannage,

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.



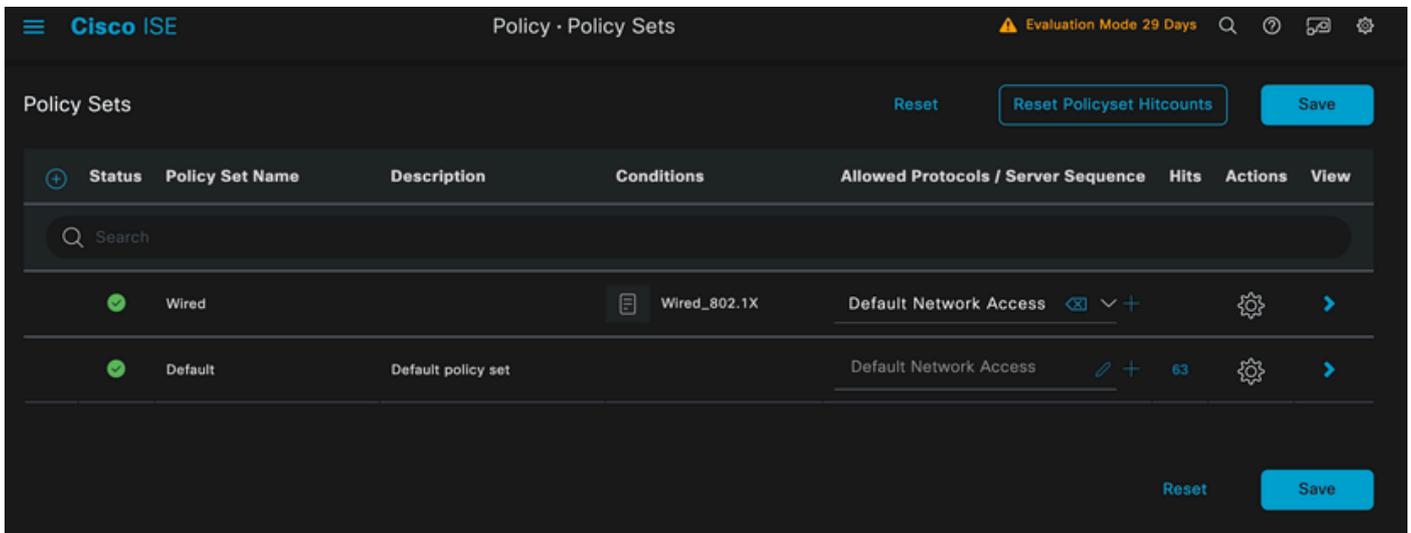
Création de politiques

La condition configurée dans cet exemple est Wired 802.1x 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.

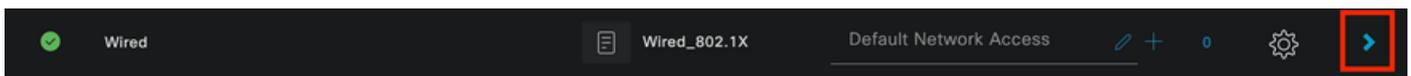


Vue Jeu de stratégies

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 +.



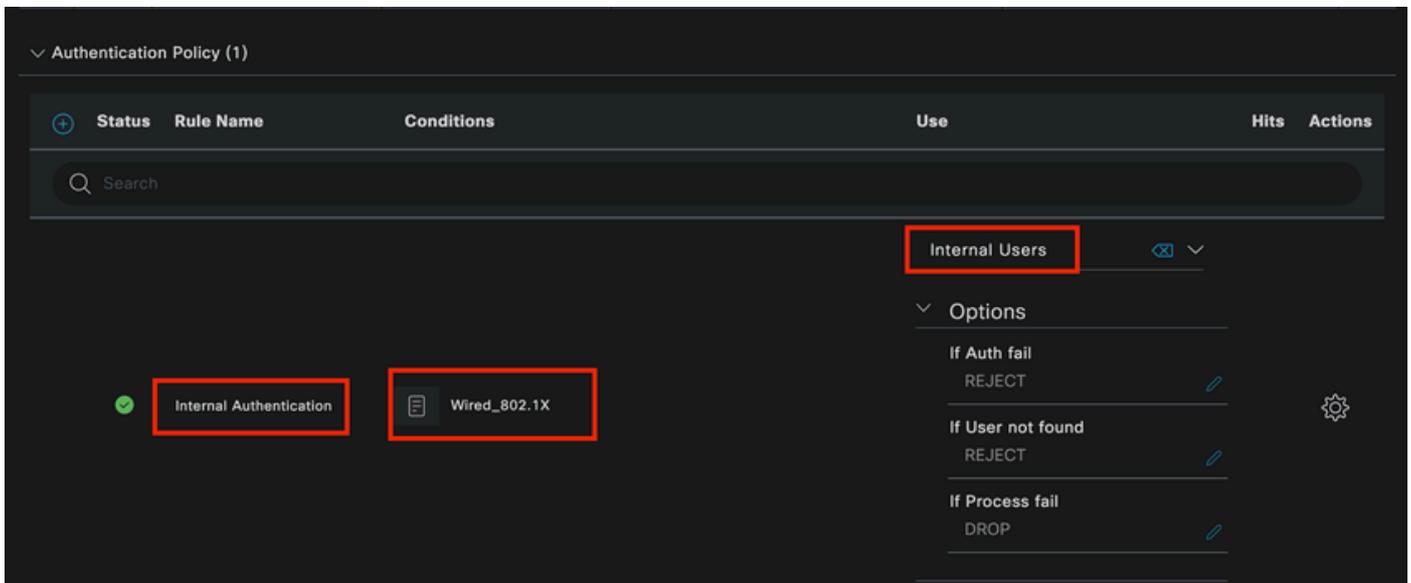
Ajouter une stratégie d'authentification

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.

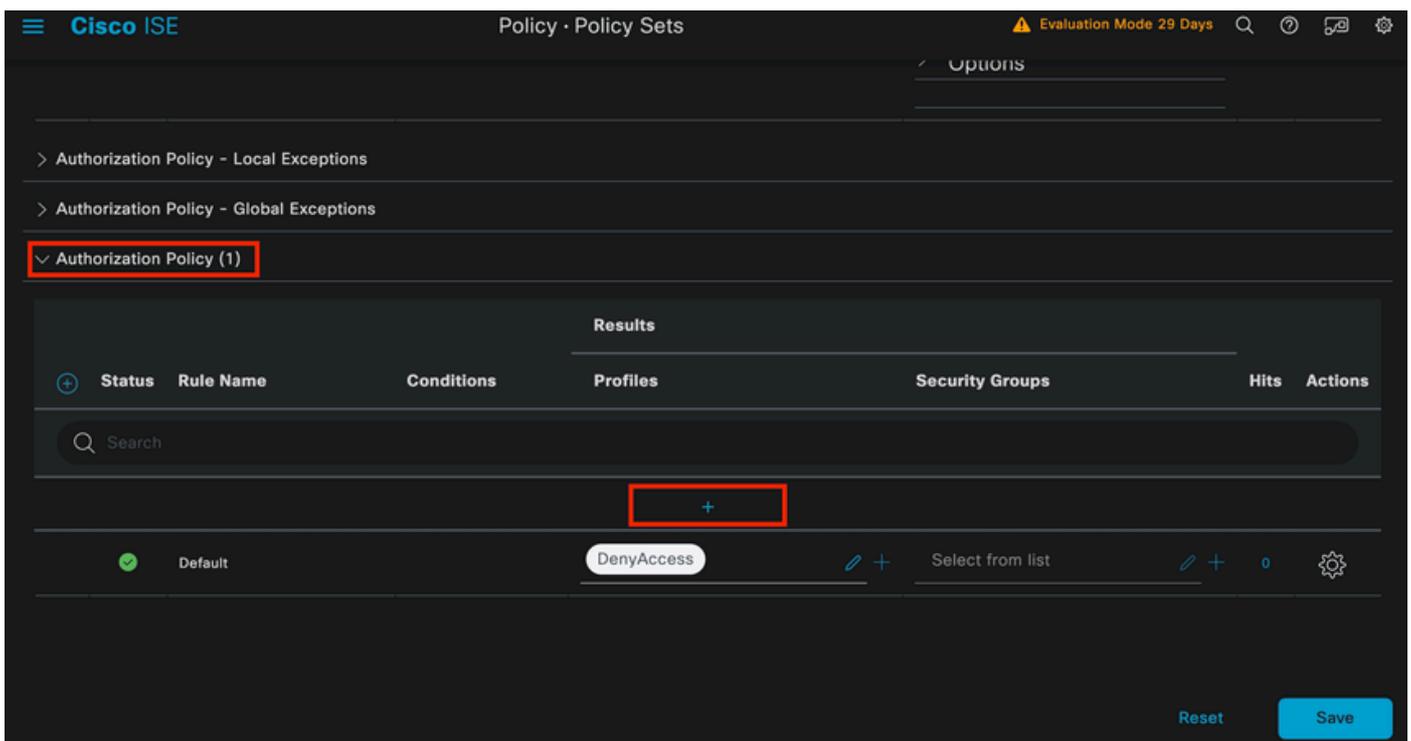
Enfin, dans la colonne Use, sélectionnez Internal Users dans la liste déroulante.



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.

