

Configuration et déploiement du profil NAM du client sécurisé via ISE 3.3 sous Windows

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration](#)

[Diagramme du réseau](#)

[Flux de données](#)

[Configurer le commutateur](#)

[Télécharger le package client sécurisé](#)

[Configuration ISE](#)

[Étape 1. Télécharger le package sur ISE](#)

[Étape 2. Créer un profil NAM à partir de l'outil Éditeur de profil](#)

[Étape 3. Télécharger le profil NAM sur ISE](#)

[Étape 4. Créer un profil de posture](#)

[Étape 5. Créer une configuration d'agent](#)

[Étape 6. Politique de provisionnement client](#)

[Étape 7. Politique de posture](#)

[Étape 8. Ajouter un périphérique réseau](#)

[Étape 9. Profil d'autorisation](#)

[Étape 10. Protocoles autorisés](#)

[Étape 11. Active Directory](#)

[Étape 12. Ensembles de stratégies](#)

[Vérifier](#)

[Étape 1. Téléchargez et installez le module Secure Client Posture/NAM depuis ISE](#)

[Étape 2. EAP-FAST](#)

[Étape 3. Balayage De Posture](#)

[Dépannage](#)

[Étape 1. Profil NAM](#)

[Étape 2. Journalisation étendue NAM](#)

[Étape 3. Débogages sur le commutateur](#)

[Étape 4. Débogages sur ISE](#)

[Informations connexes](#)

Introduction

Ce document décrit comment déployer le profil Cisco Secure Client Network Access Manager (NAM) via Identity Services Engine (ISE).

Informations générales

L'authentification EAP-FAST se déroule en deux phases. Dans la première phase, EAP-FAST utilise une connexion TLS pour fournir et authentifier les échanges de clés à l'aide d'objets Type-Length-Values (TLV) afin d'établir un tunnel protégé. Ces objets TLV sont utilisés pour transmettre des données liées à l'authentification entre le client et le serveur. Une fois le tunnel établi, la deuxième phase commence avec le client et le noeud ISE qui engagent d'autres conversations pour établir les politiques d'authentification et d'autorisation requises.

Le profil de configuration NAM est configuré pour utiliser EAP-FAST comme méthode d'authentification et est disponible pour les réseaux définis par l'administrateur.

En outre, les types de connexion des ordinateurs et des utilisateurs peuvent être configurés dans le profil de configuration NAM.

Le périphérique Windows d'entreprise obtient un accès complet à l'entreprise en utilisant le NAM avec contrôle de position.

Le périphérique Windows personnel accède à un réseau restreint à l'aide de la même configuration NAM.

Ce document fournit des instructions pour déployer le profil Cisco Secure Client Network Access Manager (NAM) via le portail Posture Identity Services Engine (ISE) à l'aide du déploiement Web, ainsi que la vérification de la conformité de la position.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Identity Services Engine (ISE)
- AnyConnect NAM et Éditeur de profil
- Politique de posture
- Configuration de Cisco Catalyst pour les services 802.1x

Composants utilisés

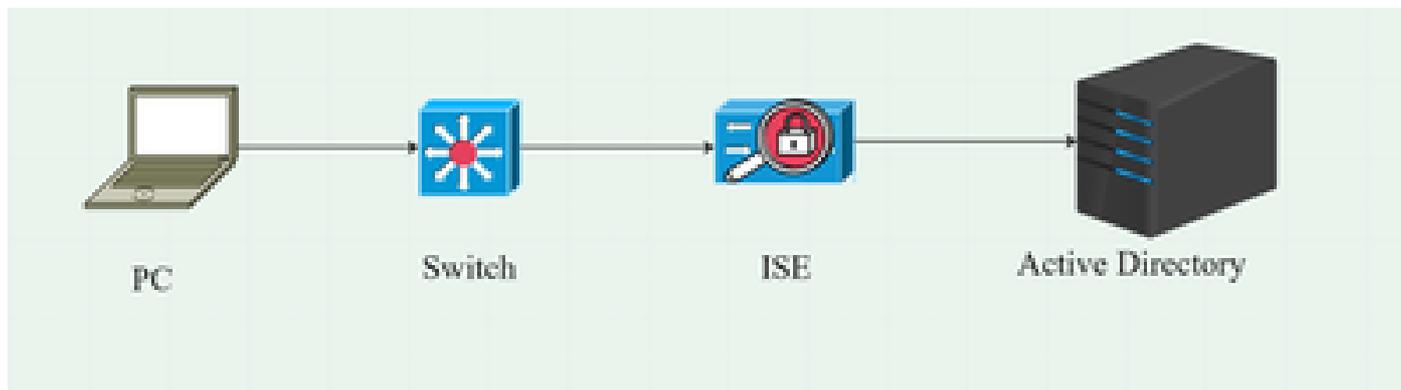
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE, versions 3.3 et ultérieures
- Windows 10 avec Cisco Secure Mobility Client 5.1.4.74 et versions ultérieures
- Commutateur Cisco Catalyst 9200 avec logiciel Cisco IOS® XE 17.6.5 et versions ultérieures
- Active Directory 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Diagramme du réseau



Flux de données

Lorsqu'un PC se connecte au réseau, l'ISE fournit la stratégie d'autorisation pour la redirection vers le Portail Posture.

Le trafic http sur le PC est redirigé vers la page de mise en service du client ISE, où l'application NSA est téléchargée à partir d'ISE.

La NSA installe ensuite les modules d'agent Secure Client sur le PC.

Une fois l'installation de l'agent terminée, l'agent télécharge les profils Posture et NAM configurés sur ISE.

L'installation du module NAM déclenche un redémarrage sur l'ordinateur.

Après le redémarrage, le module NAM effectue l'authentification EAP-FAST en fonction du profil NAM.

L'analyse de position est ensuite déclenchée et la conformité est vérifiée en fonction de la stratégie de position ISE.

Configurer le commutateur

Configurez le commutateur d'accès pour l'authentification et la redirection dot1x.

```
aaa new-model  
  
aaa authentication dot1x default group radius  
aaa authorization network default group radius  
aaa accounting dot1x default start-stop group radius  
serveur aaa radius dynamic-author  
client 10.127.197.53 clé-serveur Qwerty123  
auth-type any
```

```
aaa session-id common
ip radius source-interface Vlan100
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf majuscules
Serveur RADIUS RAD1
address ipv4 <IP du serveur ISE> auth-port 1812 acct-port 1813
key <clé-secrète>

dot1x system-auth-control
```

Configurez la liste de contrôle d'accès de redirection pour que l'utilisateur soit redirigé vers ISE Client Provisioning Portal.

```
ip access-list extended redirect-acl
10 deny udp any any tout domaine eq
20 deny tcp any any any eq domain
30 deny udp any eq bootpc any eq bootps
40 deny ip any host <IP du serveur ISE>
50 permit tcp any any eq www
60 permit tcp any any eq 443
```

Activez le suivi des périphériques et la redirection http sur le commutateur.

```
stratégie de suivi des périphériques <nom de la stratégie de suivi des périphériques>
activation du suivi
interface <nom de l'interface>
device-tracking attach-policy <nom de la stratégie de suivi des périphériques>

ip http server
ip http secure-server
```

Télécharger le package client sécurisé

Téléchargez manuellement les fichiers de déploiement Web de l'Éditeur de profil, des fenêtres Secure Client et du Module de conformité depuis software.cisco.com

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

Téléchargements Accueil > Sécurité > Sécurité des terminaux > Client sécurisé (y compris AnyConnect) > Client sécurisé 5 > Logiciel client VPN AnyConnect

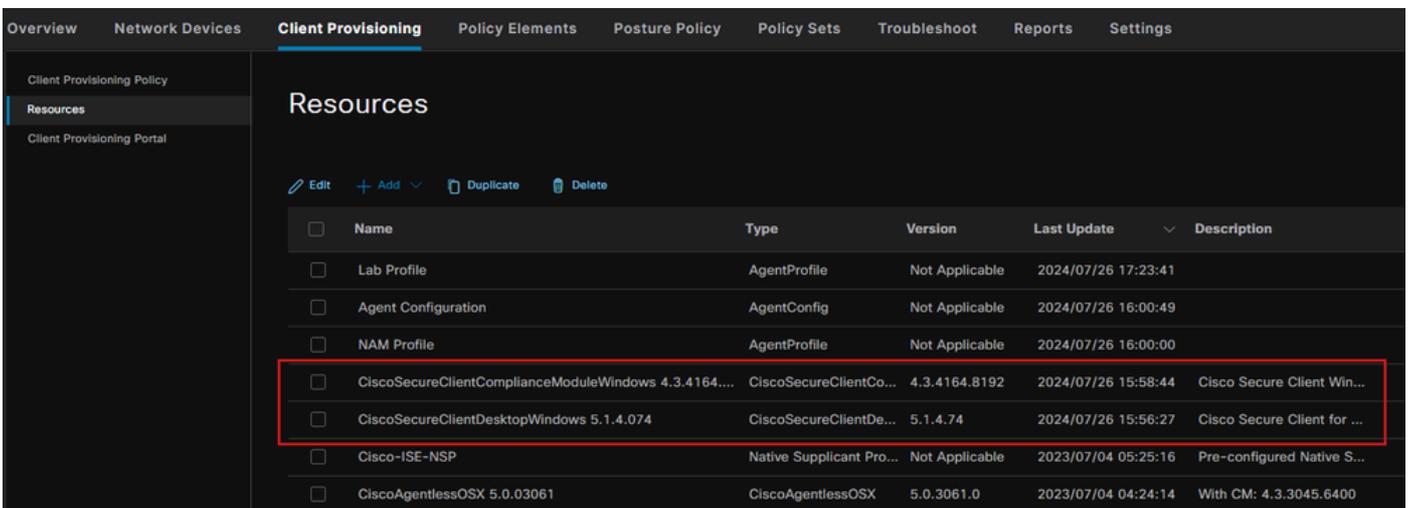
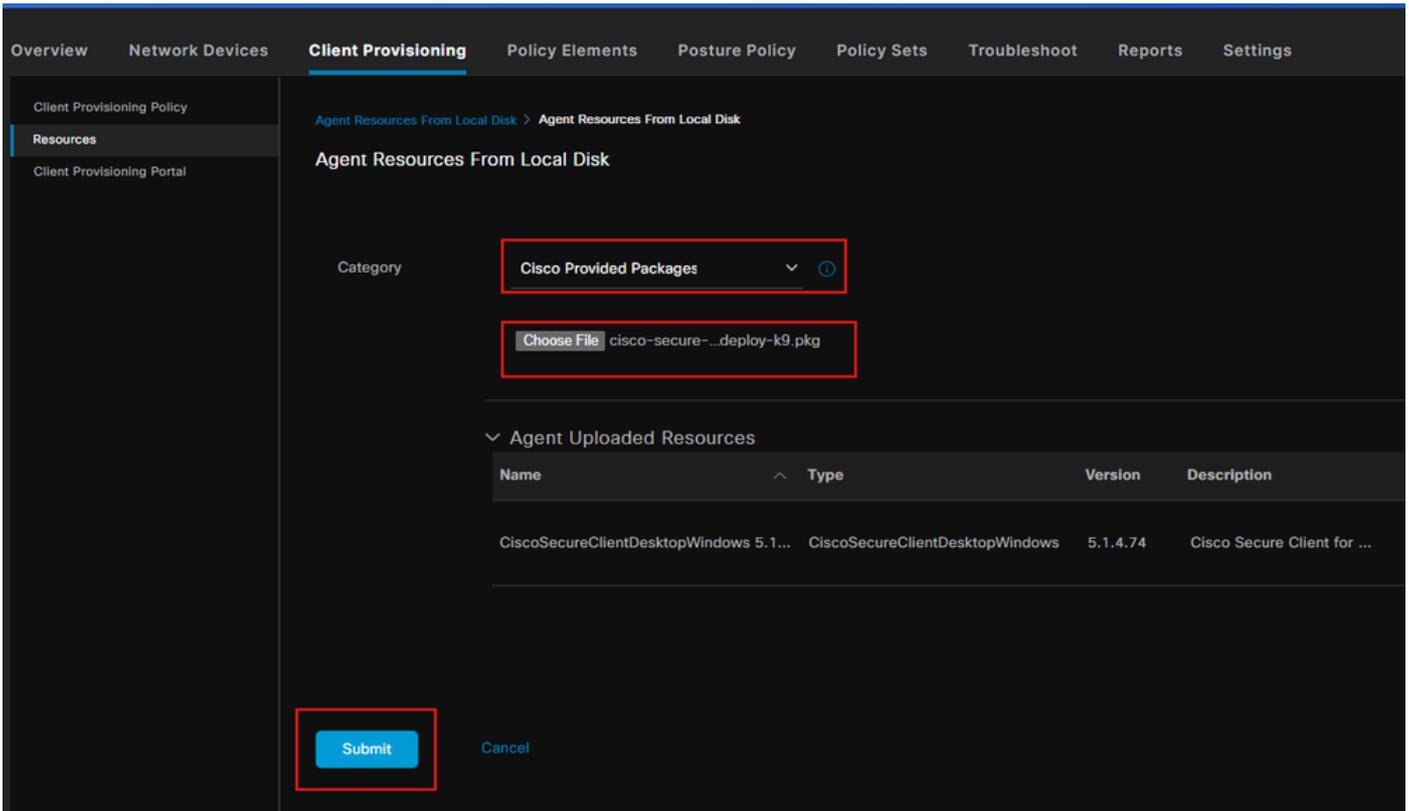
- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

- cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

Configuration ISE

Étape 1. Télécharger le package sur ISE

Pour télécharger les packages de déploiement Web Secure Client and Compliance Module sur ISE, accédez à Workcenter > Posture > Client Provisioning > Resources > Add > Agent Resources from Local Disk.

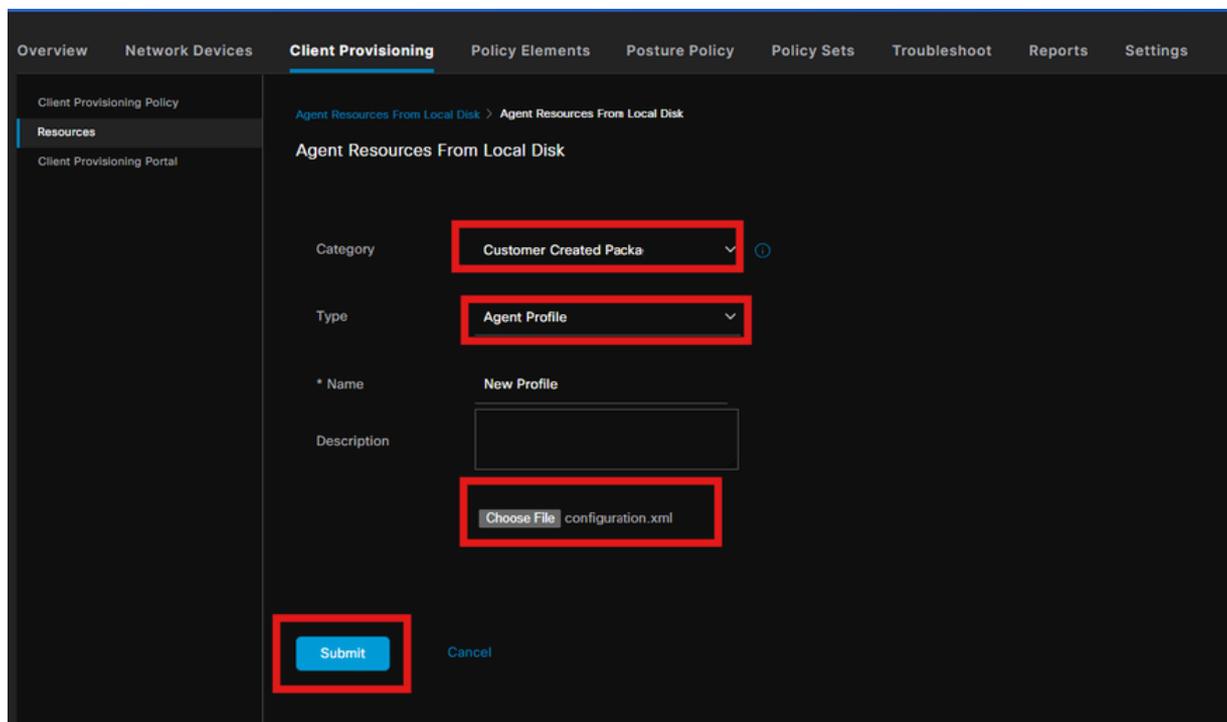


Étape 2. Créer un profil NAM à partir de l'outil Éditeur de profil

Pour plus d'informations sur la façon de configurer un profil NAM, référez-vous à ce guide [Configure Secure Client NAM Profile](#) .

Étape 3. Télécharger le profil NAM sur ISE

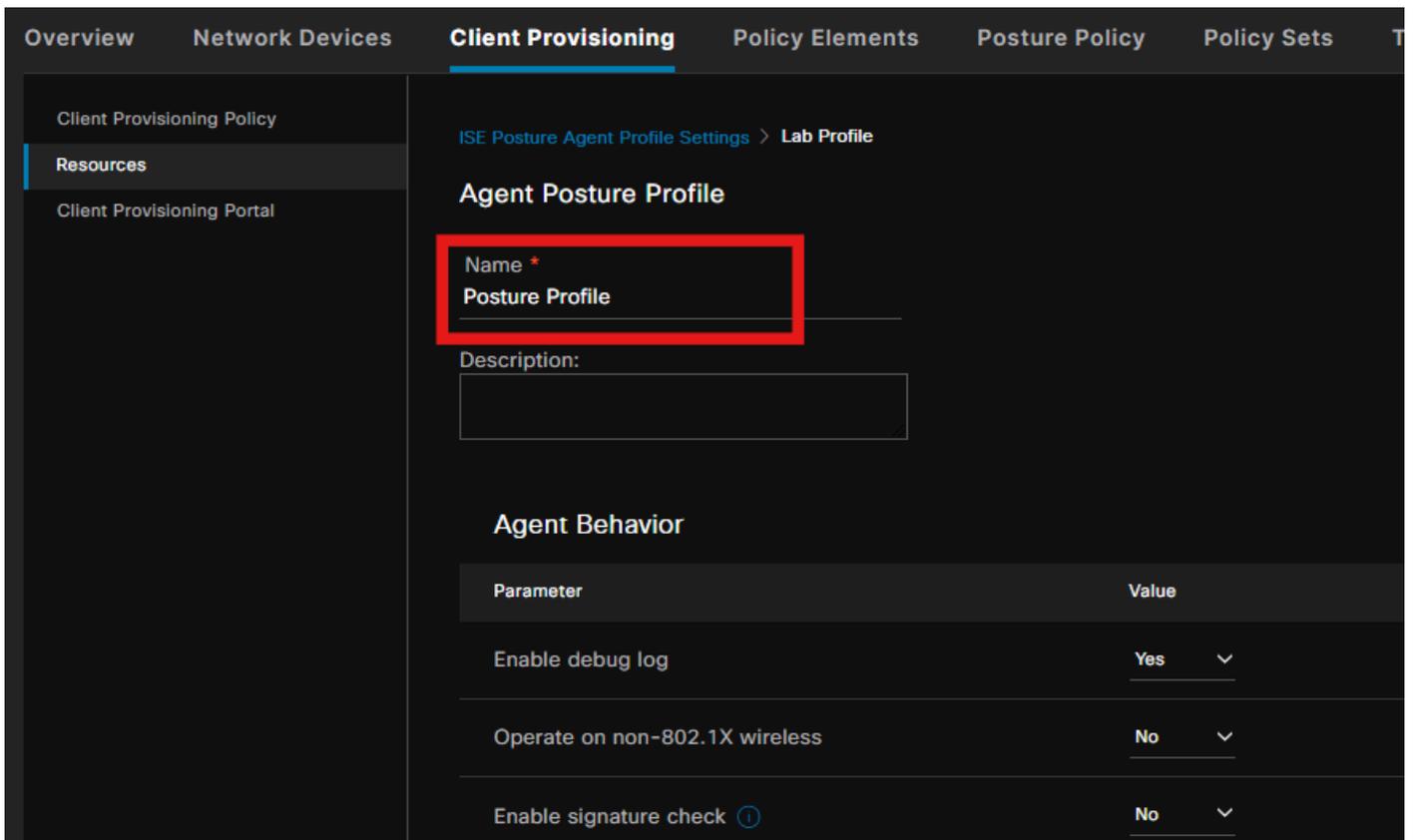
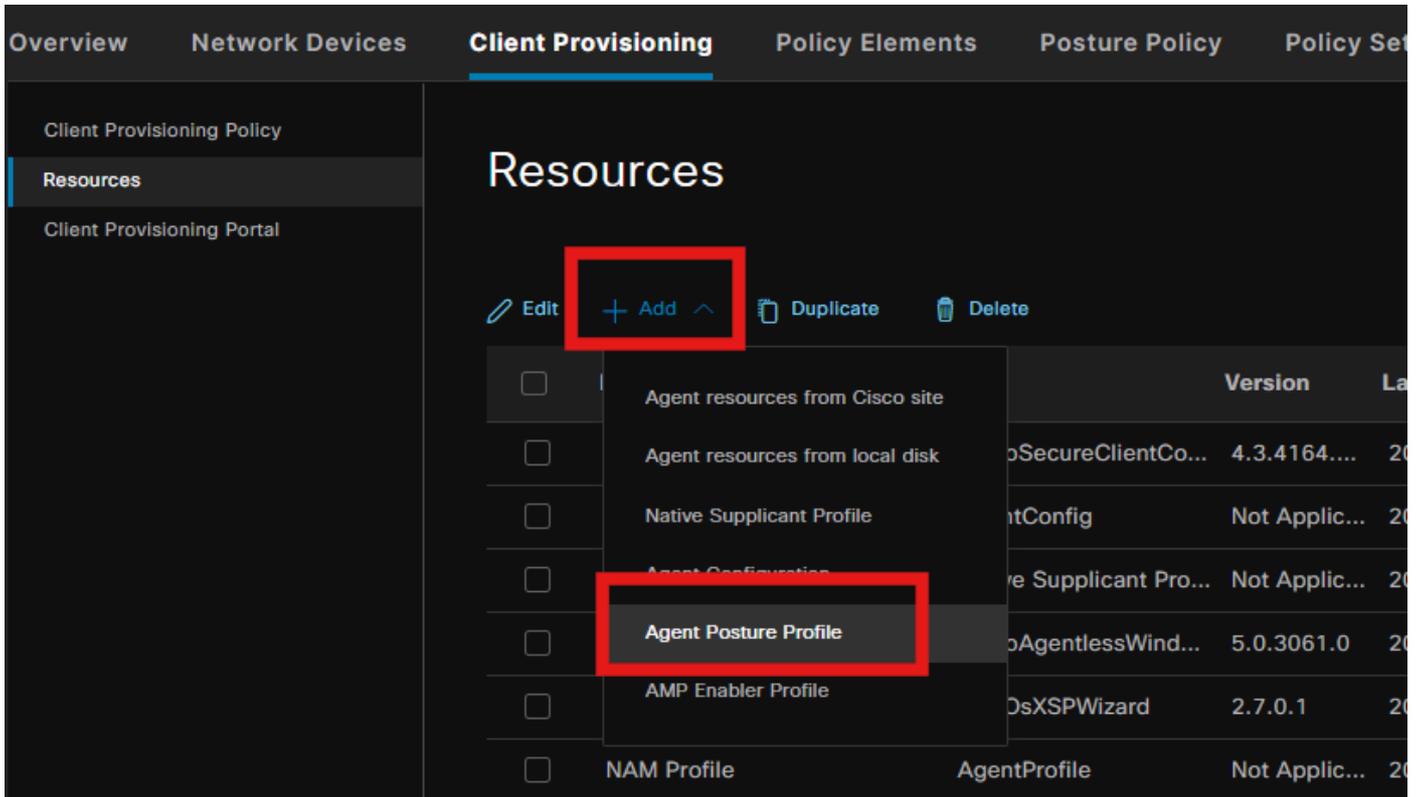
Pour télécharger le profil NAM « Configuration.xml » sur ISE en tant que profil d'agent, accédez à Client Provisioning > Resources > Agent Resources From Local Disk.