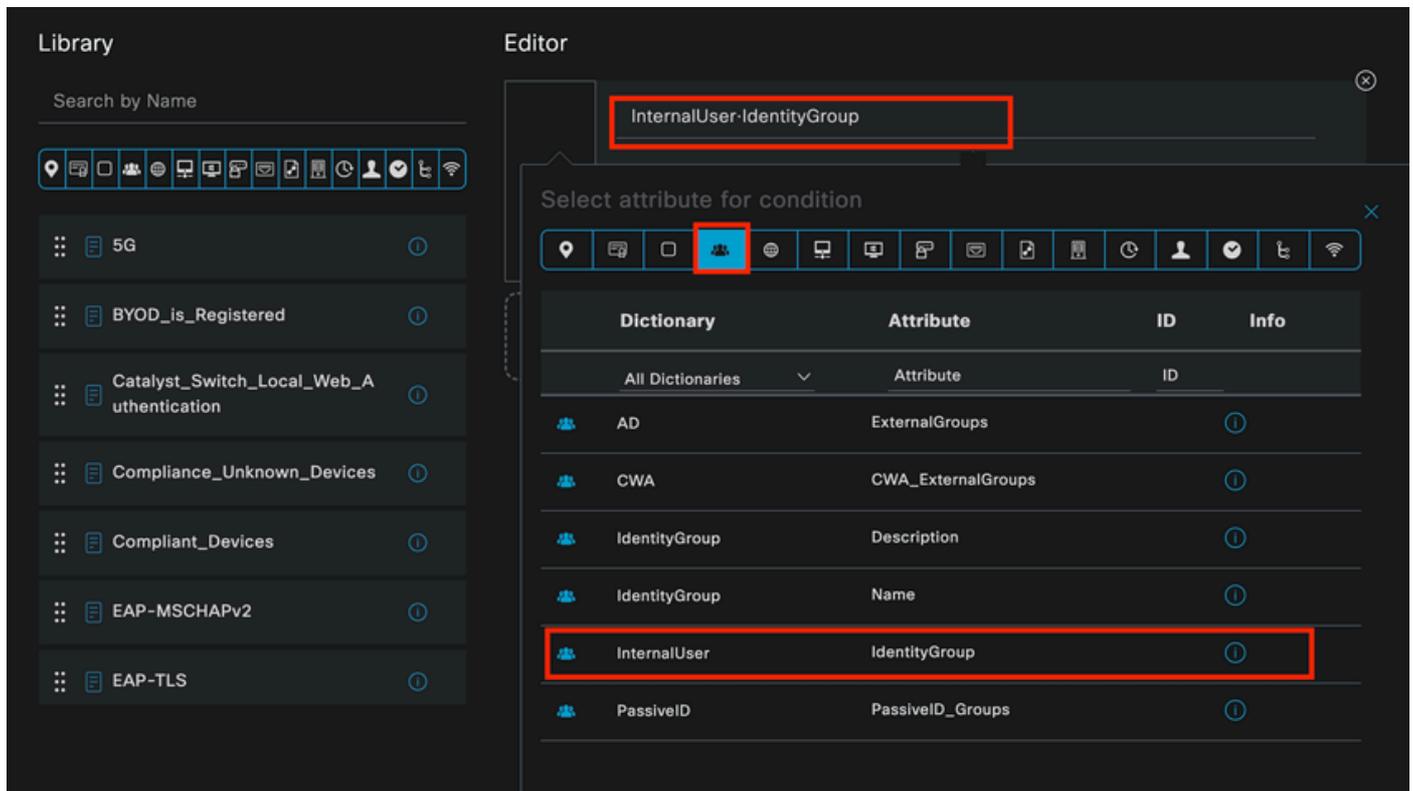
Pour créer une condition pour cette stratégie d'autorisation, cliquez sur l'icône + dans la colonne Conditions.

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.

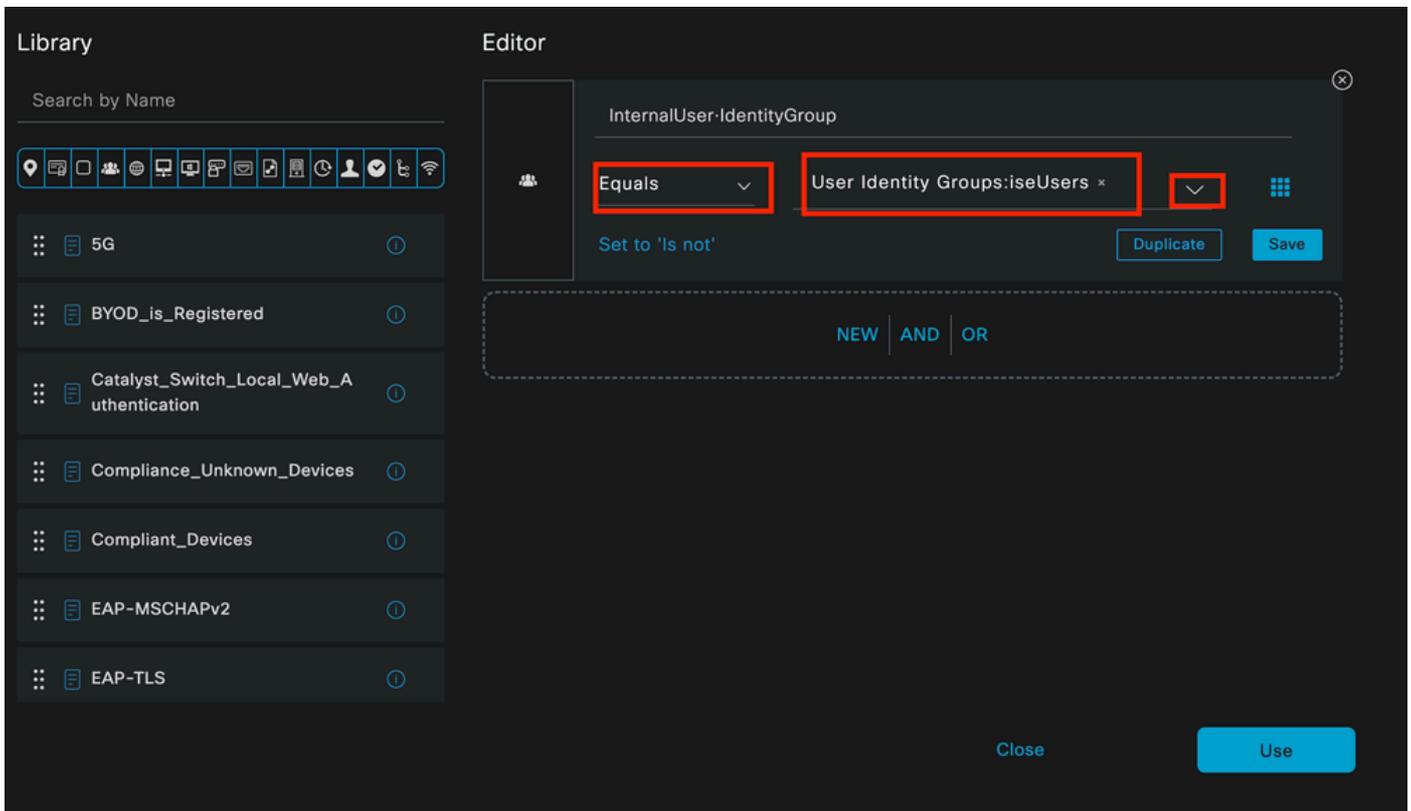
Dans le dictionnaire, sélectionnez le dictionnaire InternalUser fourni avec l'attribut Identity Group.



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

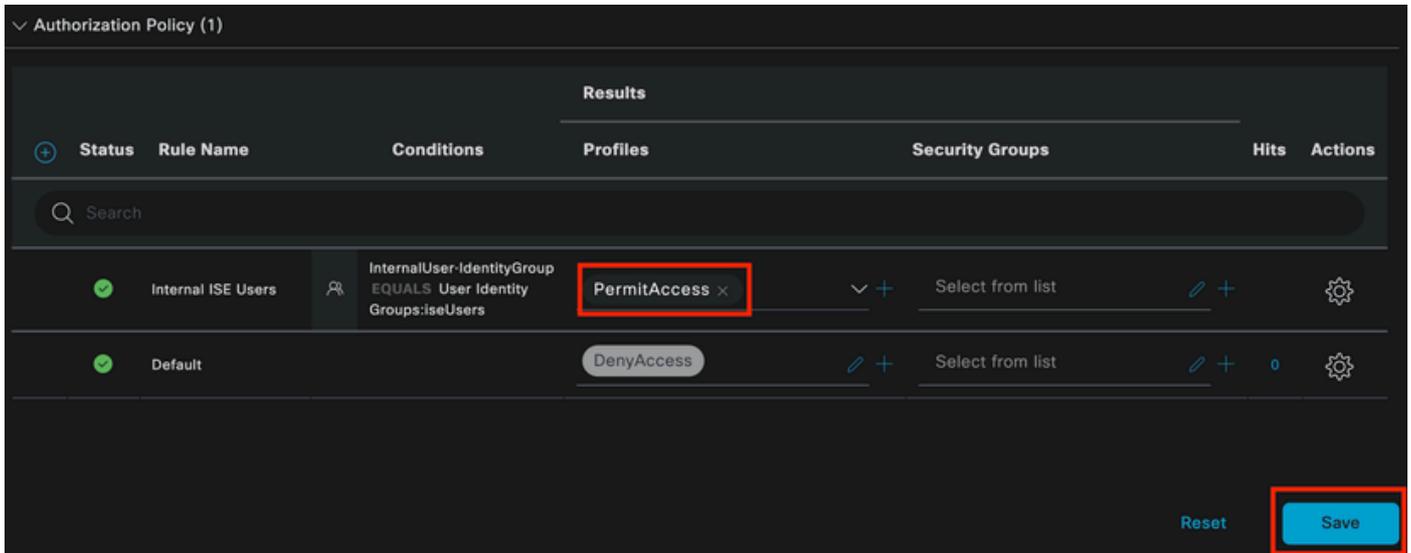
Cliquez sur Utiliser.

Enfin, sélectionnez le profil d'autorisation de résultat qui reçoit la partie authentications 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