The screenshot displays the ISE Client Provisioning interface. The top navigation bar includes 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Settings'. The left sidebar shows 'Client Provisioning Policy', 'Resources', and 'Client Provisioning Portal'. The main content area is titled 'Agent Resources From Local Disk' and contains the following fields:

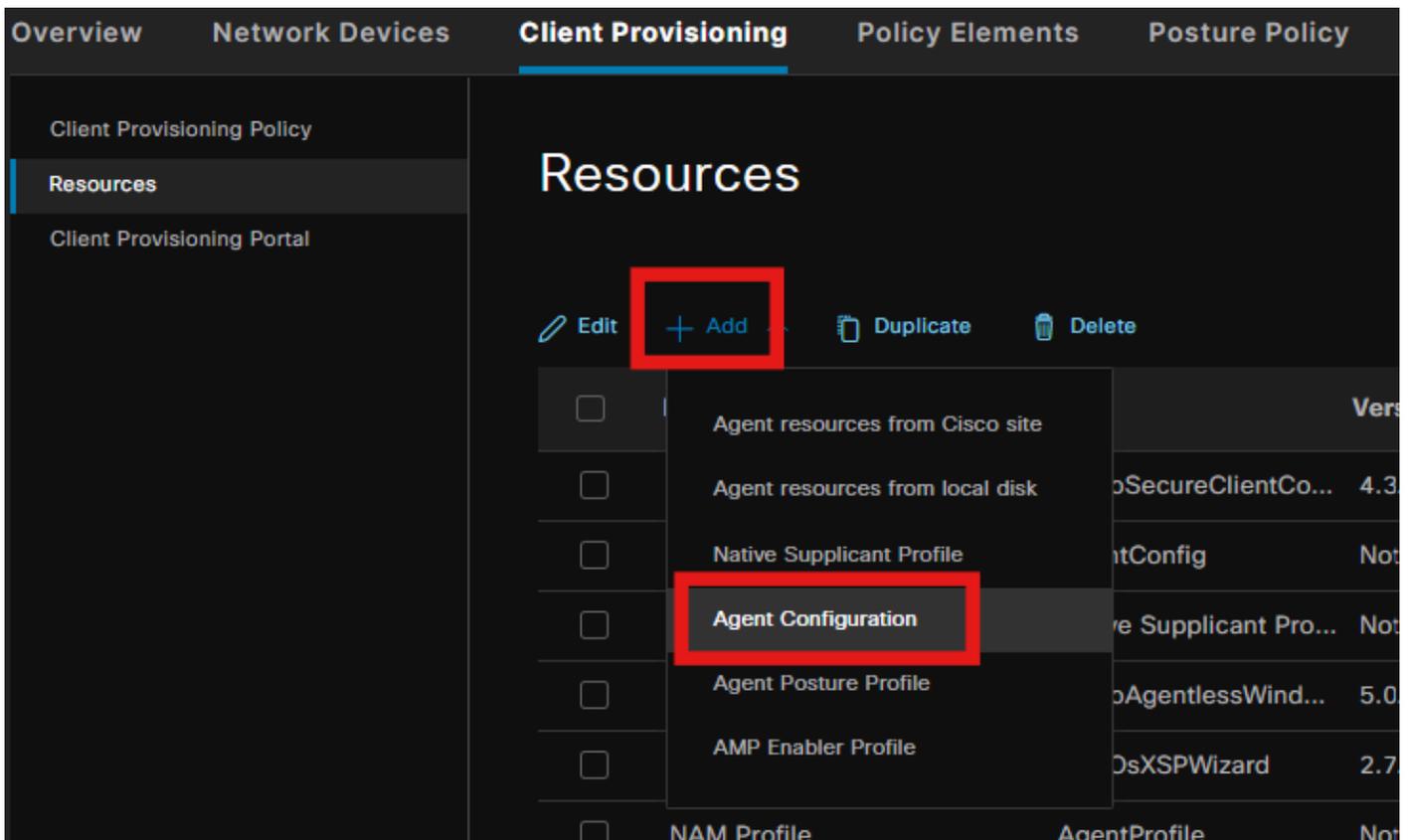
- Category:** A dropdown menu set to 'Customer Created Packs'.
- Type:** A dropdown menu set to 'Agent Profile'.
- * Name:** A text input field containing 'New Profile'.
- Description:** An empty text input field.
- File Selection:** A 'Choose File' button next to the filename 'configuration.xml'.
- Buttons:** A blue 'Submit' button and a grey 'Cancel' button.

Étape 4. Créer un profil de posture



Dans la section Protocole de posture, n'oubliez pas d'ajouter * afin de permettre à l'agent de se connecter à tous les serveurs.

Étape 5. Créer une configuration d'agent



Sélectionnez le package client sécurisé et module de conformité téléchargé et, sous Module selection, sélectionnez les modules ISE Posture, NAM et DART

Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets

Client Provisioning Policy
Resources
Client Provisioning Portal

[Agent Configuration](#) > **New Agent Configuration**

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 ▾

* Configuration Name:

Description:

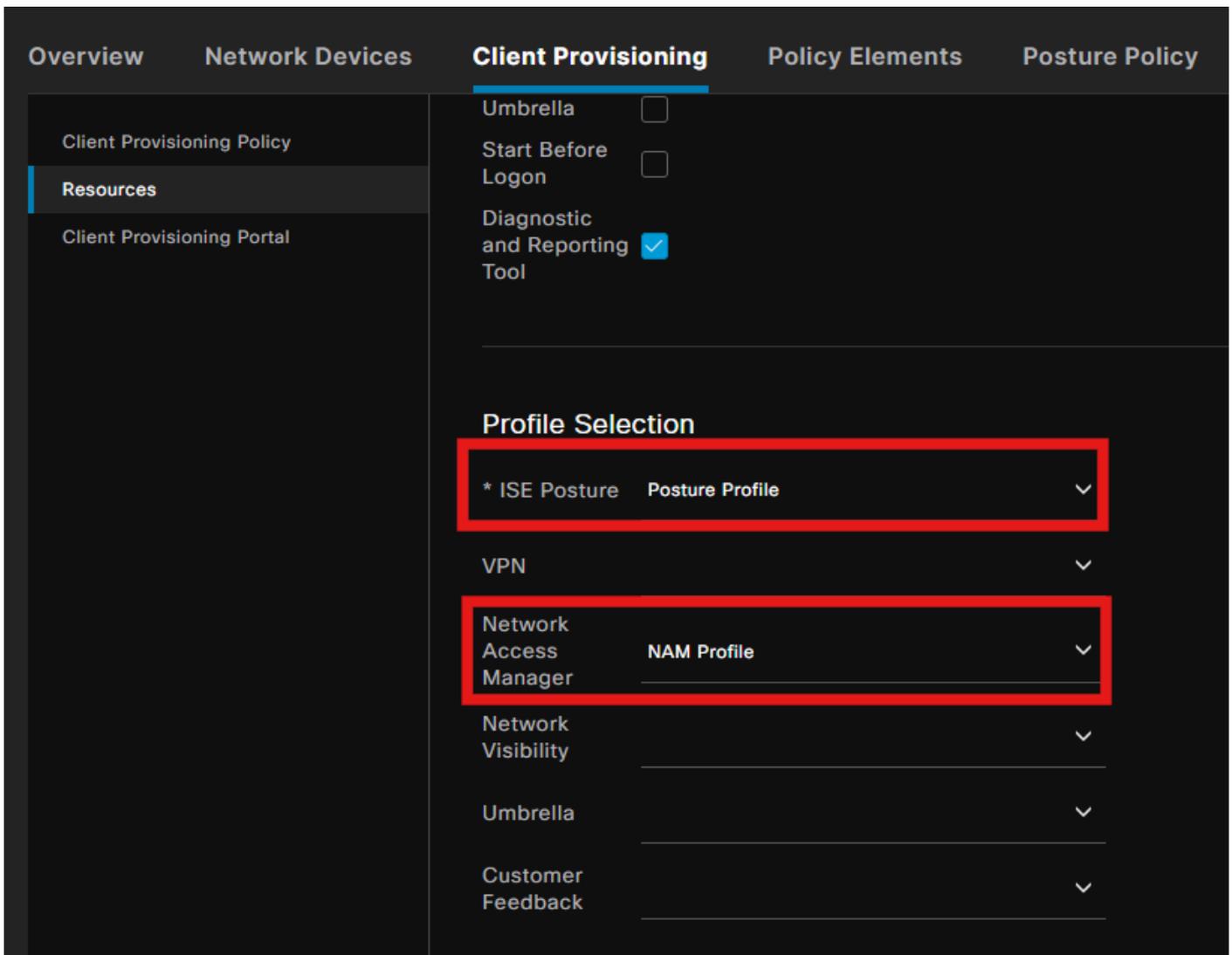
Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleW ▾