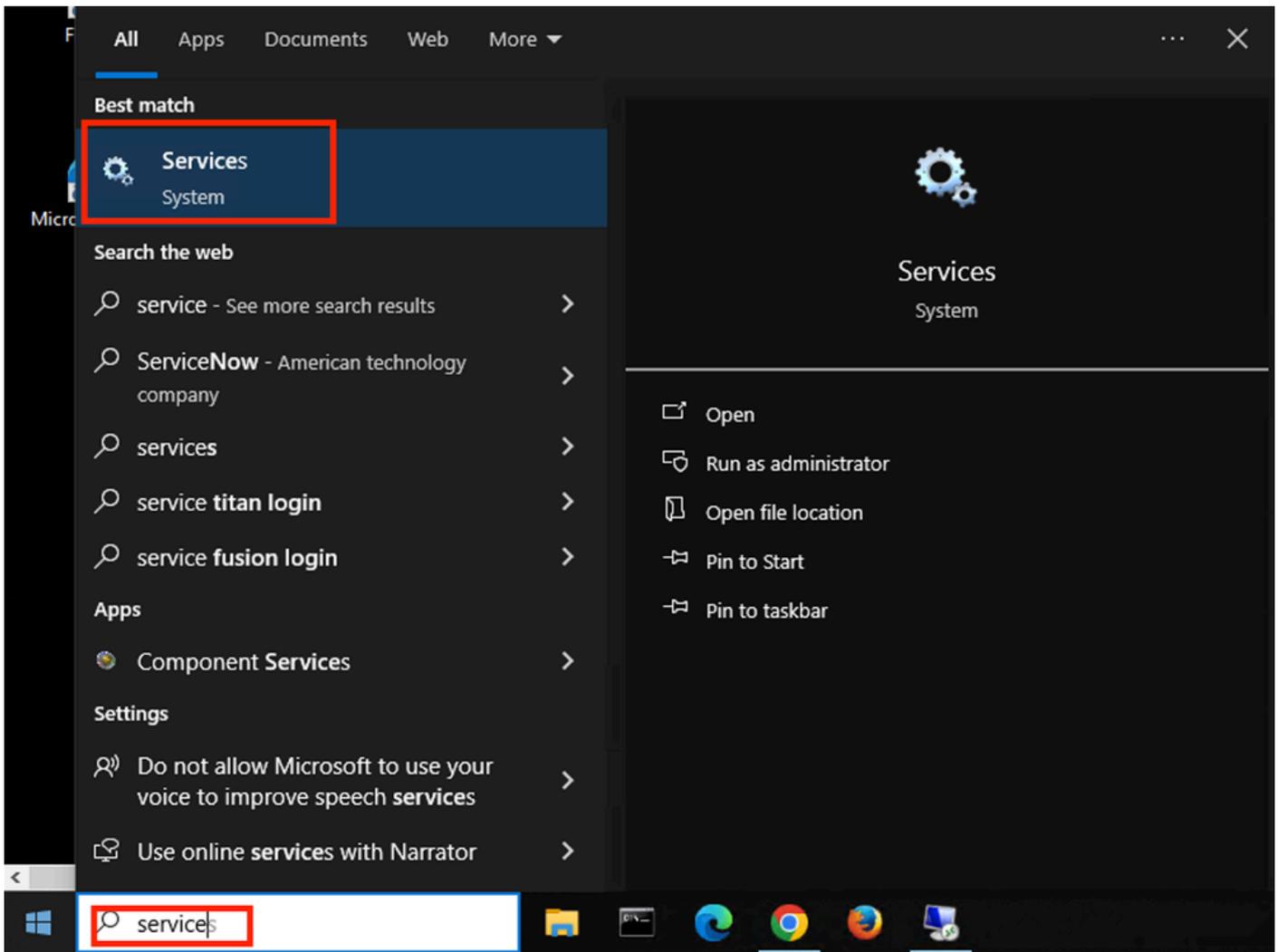
Cliquez sur Save.

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.

Wired AutoConfig Properties (Local Computer)



General Log On Recovery Dependencies

Service name: dot3svc

Display name: Wired AutoConfig

Description: responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X

Path to executable:

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

Startup type: Manual

Service status: Stopped

Start

Stop

Pause

Resume

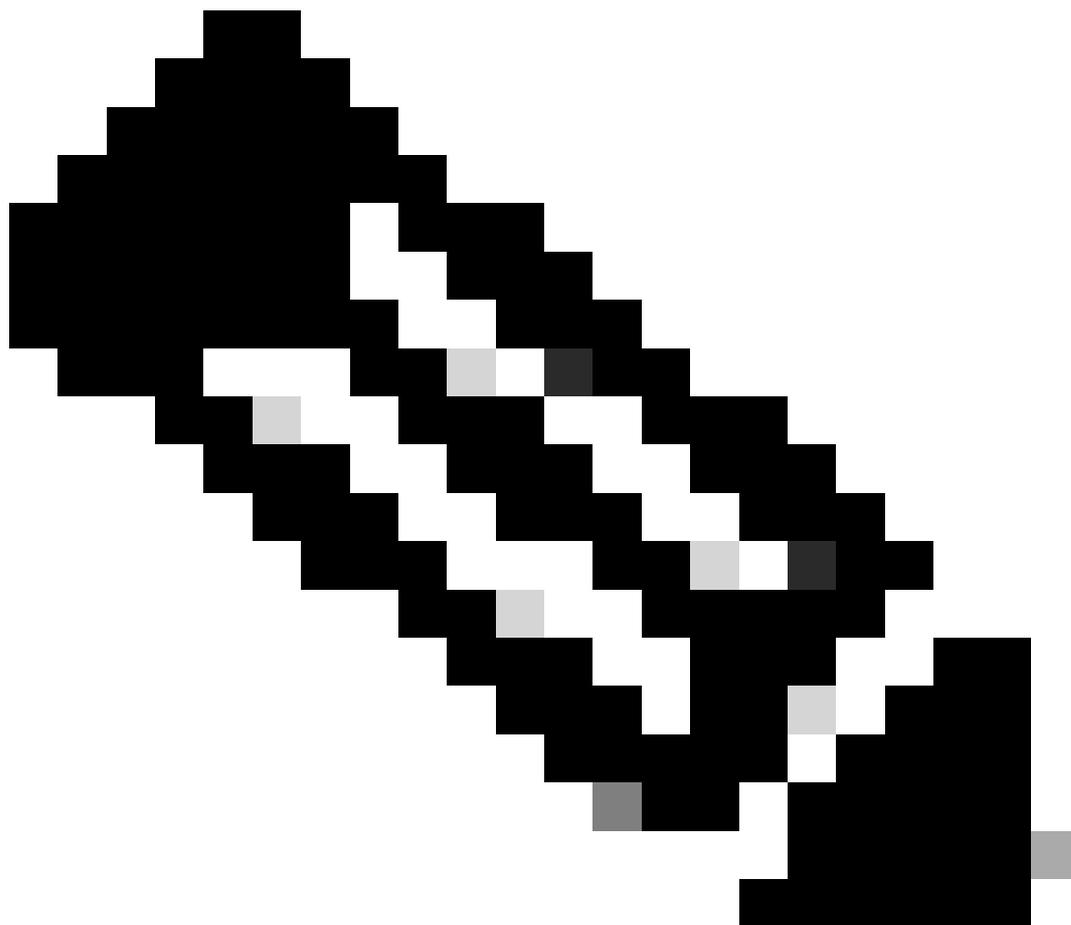
You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK

Cancel

Apply



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.

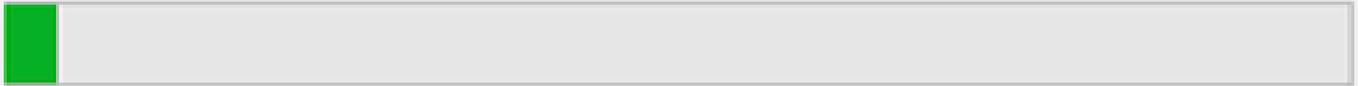
Puisque l'état du service est Arrêté. Cliquez sur Démarrer.

Service Control



Windows is attempting to start the following service on Local Computer...

Wired AutoConfig



Close

Contrôle des services

Cliquez ensuite sur OK.

Le service s'exécute ensuite.

	Windows Update	Enables the ...	Running	Manual (Trig...	Local System...
	Windows Update Medic Service	Enables rem...		Manual	Local System...
	WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
	Wired AutoConfig	The Wired A...	Running	Manual	Local System...
	WLAN AutoConfig	The WLANS...		Manual	Local System...
	WMI Performance Adapter	Provides pe...		Manual	Local System...
	Work Folders	This service ...		Manual	Local Service

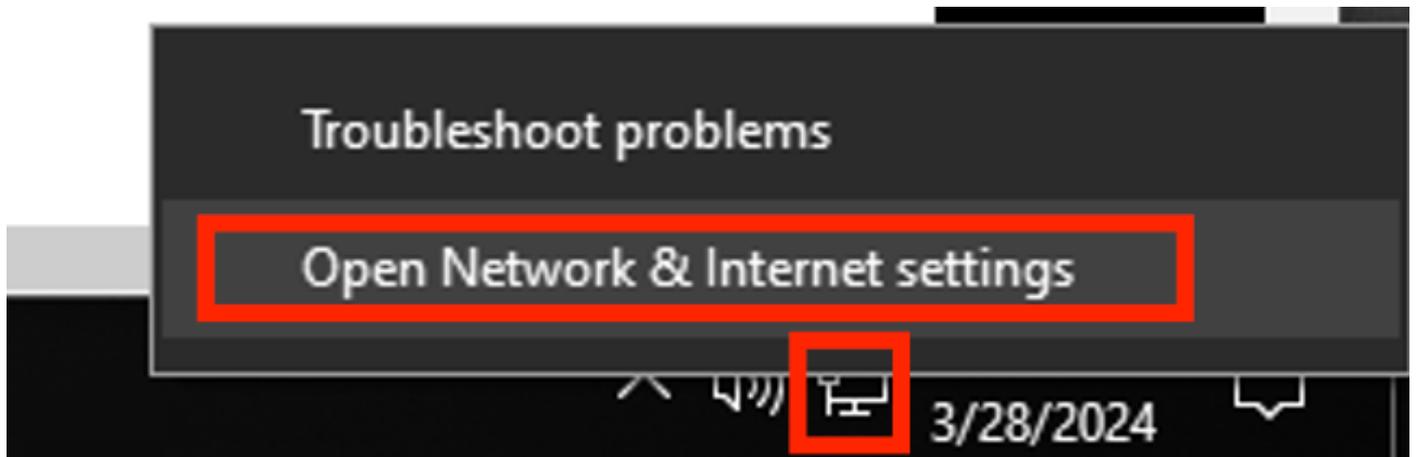
Service de configuration automatique filaire

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.