Cisco Secure Client Module Selection

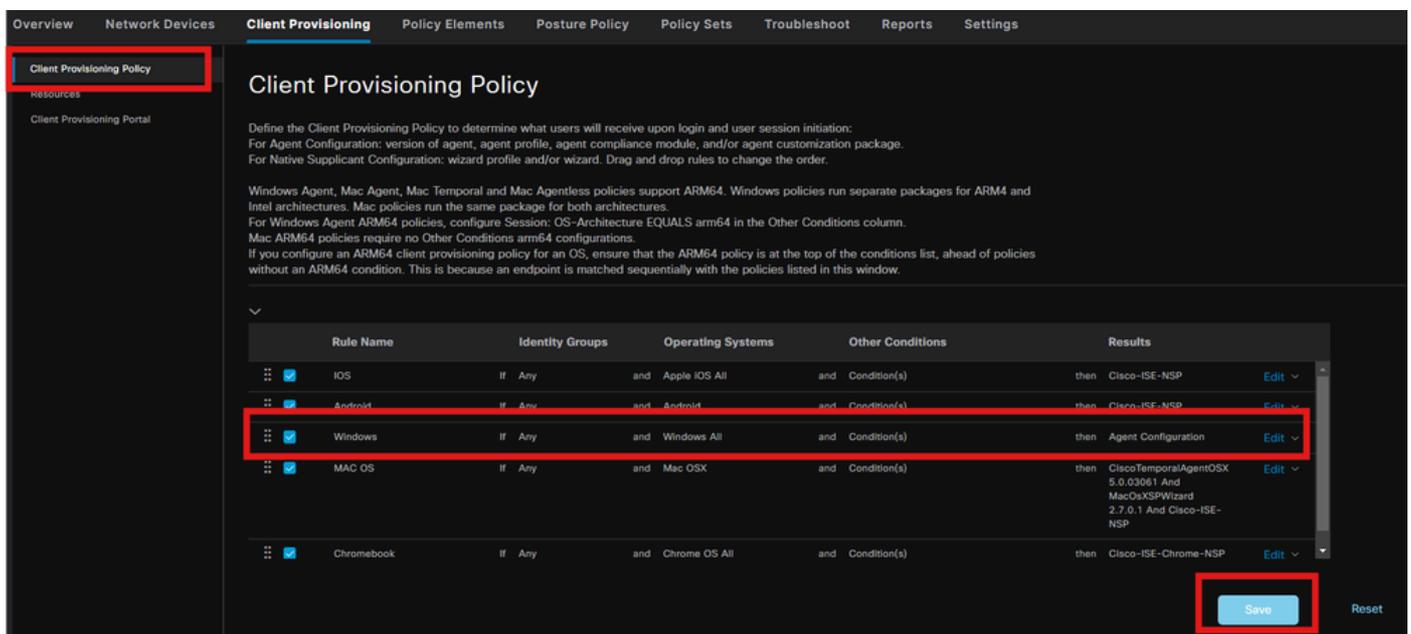
ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input checked="" type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>

Sous Profile select, choisissez la Posture et le profil NAM, puis cliquez sur Submit.



Étape 6. Politique de provisionnement client

Créez une stratégie d'approvisionnement de client pour le système d'exploitation Windows et sélectionnez la configuration de l'agent créée à l'étape précédente.

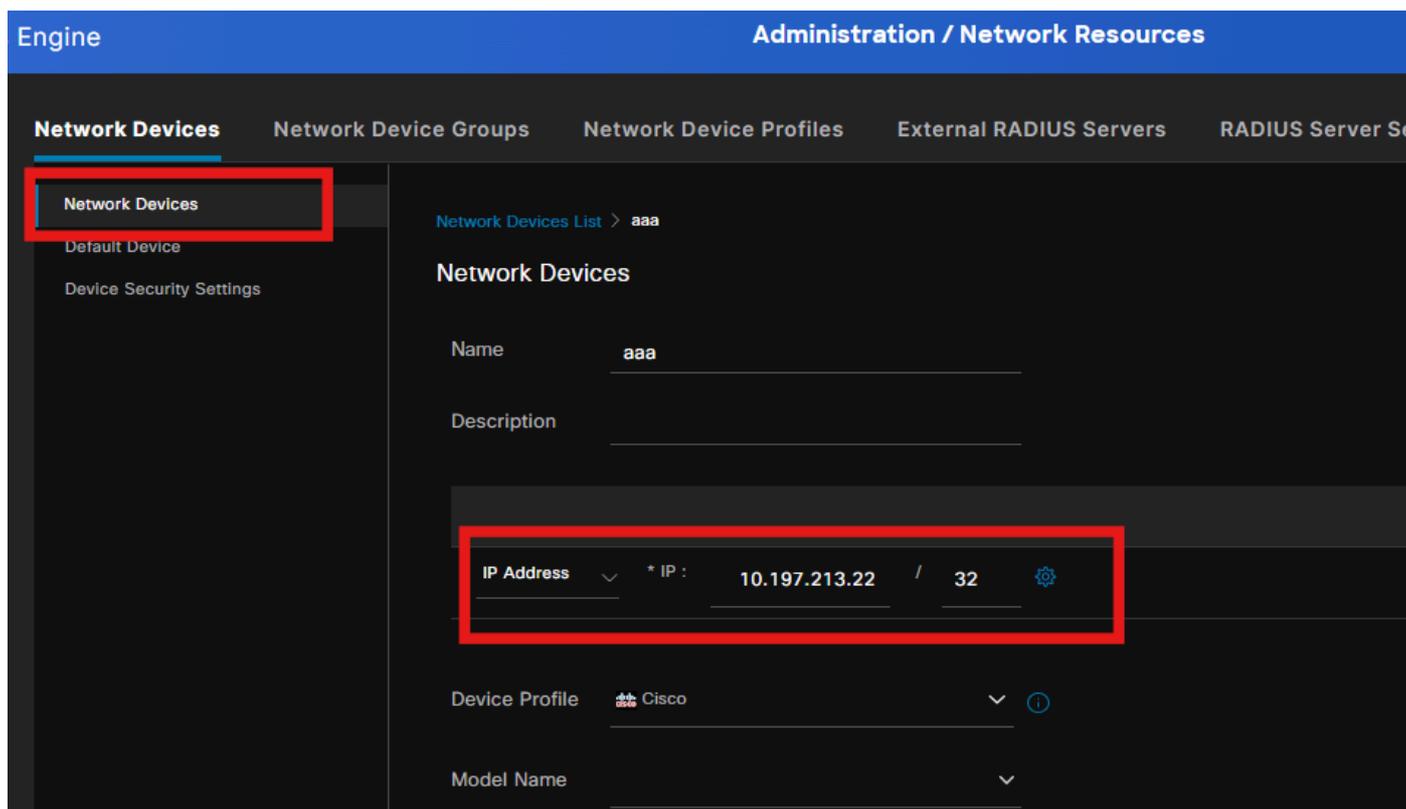


Étape 7. Politique de posture

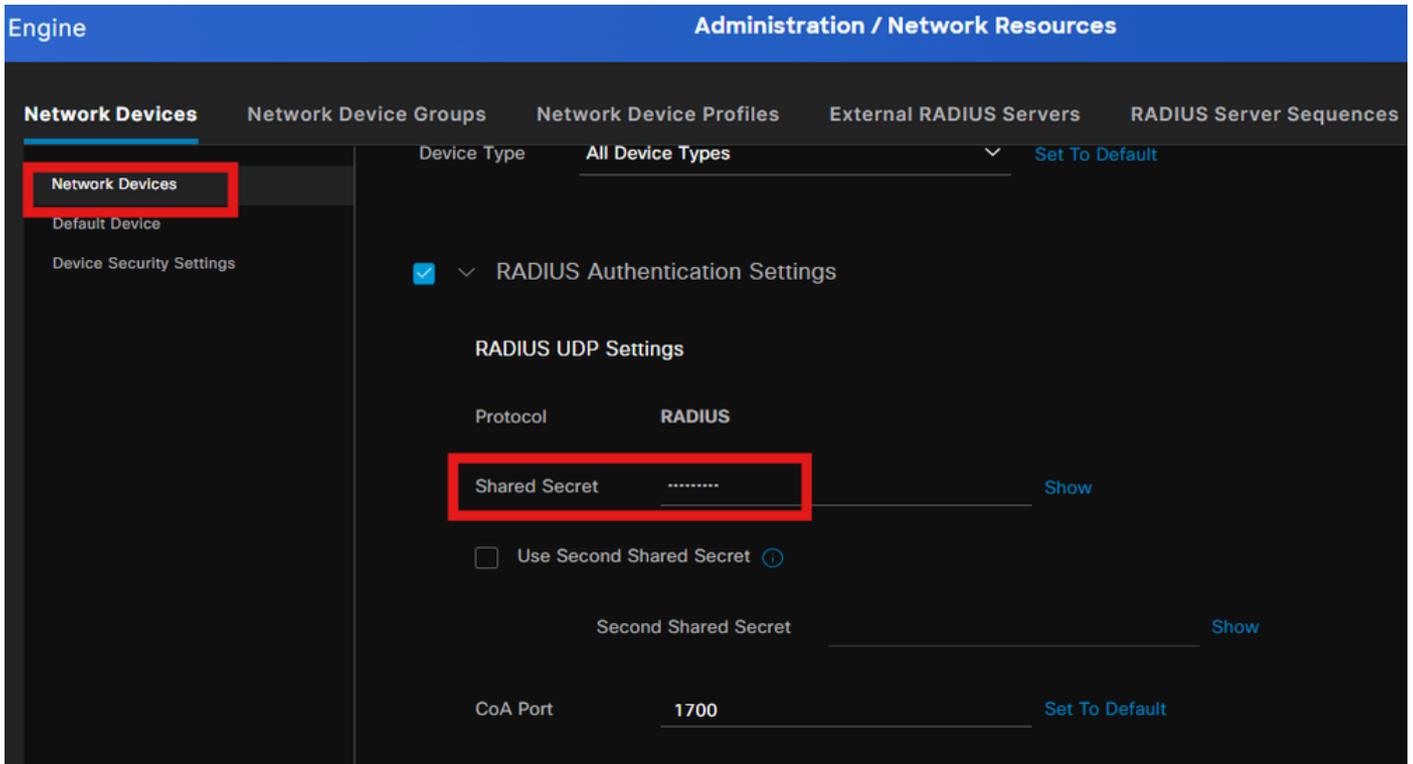
Pour plus d'informations sur la façon de créer la politique de posture et les conditions, référez-vous à ce guide [Guide de déploiement prescriptif de posture ISE](#) .

Étape 8. Ajouter un périphérique réseau

Pour ajouter l'adresse IP du commutateur et la clé secrète partagée radius, accédez à Administration > Network Resources.