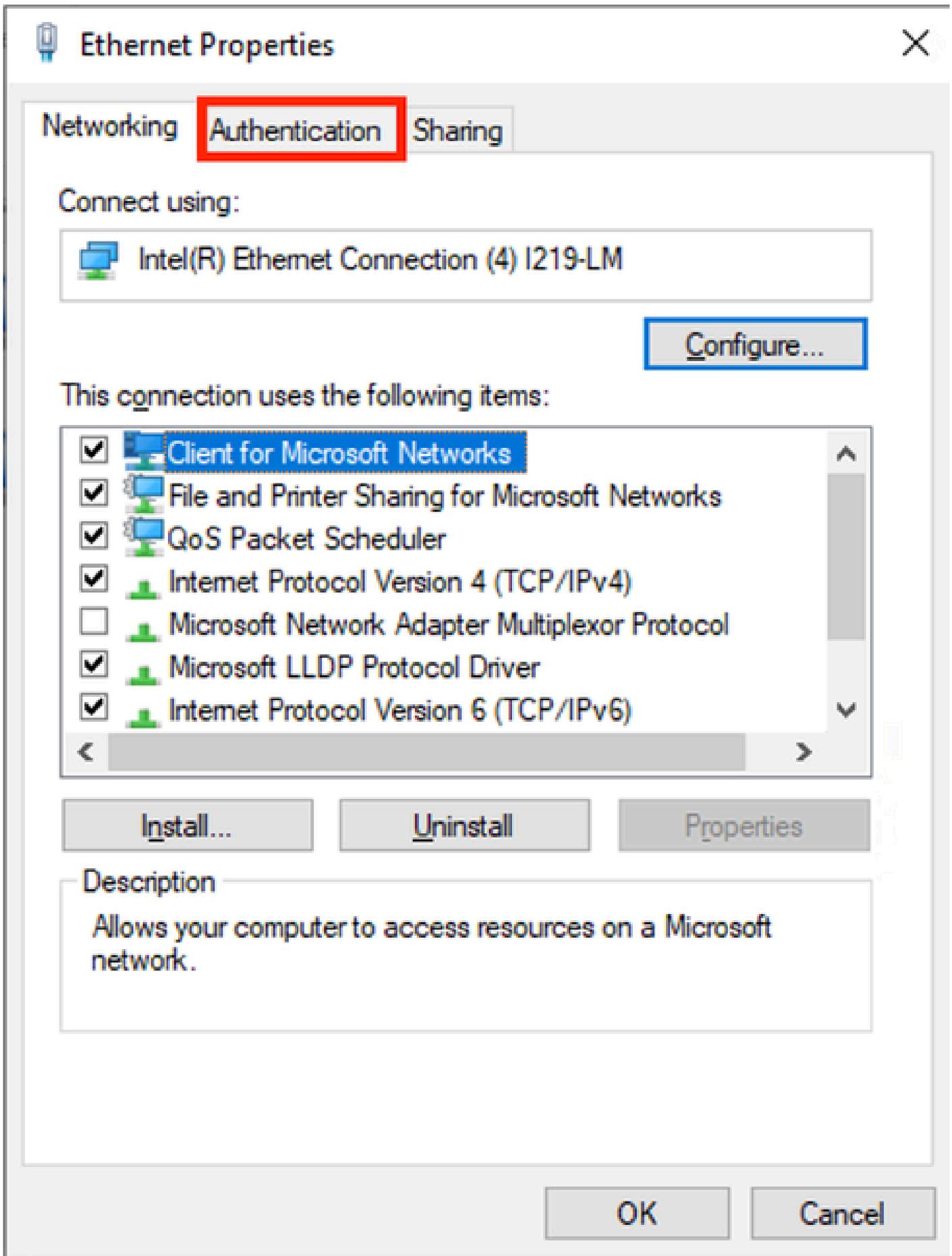
Sélectionnez Ouvrir les paramètres réseau et Internet.



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.



Ethernet Properties



Networking

Authentication

Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) ▾

Settings

Remember my credentials for this connection each time I'm logged on

Fallback to unauthorized network access

Additional Settings...

OK

Cancel

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.

Protected EAP Properties



When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2;. *\.srv3\.com):

Trusted Root Certification Authorities:

- AAA Certificate Services
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

Enable Identity Privacy

OK

Cancel

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 authentication

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.

The screenshot shows the Cisco ISE Operations - RADIUS Live Logs 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' (1), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). The main area displays a table of log entries. The table has columns: Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Name, Authentication Policy, and Authn. Two records are shown, both with the Identity 'iseiscool' and Authentication Policy 'Wired >> Internal Authentication'. The Identity and Authentication Policy columns are highlighted with red boxes.

Time	Status	Details	Repeats	Identity	Endpoint ID	Endpoint Name	Authentication Policy	Authn
Mar 28, 2024 07:04:35.4...	●		0	iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired
Mar 28, 2024 07:04:35.3...	✓		0	iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired

ISE Livelogs

The screenshot shows the Cisco ISE Operations - RADIUS Live Logs 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' (1), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). The main area displays a table of log entries. The table has columns: Authorization Policy, Authoriz..., IP Address, Network De..., Device Port, Identity Group, Posture..., and Server. Two records are shown, both with the Identity Group 'User Identity Groups:iseUsers'. The Identity Group and Server columns are highlighted with red boxes.

Authorization Policy	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Wired >> Internal ISE Users	PermitAcc...	IP Address		GigabitEthernet0/1/0			PSN01
Wired >> Internal ISE Users	PermitAcc...		ISR1100	GigabitEthernet0/1/0	User Identity Groups:iseUsers		PSN01

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

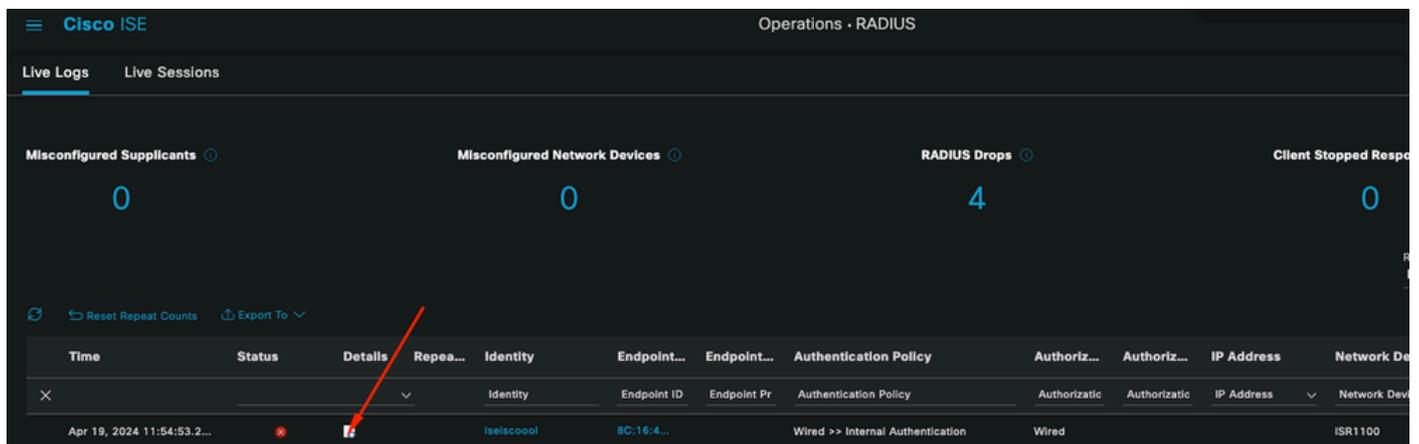
1 - Lecture des détails du journal en direct ISE

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.



The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are tabs for 'Live Logs' and 'Live Sessions'. Below this, there are four summary cards: 'Misconfigured Suppliants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (4), and 'Client Stopped Respo' (0). Below the summary cards, there are buttons for 'Reset Repeat Counts' and 'Export To'. A table of live logs is displayed with columns: Time, Status, Details, Repea..., Identity, Endpoint..., Endpoint..., Authentication Policy, Authoriz..., Authoriz..., IP Address, and Network De. A red arrow points to a search icon in the 'Details' column of the first row.

Time	Status	Details	Repea...	Identity	Endpoint...	Endpoint...	Authentication Policy	Authoriz...	Authoriz...	IP Address	Network De
Apr 19, 2024 11:54:53.2...	✖	🔍	▼	Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorizatic	Authorizatic	IP Address	Network Dev
				Iselscoool	8C:16:4...		Wired >> Internal Authentication	Wired			ISR1100

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.

Overview

Event	5400 Authentication failed
Username	iseiscool
Endpoint Id	<ENDPOINT MAC ADDRESS>#
Endpoint Profile	
Authentication Policy	Wired >> Internal Authentication
Authorization Policy	Wired
Authorization Result	

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.

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 resolution settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).
Username	iseiscool

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

15041 Evaluating Identity Policy

15013 Selected Identity Source - Internal Users ←

24210 Looking up User in Internal Users IDStore - iseiscoool ←

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 ←

11815 Inner EAP-MSCHAP authentication failed ←

11520 Prepared EAP-Failure for inner EAP method

22028 Authentication failed and the advanced options are ignored

12305 Prepared EAP-Request with another PEAP challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12304 Extracted EAP-Response containing PEAP challenge-response

61025 Open secure connection with TLS peer

12307 PEAP authentication failed ←

11504 Prepared EAP-Failure

11003 Returned RADIUS Access-Reject ←

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.

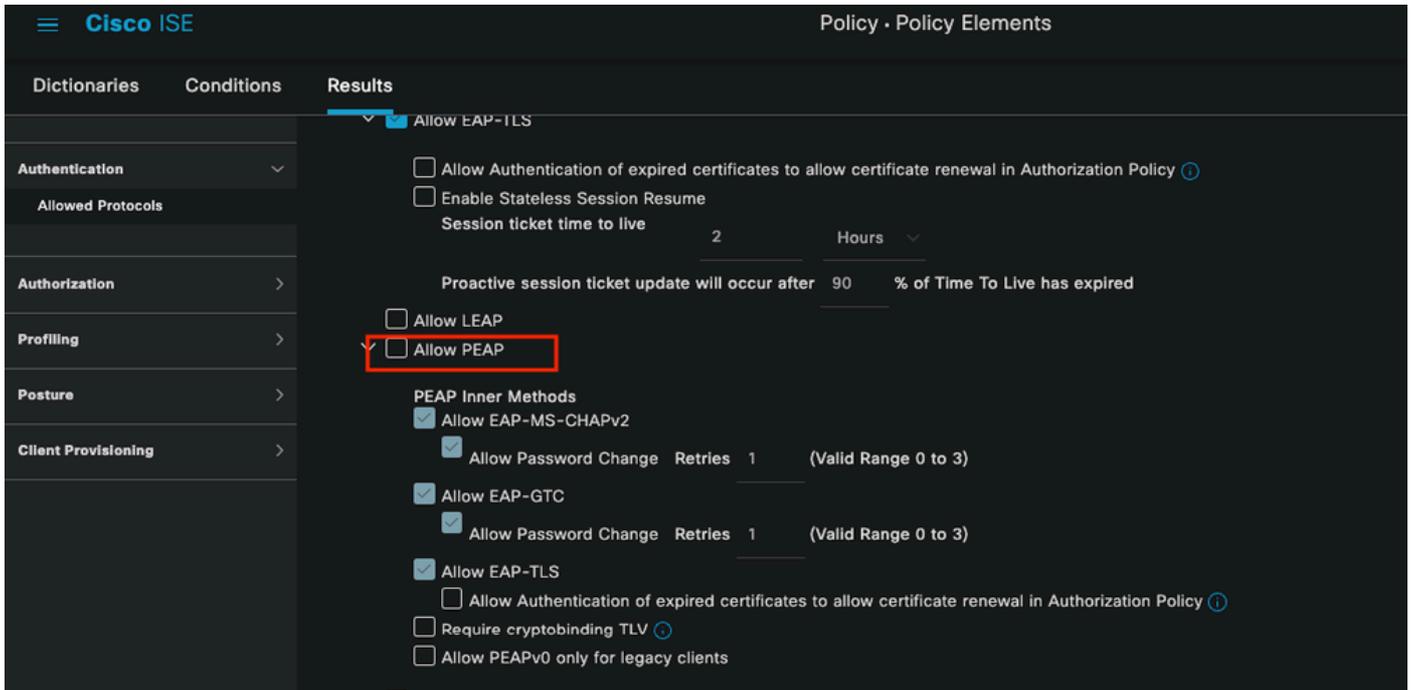
2 - PEAP désactivé

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.