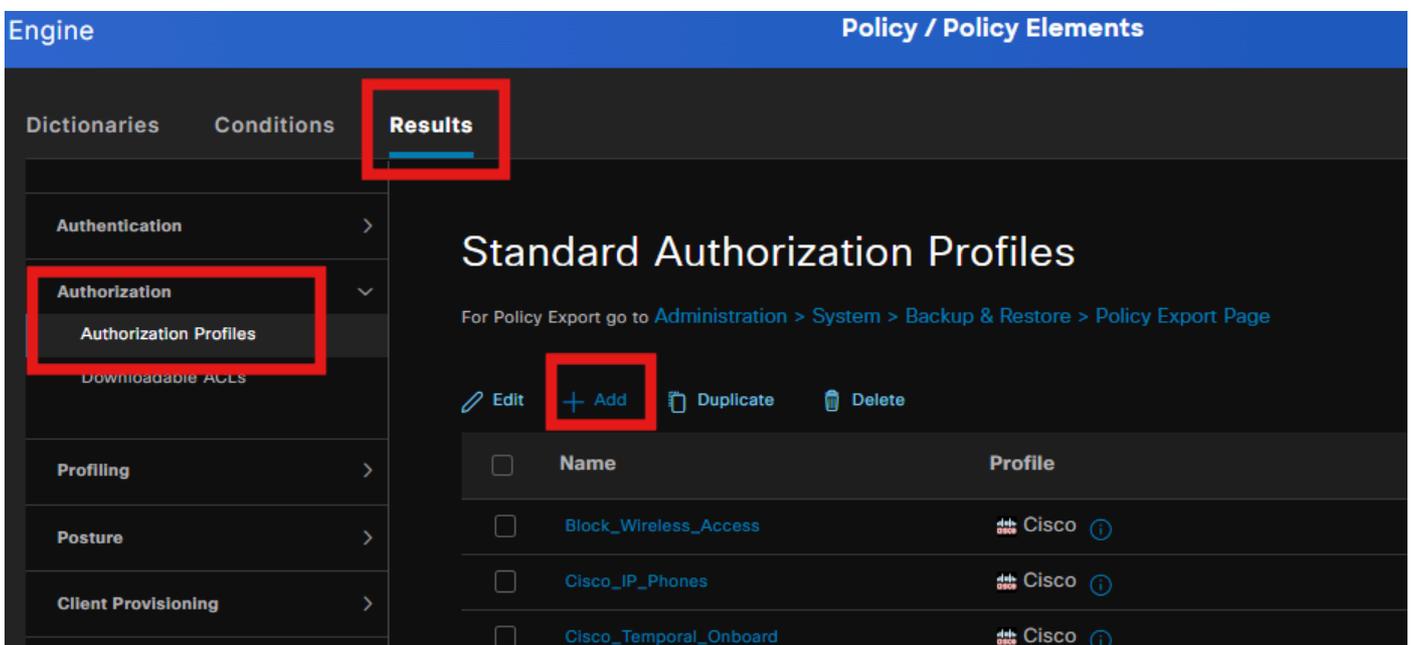


The screenshot displays the Cisco ISE Administration interface. The top navigation bar shows 'Engine' on the left and 'Administration / Network Resources' on the right. Below this, a horizontal menu contains 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', and 'RADIUS Server Se'. The 'Network Devices' menu item is highlighted with a red box. The main content area shows the configuration for a device named 'aaa'. The 'Name' field is set to 'aaa'. Below it is a 'Description' field. A red box highlights the 'IP Address' field, which is set to '10.197.213.22 / 32'. Below the IP address field is the 'Device Profile' dropdown menu, which is set to 'Cisco'. At the bottom, the 'Model Name' field is visible but empty.

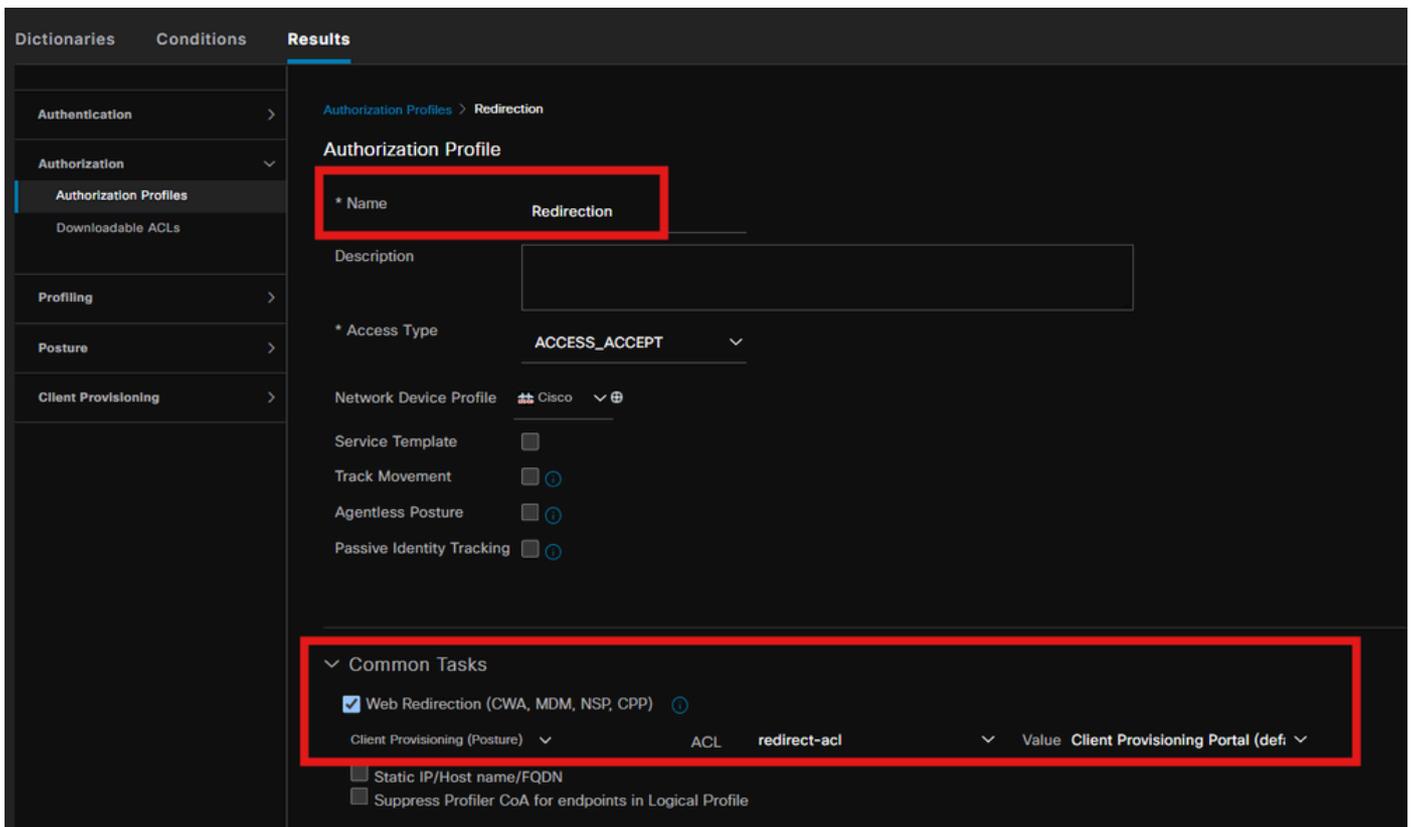


Étape 9. Profil d'autorisation

Pour créer un profil de redirection de position, accédez à Stratégie > Éléments de stratégie > Résultats.

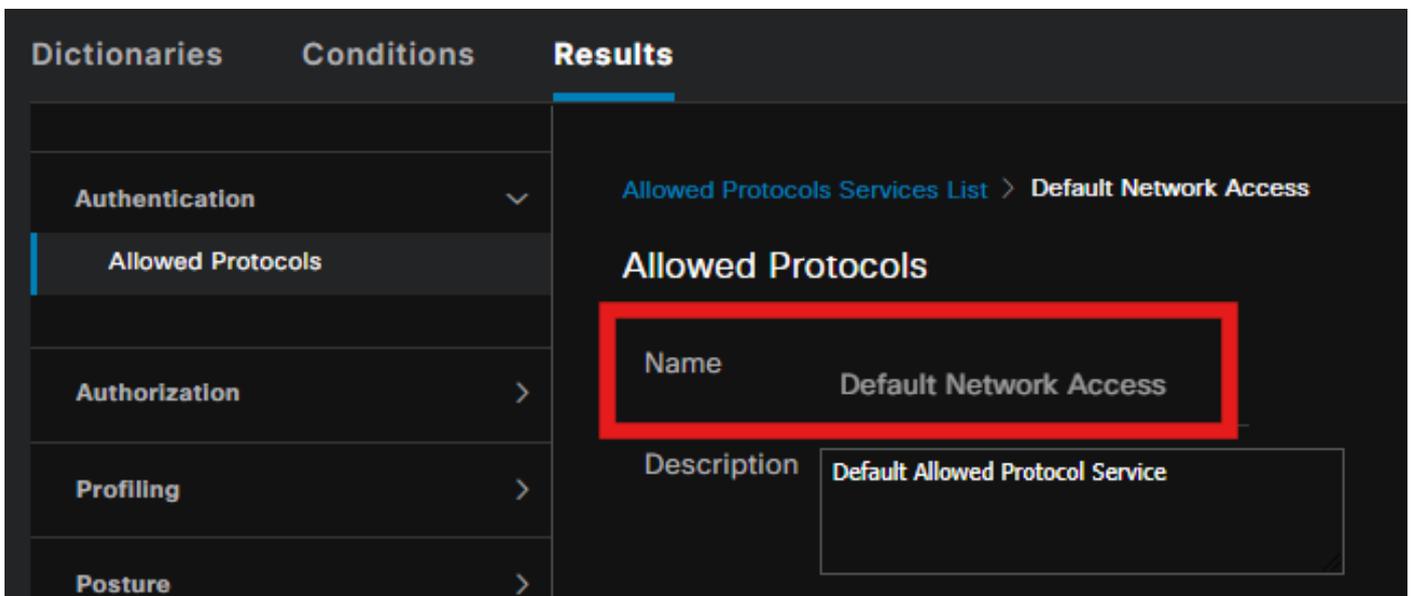


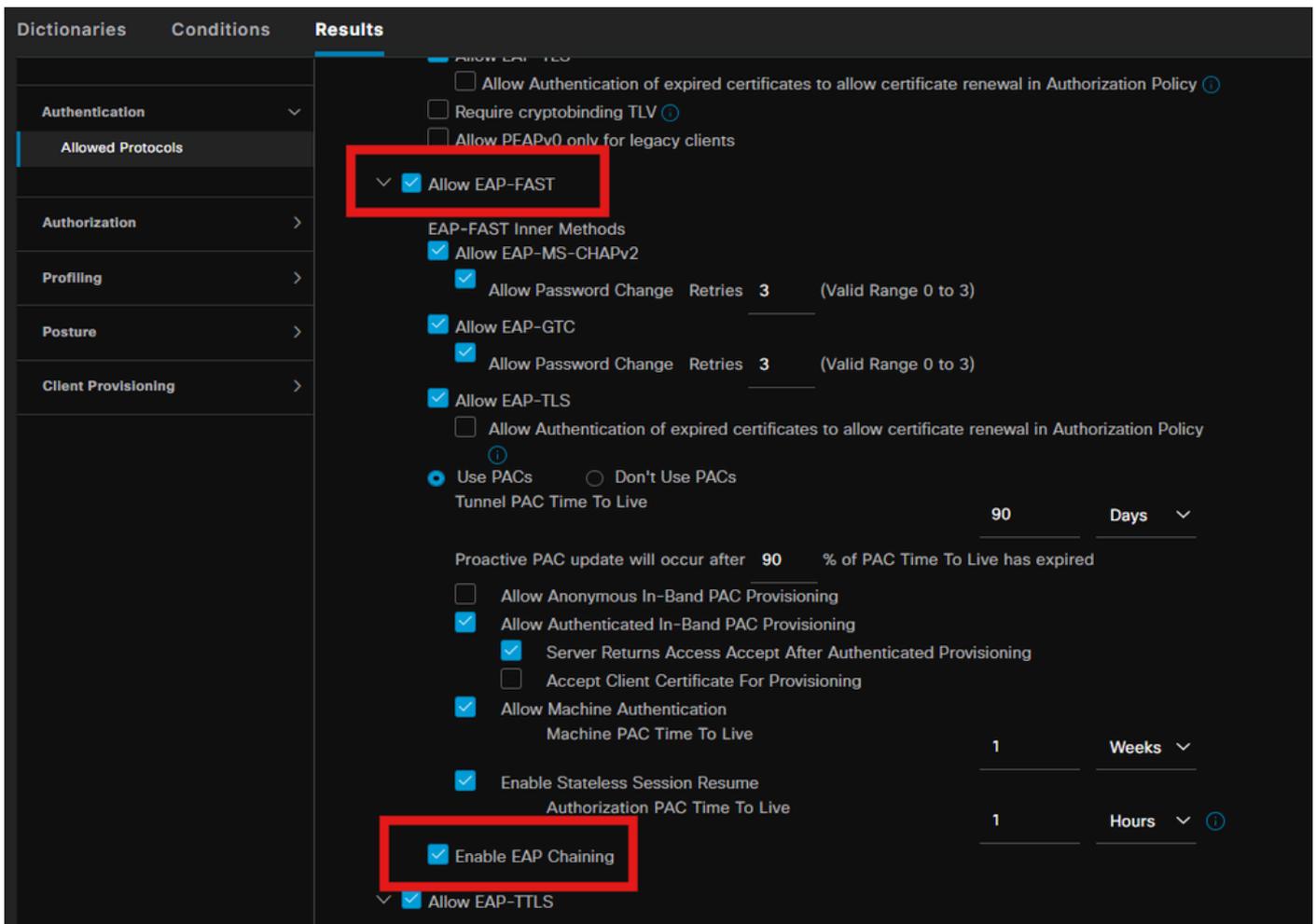
Sous tâche de commande, sélectionnez le client Provisioning Portal avec ACL de redirection.



Étape 10. Protocoles autorisés

Accédez à Policy > Policy elements > Results > Authentication > Allowed Protocols, sélectionnez les paramètres de chaînage EAP,

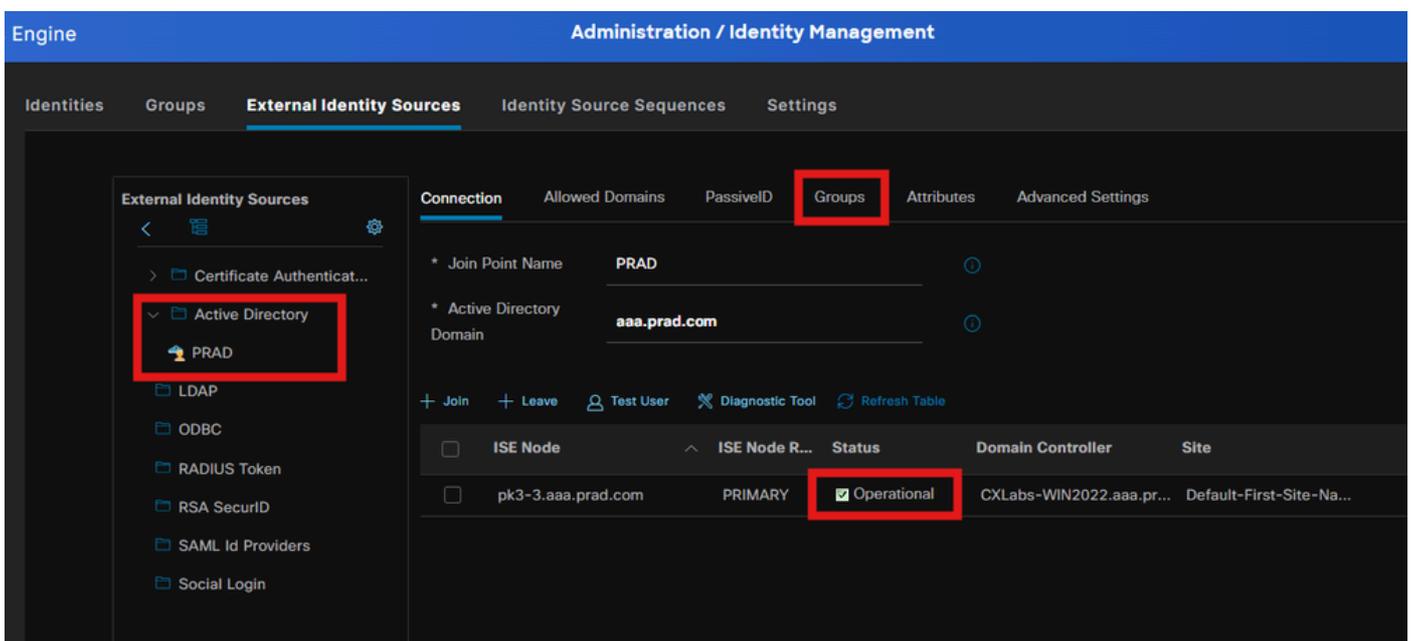




Étape 11. Active Directory

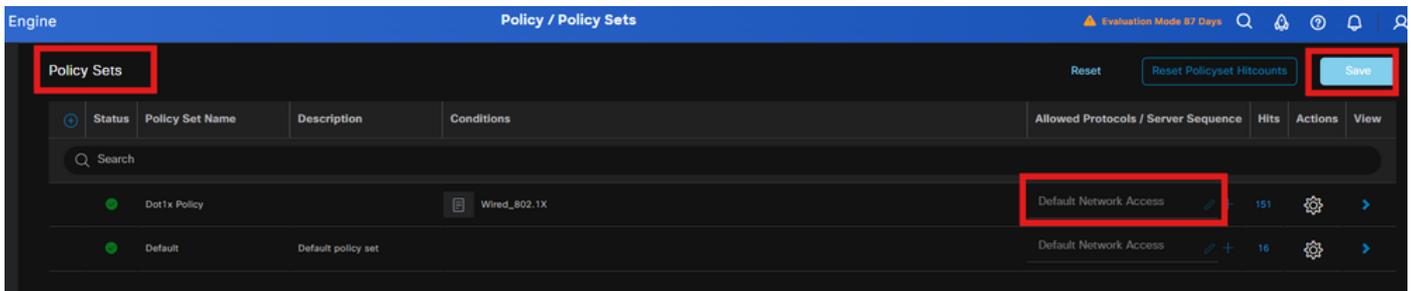
Valider ISE est joint au domaine Active Directory et les groupes de domaines sont sélectionnés si nécessaire pour les conditions d'autorisation.

Administration > Gestion des identités > Sources d'identités externes > Active Directory

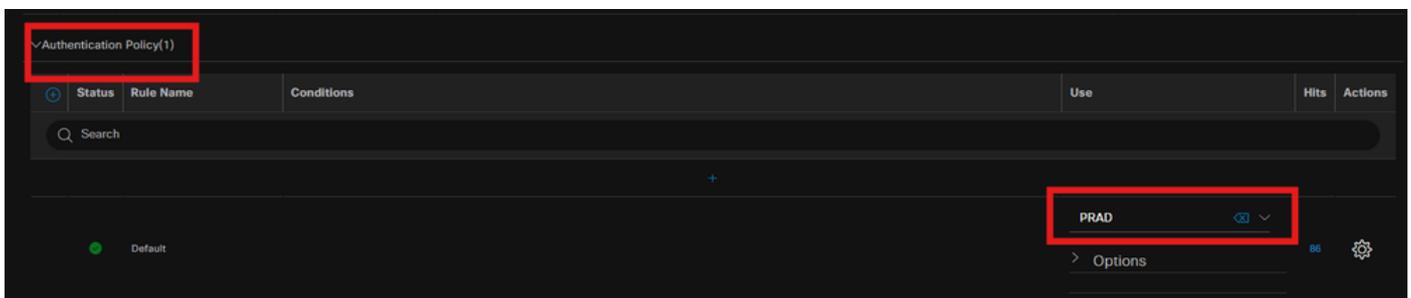


Étape 12. Ensembles de stratégies

Créez un ensemble de stratégies sur ISE pour authentifier la requête dot1x. Rendez-vous à Policy > Policy Sets (Politique > Ensembles de politiques).



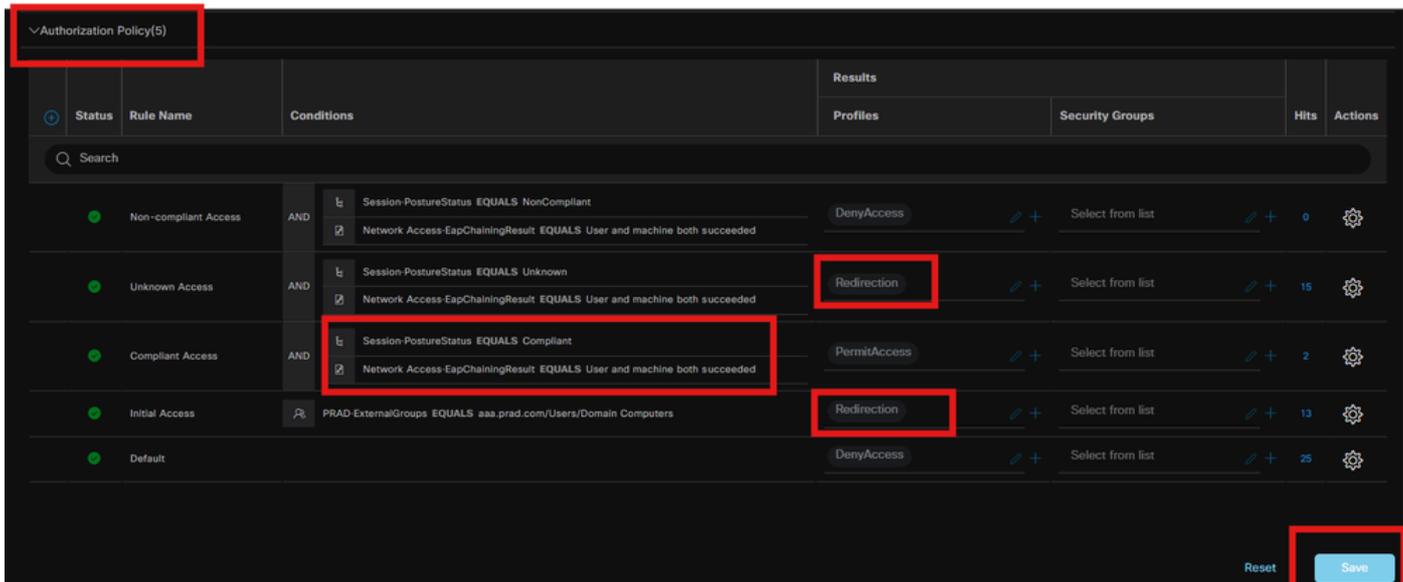
Sélectionnez Active Directory comme source d'identité pour la stratégie d'authentification.



Configurez différentes règles d'autorisation en fonction de l'état de position inconnu, non conforme et conforme.

Dans ce cas d'utilisation.