Authentication Details

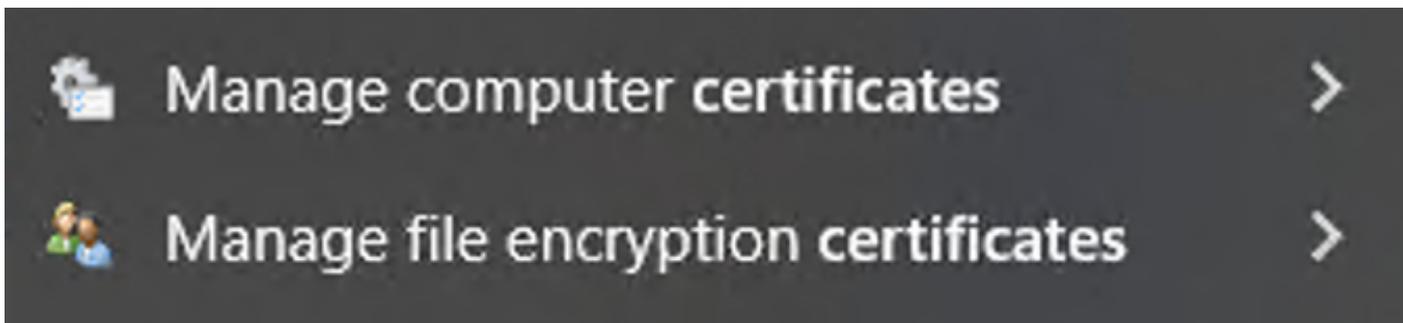
Source Timestamp	2024-04-20 04:37:42.007
Received Timestamp	2024-04-20 04:37:42.007
Policy Server	ISE PSN
Event	5411 Supplicant stopped responding to ISE
Failure Reason	12934 Supplicant stopped responding to ISE during PEAP tunnel establishment
Resolution	Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page (Administration > System > Certificates > Local Certificates). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information.
Root cause	PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate
Username	iseiscool

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.

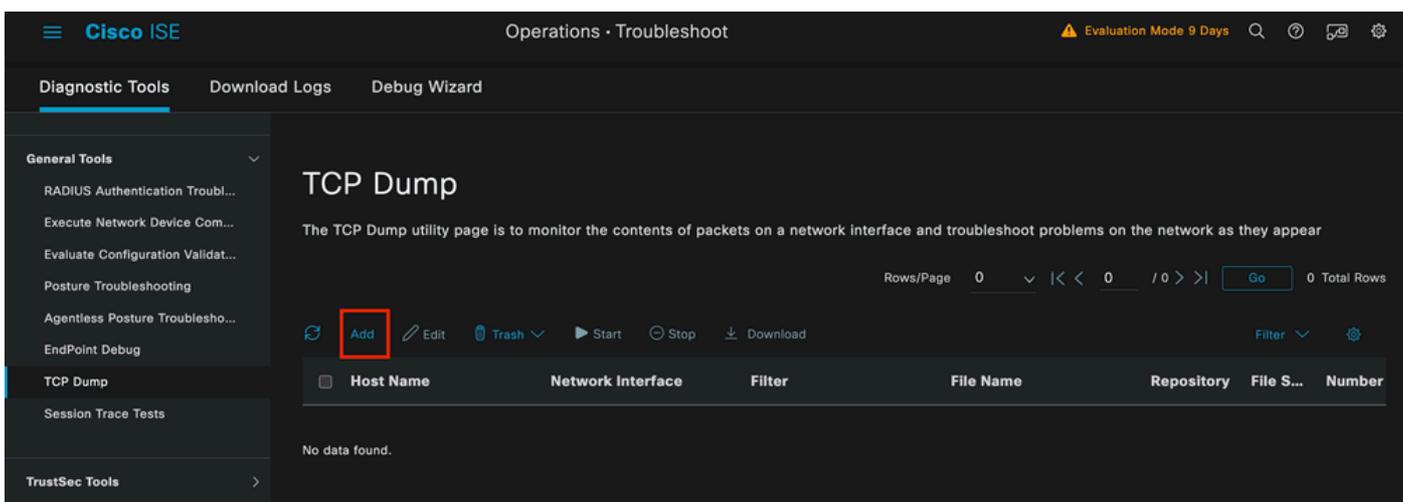


Résultats de la barre de recherche Windows

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.

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*

ISE PSN



Network Interface*

GigabitEthernet 0 [Up, Running]



Filter



E.g: ip host 10.77.122.123 and not
10.177.122.119

File Name

ISEPCAP

Création de vidage TCP

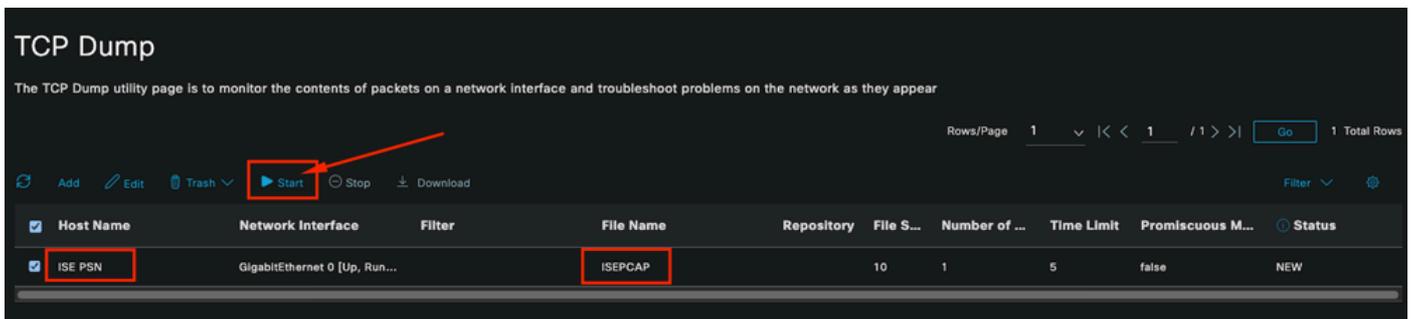
The screenshot shows a configuration window with a dark background. At the top, there is a 'Repository' dropdown menu with a downward arrow and an information icon. Below it are four input fields, each with an information icon to its right: 'File Size' with the value '10' and unit 'Mb'; 'Limit to' with the value '1' and unit 'File(s)'; and 'Time Limit' with the value '5' and unit 'Minute(s)'. At the bottom left, there is a checkbox labeled 'Promiscuous Mode' which is currently unchecked. At the bottom right, there are three buttons: 'Cancel', 'Save' (highlighted with a red border), and 'Save and Run'.

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.

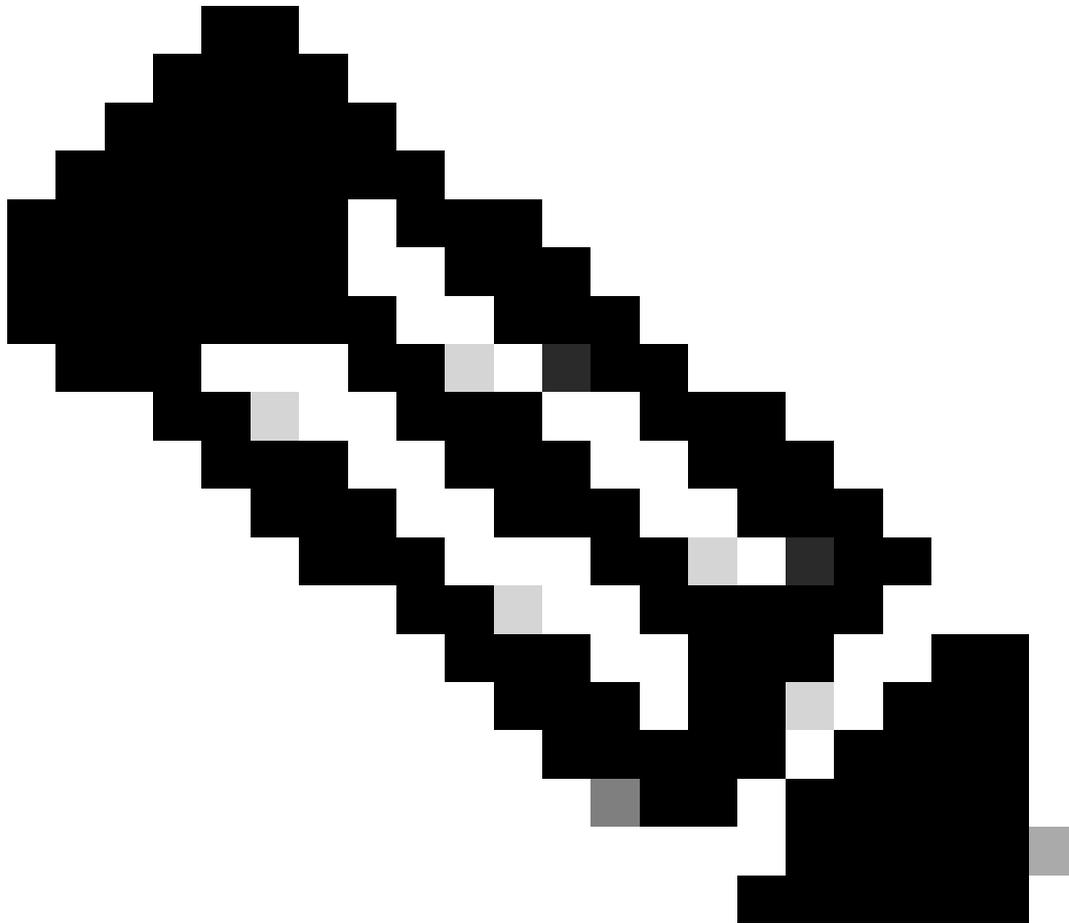
Enfin, cliquez sur le bouton Save.