- Accès initial : redirection vers le portail d'approvisionnement du client ISE pour installer l'agent client sécurisé et le profil NAM
- Accès inconnu : accès au portail d'approvisionnement client pour la détection de posture basée sur la redirection
- Accès conforme : accès complet au réseau
- Non conforme : Refuser l'accès



Vérifier

Étape 1. Téléchargez et installez le module Secure Client Posture/NAM depuis ISE

Sélectionnez le point de terminaison authentifié via dot1x, en appuyant sur la règle d'autorisation "Accès initial". Accédez à Operations > Radius > Live Logs

Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:10:17...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:10:17...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
Jul 27, 2024 12:09:31...	●	🔒	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a...	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Sur le commutateur, spécifiez l'URL de redirection et la liste de contrôle d'accès appliquée au point de terminaison.

```
Switch#show authentication session interface te1/0/24 details
Interface : TenGigabitEthernet1/0/24
IIF-ID : 0x19262768
Adresse MAC : x4x6.xxxx.xxxx
Adresse IPv6 : inconnue
Adresse IPv4 : <client-IP>
Nom d'utilisateur : host/DESKTOP-xxxxxx.aaa.prad.com
État : autorisé
Domaine : DONNÉES
Mode par hôte : hôte unique
Oper control dir : les deux
Délai d'expiration de session : N/A
ID de session commun : 16D5C50A0000002CF067366B
ID de session de compte : 0x0000001f
```

Poignée : 0x7a000017

Politique actuelle : POLICY_Te1/0/24

Stratégies locales :

Modèle de service : DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priorité 150)

Stratégie de sécurité : devrait sécuriser

État de sécurité : liaison non sécurisée

Stratégies de serveur :

URL Redirect ACL : redirect-acl

Redirection d'URL :

<https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee397180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2>

ACS ACL : xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Liste d'état de méthode :

Etat de méthode

dot1x Authc Success

Switch#sh interface de base de données de suivi des périphériques te1/0/24

Adresse de la couche réseau Adresse de la couche liaison Interface vlan prlvl age state Temps restant
ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn REACHABLE 39 s try 0

Sur le point de terminaison, vérifiez le trafic redirigé vers la posture ISE et cliquez sur Démarrer pour télécharger l'assistant de configuration réseau sur le point de terminaison.

Google Chrome isn't your default browser

Set as default



Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Start

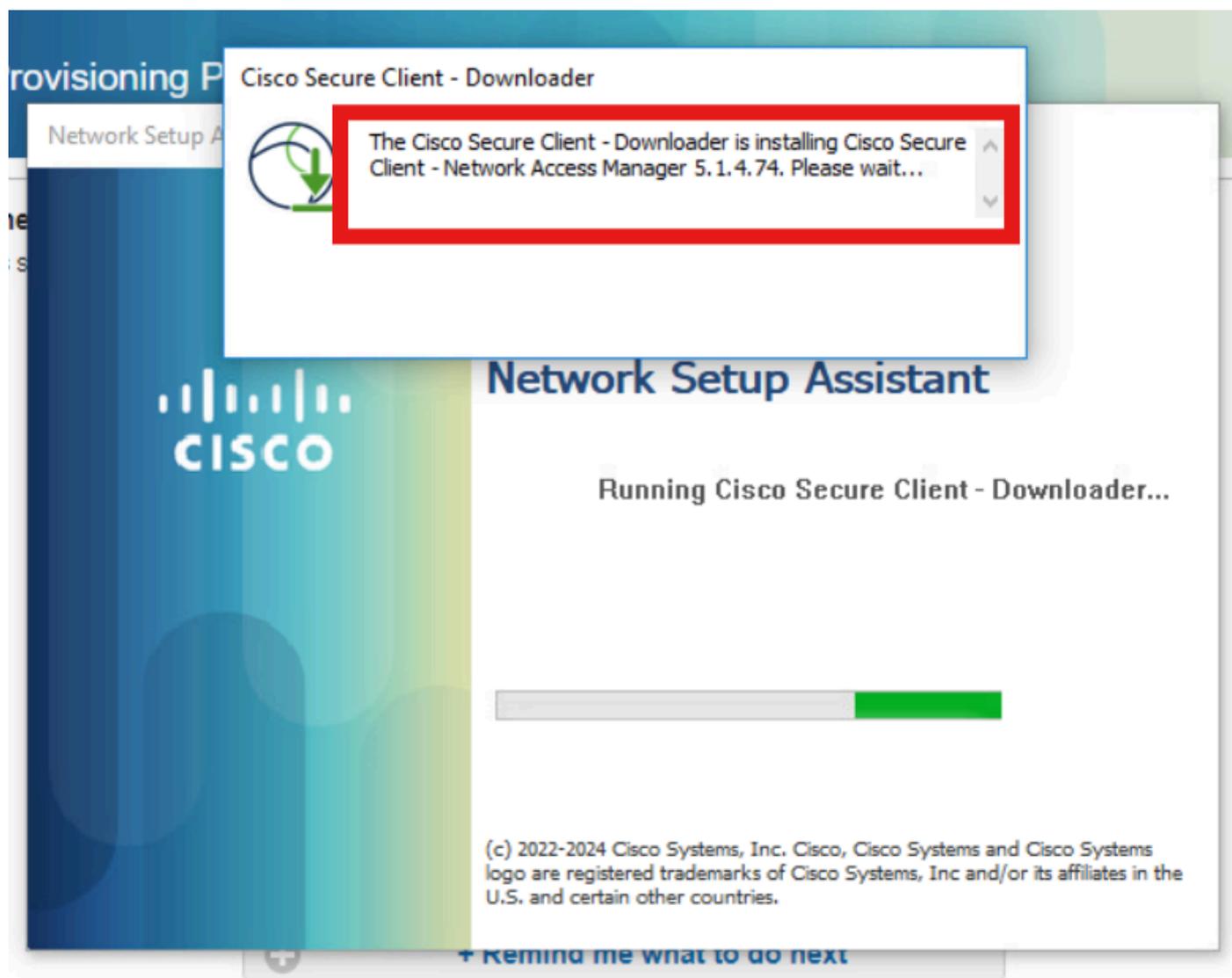
The screenshot shows the Cisco Client Provisioning Portal interface. At the top left is the 'SCO Client Provisioning Portal' header. Below it is a 'Device Security Check' section with the text: 'Your computer requires security software to be installed before you can connect to the network.' A central message box titled 'Unable to detect Posture Agent' contains the following text: '+ This is my first time here', '1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)', '2. After installation, Agent will automatically scan your device before allowing you access to the network.', '3. You have 4 minutes to install and for the system scan to complete.', 'Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.', and 'You have 4 minutes to install and for the compliance check to complete'. At the bottom of this message box is a '+ Remind me what to do next' button. In the top right corner, a 'Recent download history' window is open, showing a single entry: 'cisco-secure-client-ise-network-assistant-win-5.1.4.74_pk3-3.aaa.prad.com_8443_WPTsDtDOR0SunsnMYBIglg.exe' with a size of '3.0 MB' and status 'Done'. A 'Full download history' link is also visible.

Cliquez sur Run pour installer l'application NSA.

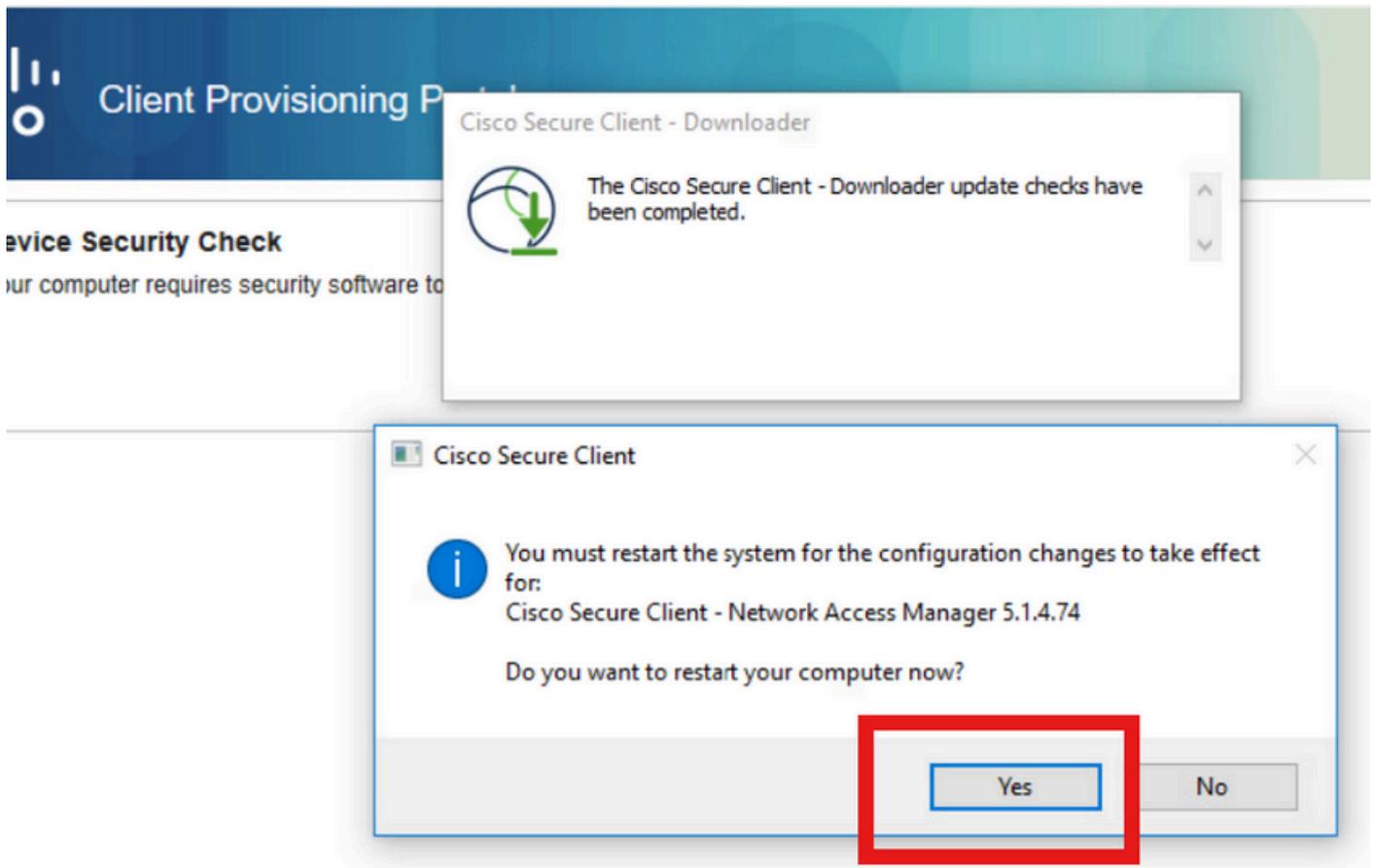
The screenshot shows a Windows SmartScreen warning dialog box overlaid on the Cisco Client Provisioning Portal. The dialog box has a blue background and contains the following text: 'SmartScreen can't be reached right now', 'Check your Internet connection. Windows Defender SmartScreen is unreachable and can't help you decide if this app is ok to run.', 'Publisher: Cisco Systems, Inc.', and 'App: cisco-secure-client-ise-network-assistant-win-5.1.4.74_pk3-...'. At the bottom of the dialog box, there are two buttons: 'Run' and 'Don't Run'. The 'Run' button is highlighted with a red dashed border.

Maintenant, la NSA appelle le téléchargement de Secure Client Agent à partir d'ISE et installe la

posture, le module NAM et le profil NAM configuration.xml .