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

The screenshot displays the Cisco ISE web interface. The top right corner shows the navigation path 'Operations · Reports'. The left sidebar contains a menu with 'Reports' and 'Endpoints and Users' highlighted. The main content area is titled 'RADIUS Authentications' and shows a table of authentication events. The table has four columns: 'Logged At', 'RADIUS Status', 'Details', and 'Identity'. The 'RADIUS Status' column shows several failed attempts marked with a red 'x'.

Logged At	RADIUS Status	Details	Identity
× Last 7 Days ×	↓		Identity
2024-04-20 05:10:59.176	×		iseiscool
2024-04-20 05:00:59.153	×		iseiscool
2024-04-20 04:50:59.135	×		iseiscool
2024-04-20 04:40:59.097	×		iseiscool

Section Rapports ISE

Endpoints and Users



Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

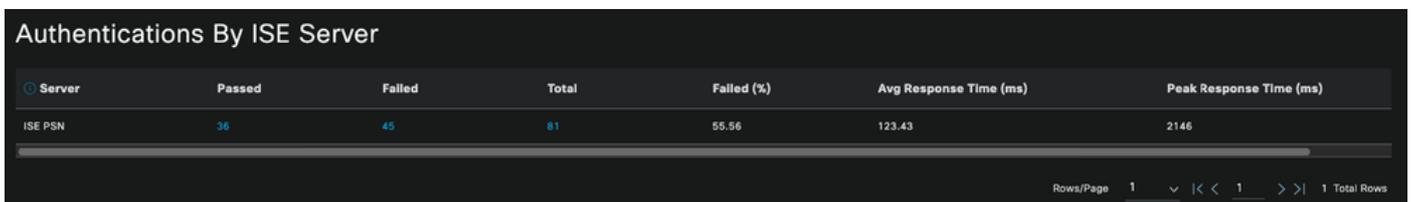
Endpoint Scripts Provisi...

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.



Server	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
ISE PSN	36	45	81	55.56	123.43	2146

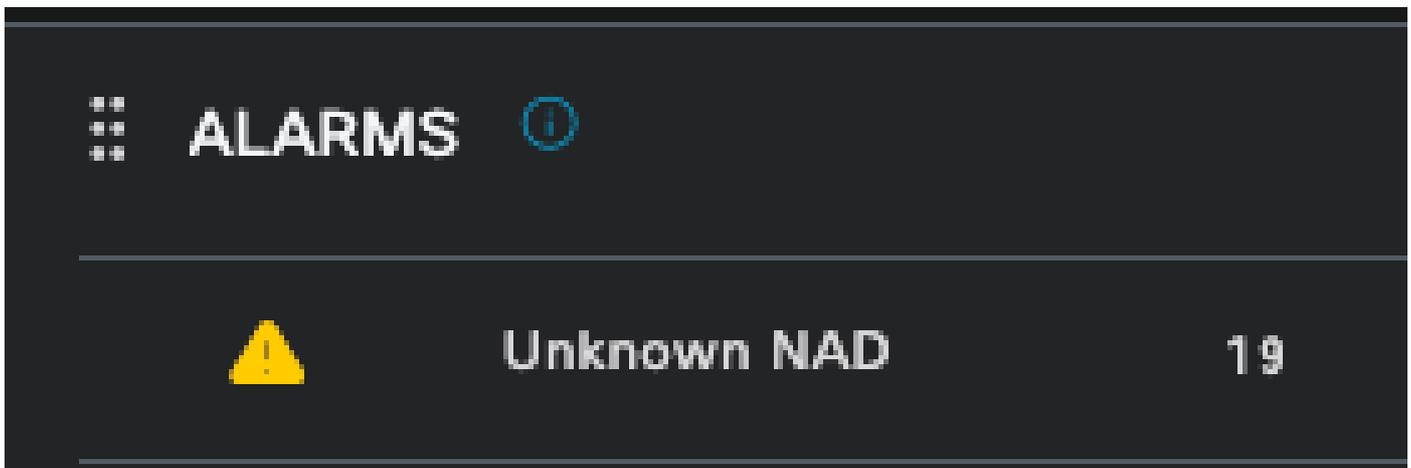
Authentications par serveur ISE

4 - Alarmes ISE

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

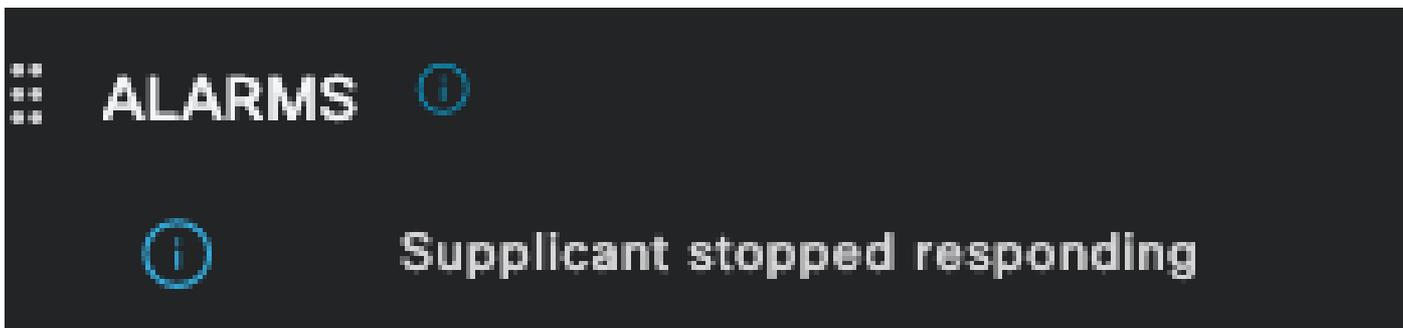
Voici plusieurs alarmes ISE qui facilitent le dépannage.

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.



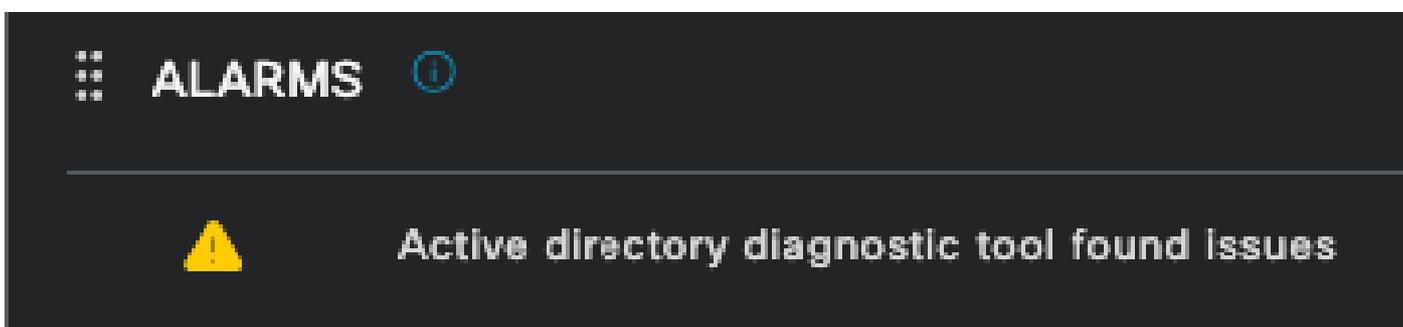
NAD inconnu

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.



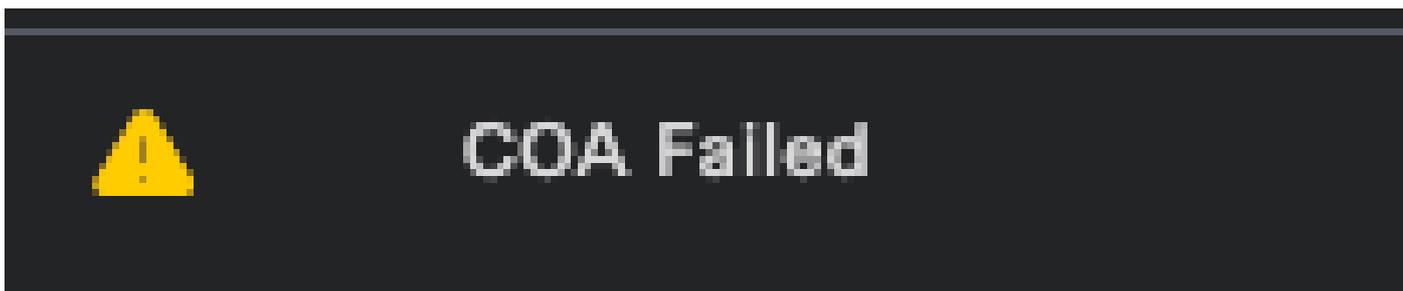
Le demandeur ne répond plus

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)

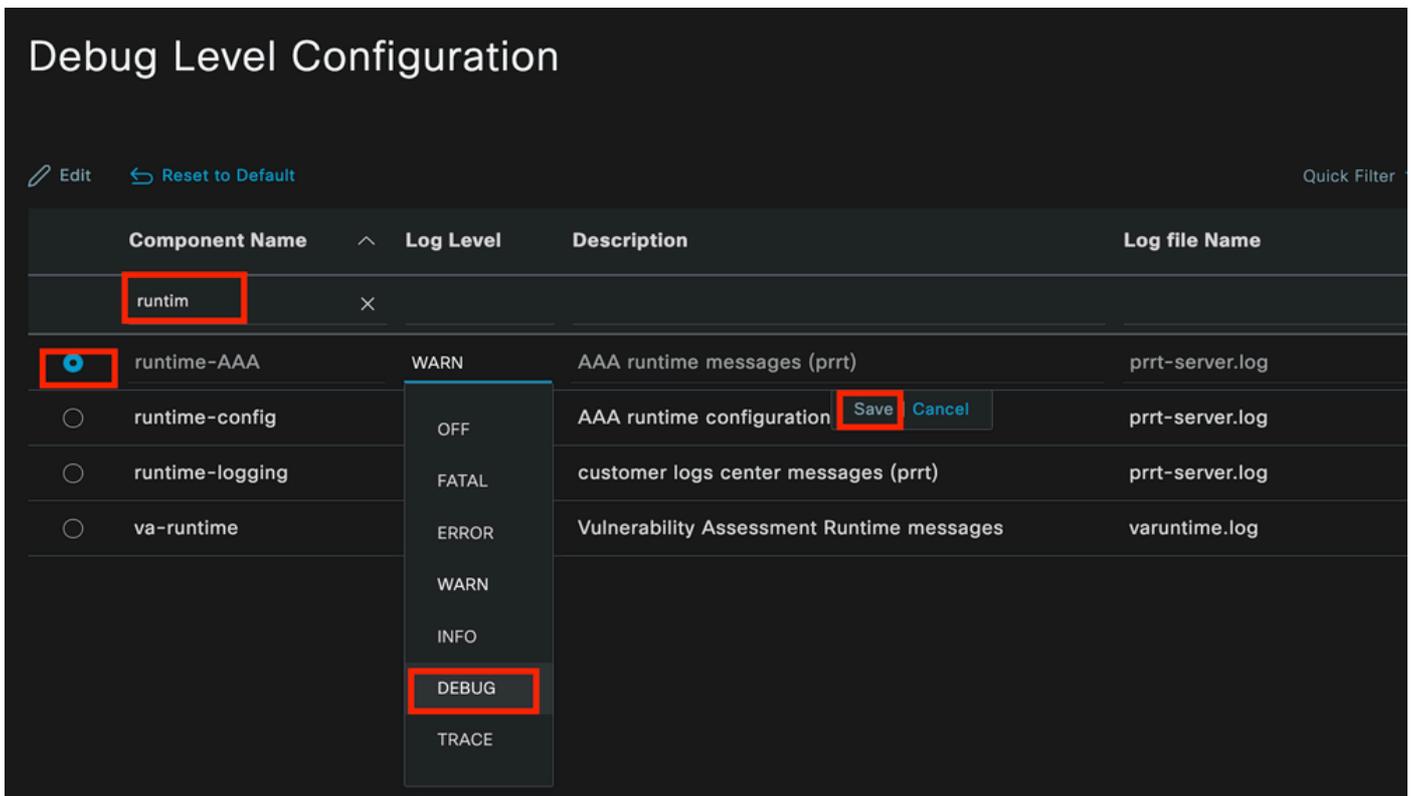
Pour activer les composants au niveau DEBUG, il est d'abord nécessaire d'identifier le PSN qui reçoit l'authentification qui échoue ou qui doit être examiné. Vous pouvez obtenir ces informations à partir des journaux en direct. Ensuite, vous devez accéder au menu ISE > Troubleshoot > Debug Wizard > Debug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

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

Component Name	Log Level	Description	Log file Name
accessfilter	INFO	RBAC resource access filter	ise-psc.log
Active Directory	WARN	Active Directory client internal messages	ad_agent.log
admin-ca	INFO	CA Service admin messages	ise-psc.log
admin-Infra	INFO	Infrastructure action messages	ise-psc.log
admin-license	INFO	License admin messages	ise-psc.log
ai-analytics	INFO	AI Analytics	ai-analytics.log
anc	INFO	Adaptive Network Control (ANC) debug messages	ise-psc.log
api-gateway	INFO	API Gateway native objects logs	api-gateway.log
apiservice	INFO	ISE API Service logs	api-service.log
bootstrap-wizard	INFO	Bootstrap wizard messages	ise-psc.log
ca-service	INFO	CA Service messages	caservice.log

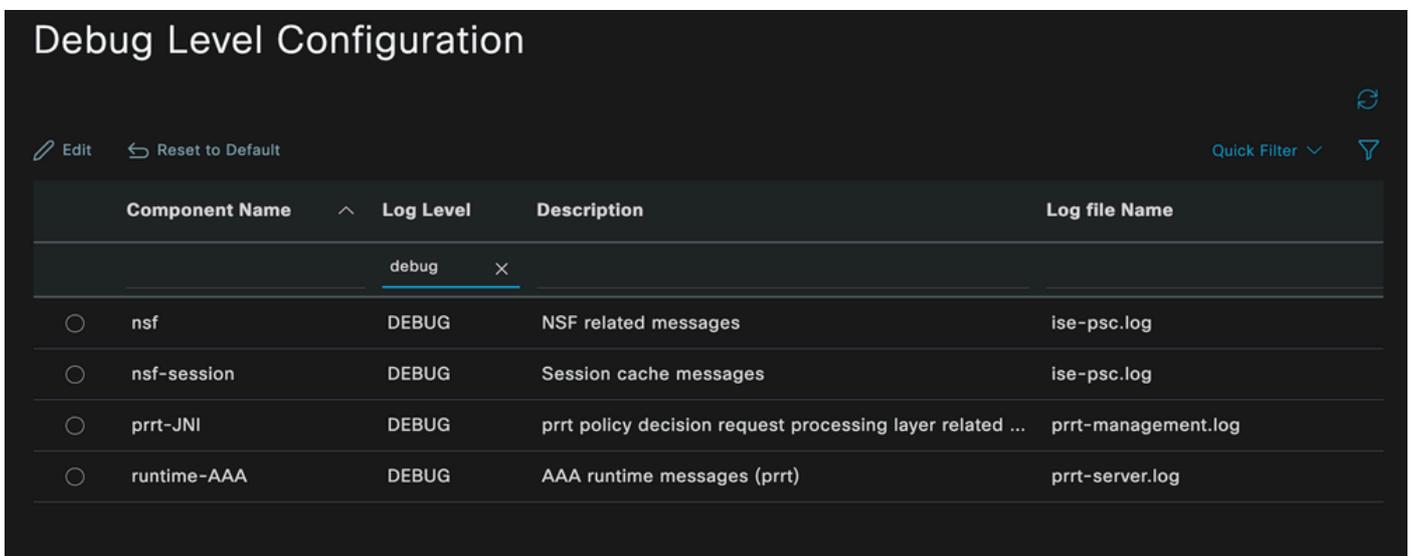
Configuration du journal de débogage

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).

Debug Log Type	Log File	Description	Size
ise-psc (16) (111 MB)			
<input type="checkbox"/>	ise-psc (all logs)	Main ise debug log messages	111 MB
<input type="checkbox"/>	ise-psc.log		5.8 MB
<input type="checkbox"/>	ise-psc.log.2024-04-03-1		7.0 MB
<input type="checkbox"/>	ise-psc.log.2024-04-04-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-05-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-06-1		7.0 MB
<input type="checkbox"/>	ise-psc.log.2024-04-07-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-08-1		6.9 MB
<input type="checkbox"/>	ise-psc.log.2024-04-09-1		7.6 MB
<input type="checkbox"/>	ise-psc.log.2024-04-10-1		8.0 MB

Journaux de débogage du noeud PSN

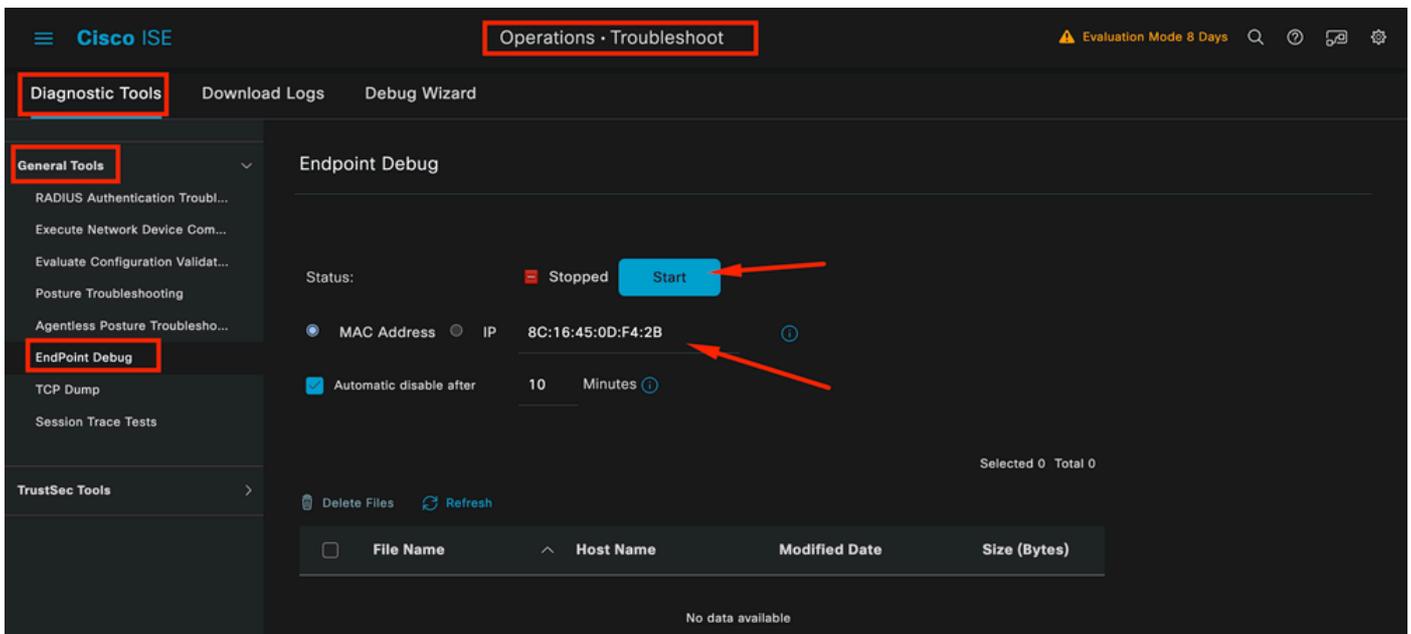
Debug Log Type	Log File	Description	Size
prrt-server (1) (7.8 MB)			
<input type="checkbox"/>	prrt-server (all logs)	Protocol Runtime runtime configuration, debug and customer logs messages	7.8 MB
<input type="checkbox"/>	prrt-server.log		7.8 MB
> pxcloud (4) (20 KB)			

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.

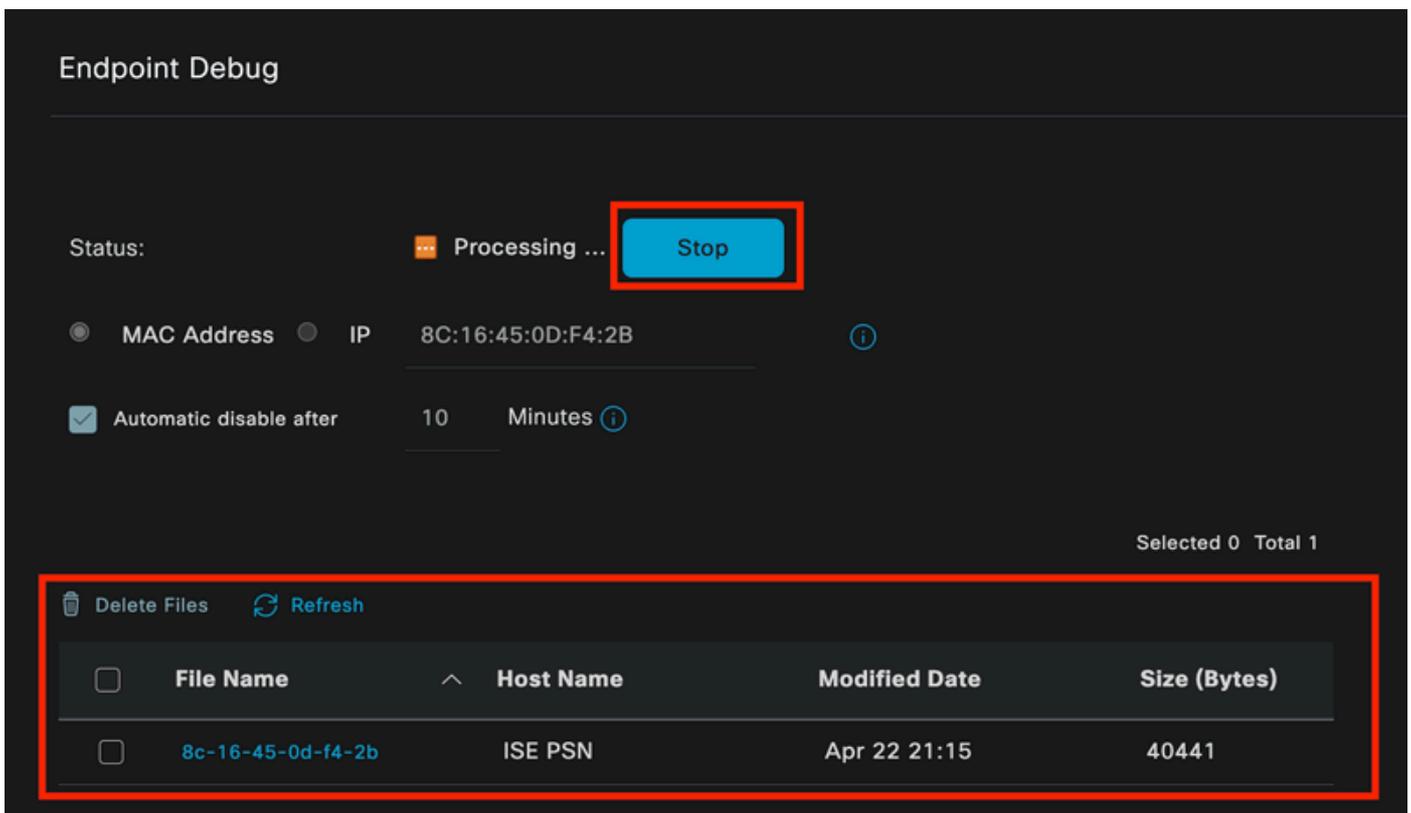
Accédez au menu ISE > Operations > Troubleshoot > Diagnostic Tools > General Tools > Endpoint Debug.



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.

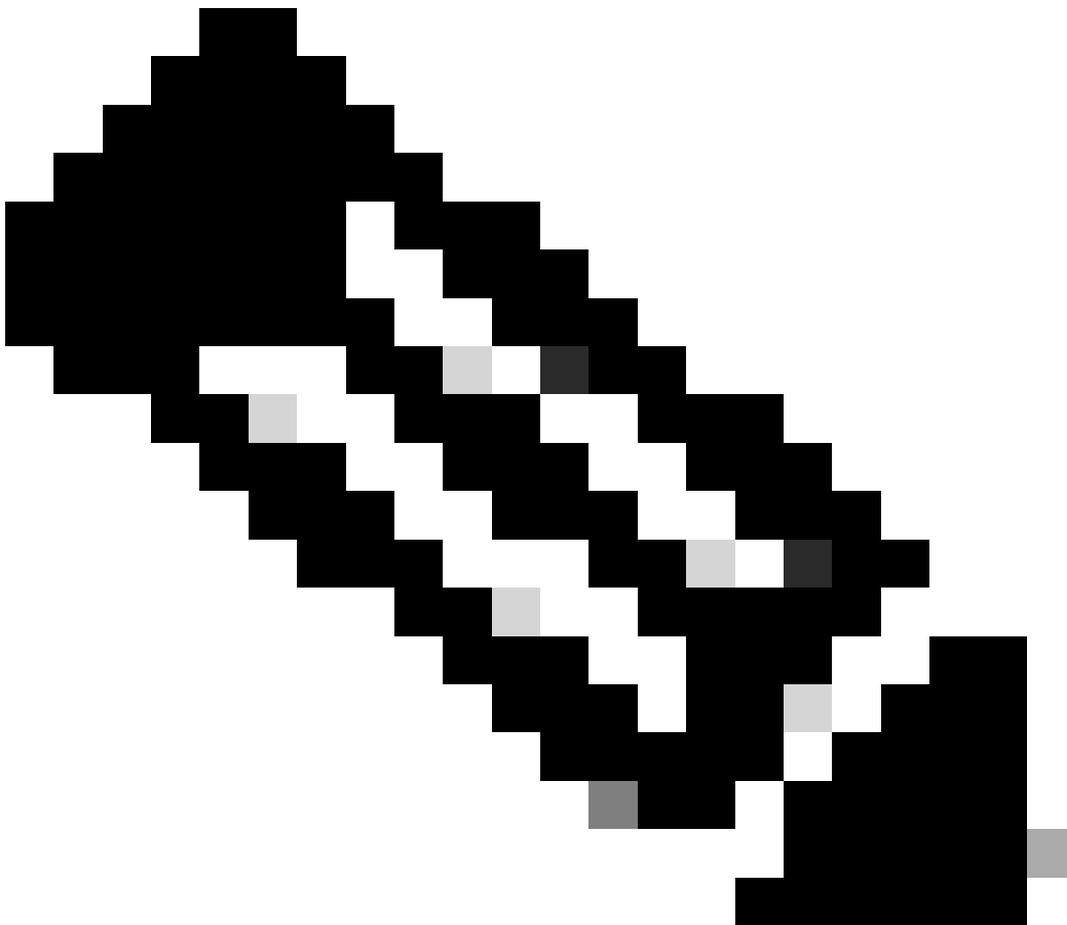
Selected 1 Total 1

Delete Files Refresh

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input checked="" type="checkbox"/>	8c-16-45-0d-f4-2b	ISE PSN	Apr 22 21:17	67959712

Débogage des terminaux

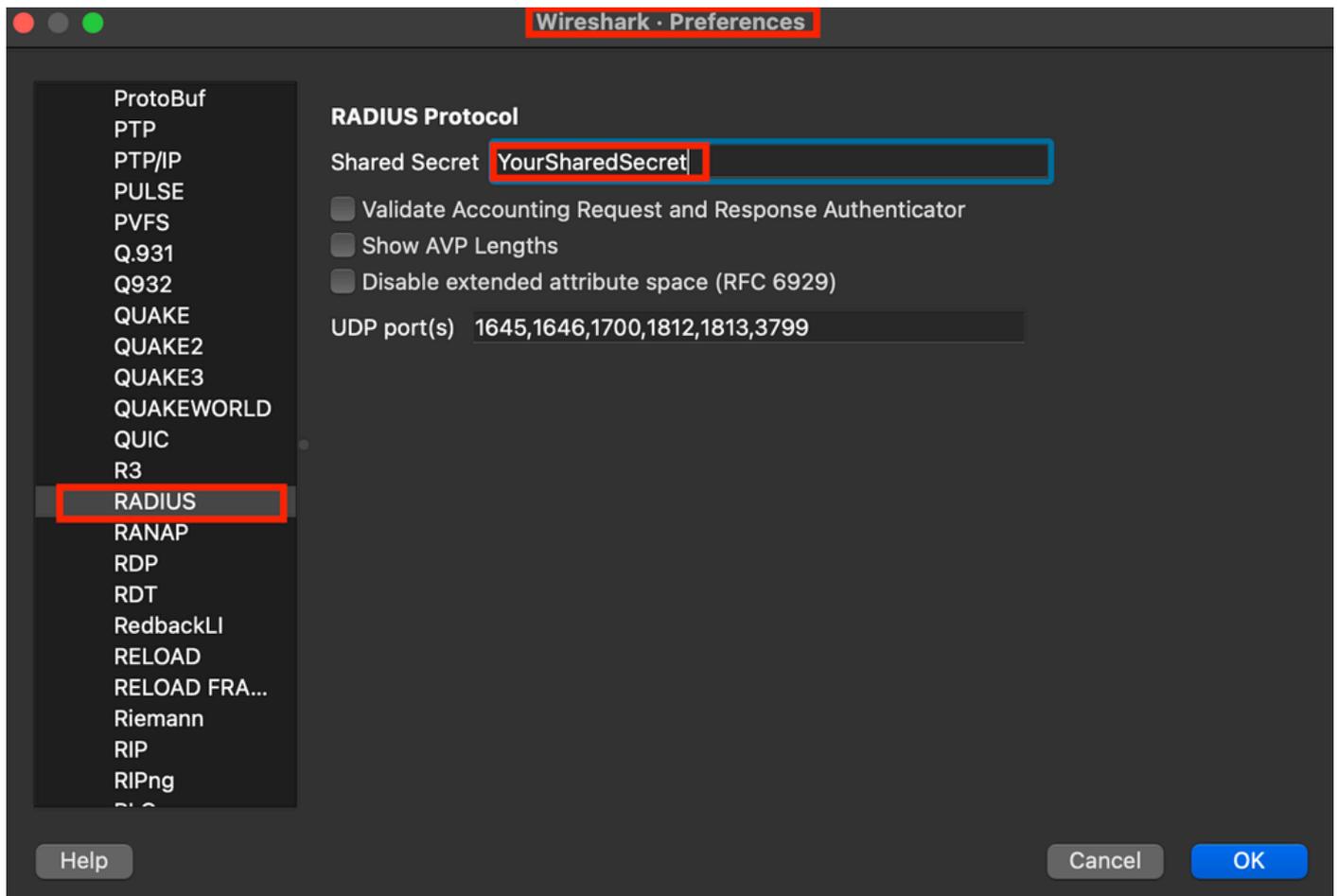
Vous devez pouvoir voir les journaux d'authentification avec les journaux DEBUG sans les activer directement à partir de la configuration du journal de débogage.



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

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

Quarantined: No

Authn: 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
    WNCN Platform: max 0, current 0 total 0
    IOSN Platform : max 0, current 0 total 0

Consecutive Timeouts: total 3
    SMD Platform : max 0, current 0 total 0
    WNCN Platform: max 0, current 0 total 0
    IOSN 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: 22781FOA0000000C0777AECD
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 COHVSRAISE01-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 COHVSRAISE01-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.