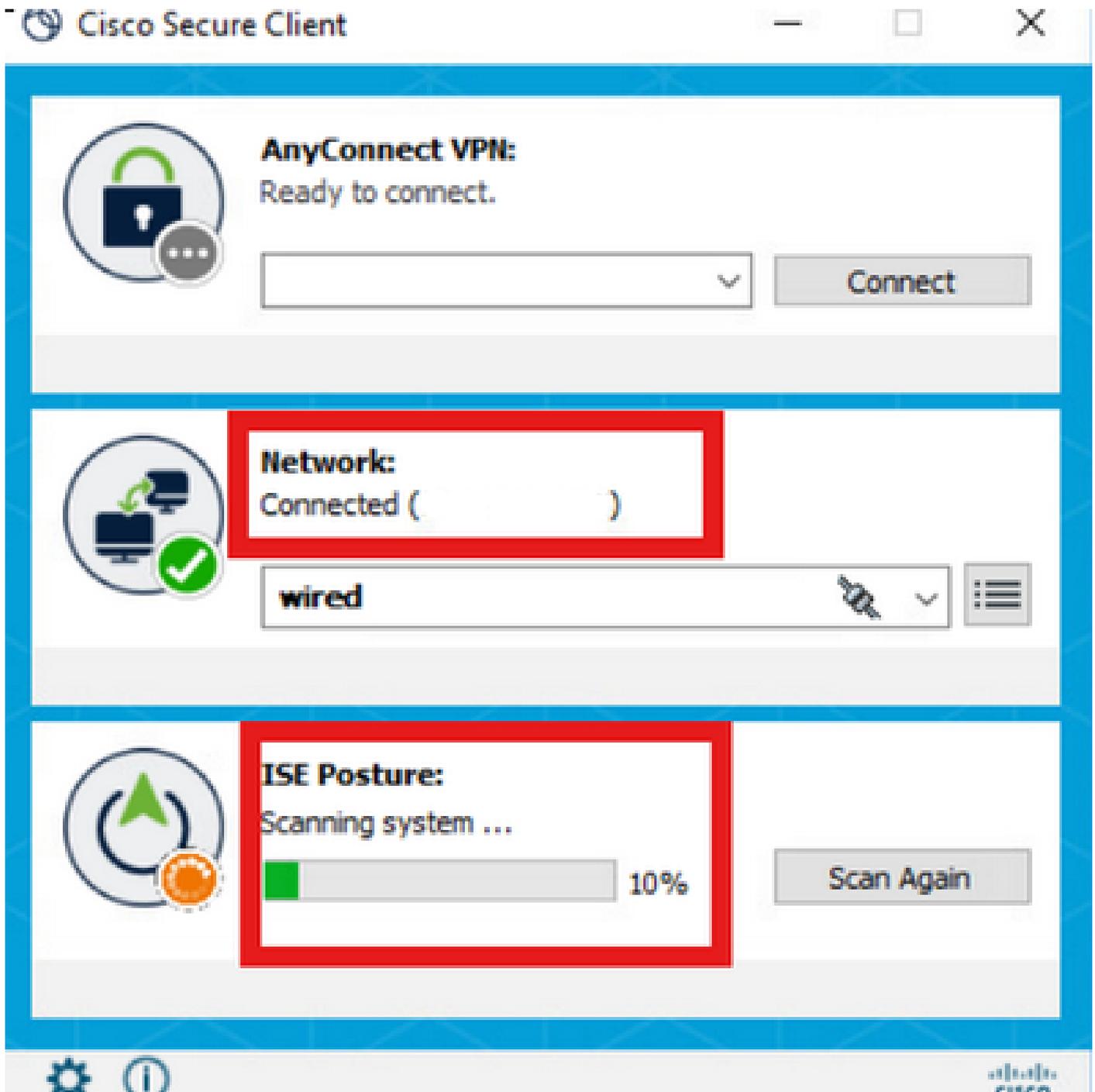
Une invite de redémarrage se déclenche après l'installation de NAM. Cliquez sur Yes.



Étape 2. EAP-FAST

Une fois que le PC a redémarré et que l'utilisateur s'est connecté, le NAM authentifie l'utilisateur et la machine via EAP-FAST.

Si le point d'extrémité s'authentifie correctement, NAM indique qu'il est connecté et le module Posture déclenche le balayage de posture.



Dans les journaux en direct ISE, le point de terminaison applique désormais la règle d'accès inconnu.

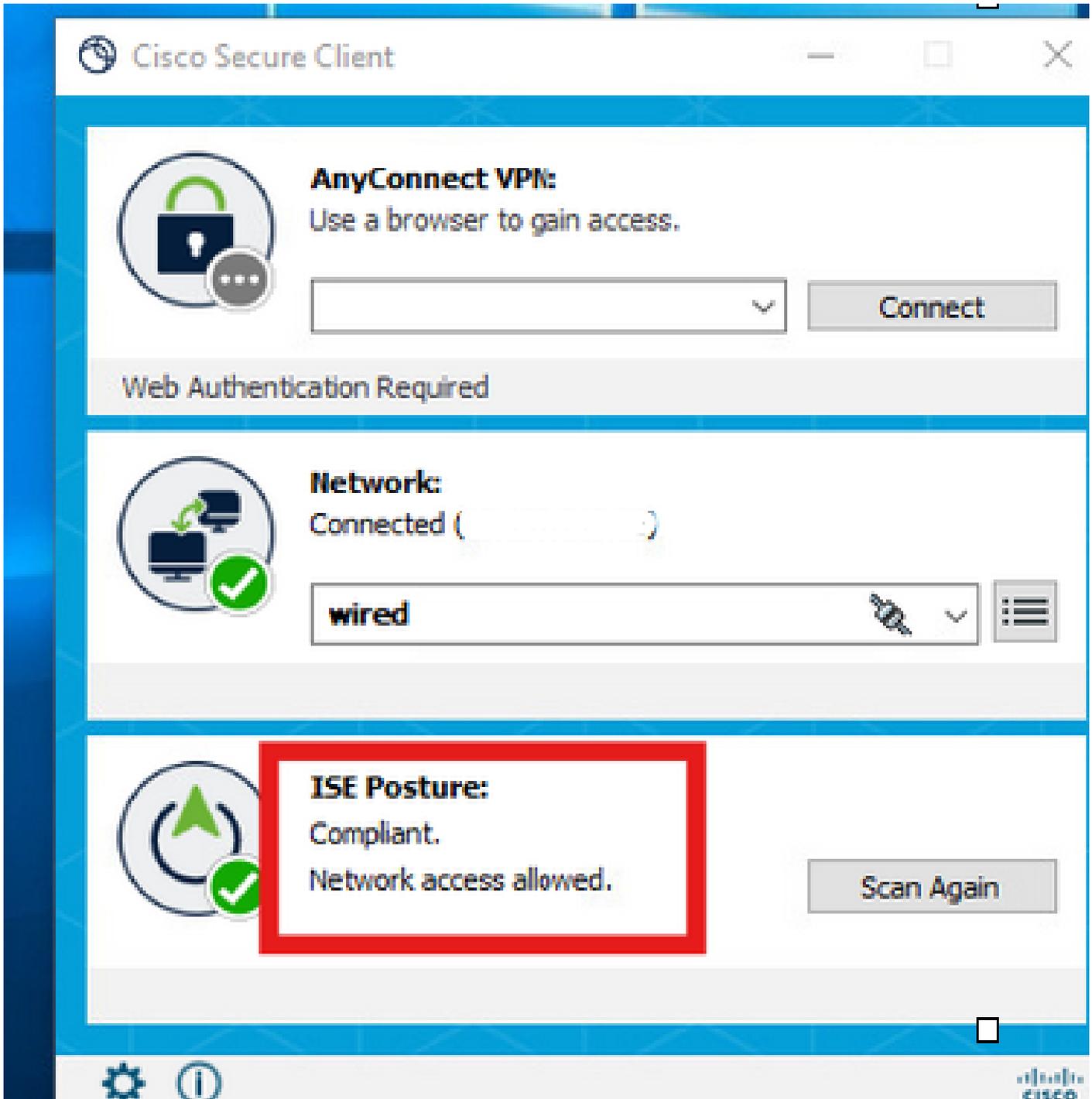
Jul 27, 2024 12:29:06...	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48...	host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Maintenant, le protocole d'authentification est EAP-FAST basé sur la configuration du profil NAM et le résultat du chaînage EAP est "Success".

AcsSessionID	pk3-3/511201330/230
NACRadiusUserName	user1
NACRadiusUserName	host/DESKTOP-QSCE4P3
SelectedAuthenticationIden...	PRAD
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatched...	Unknown Access
IssuedPacInfo	Issued PAC type=Machine Authorization with expiration time: Sat Jul 27 01:29:06 2024
EndPointMACAddress	[REDACTED]
EapChainingResult	User and machine both succeeded
ISEPolicySetName	Dot1x Policy
IdentitySelectionMatchedRule	Default
AD-User-Resolved-Identities	user1@aaa.prad.com
AD-User-Candidate-Identities	user1@aaa.prad.com
AD-Host-Resolved-Identities	DESKTOP-QSCE4P3\$@aaa.prad.com
AD-Host-Candidate-Identities	DESKTOP-QSCE4P3\$@aaa.prad.com

Étape 3. Balayage De Posture

Le module Secure Client Posture déclenche le scan de posture et est marqué comme Plainte en fonction de la stratégie de posture ISE.



Le CoA est déclenché après le scan de posture et maintenant le point d'extrémité atteint la stratégie d'accès aux plaintes.

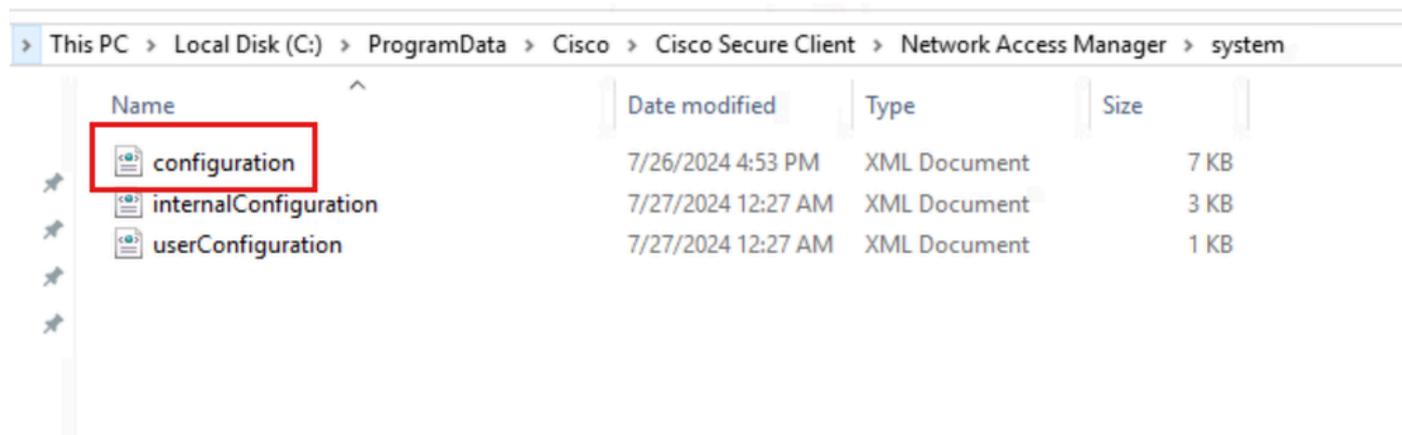
Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Jul 27, 2024 12:29:32...			B4:96:91:F9:56:8B	user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:32...				user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant
Jul 27, 2024 12:29:31...								Compliant
Jul 27, 2024 12:29:06...				user1_host/DESKTOP-QSC...	Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection	Pending
Jul 27, 2024 12:28:48...				host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

Dépannage

Étape 1. Profil NAM

Vérifiez que le fichier configuration.xml du profil NAM est présent dans ce chemin d'accès sur le PC après l'installation du module NAM.

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

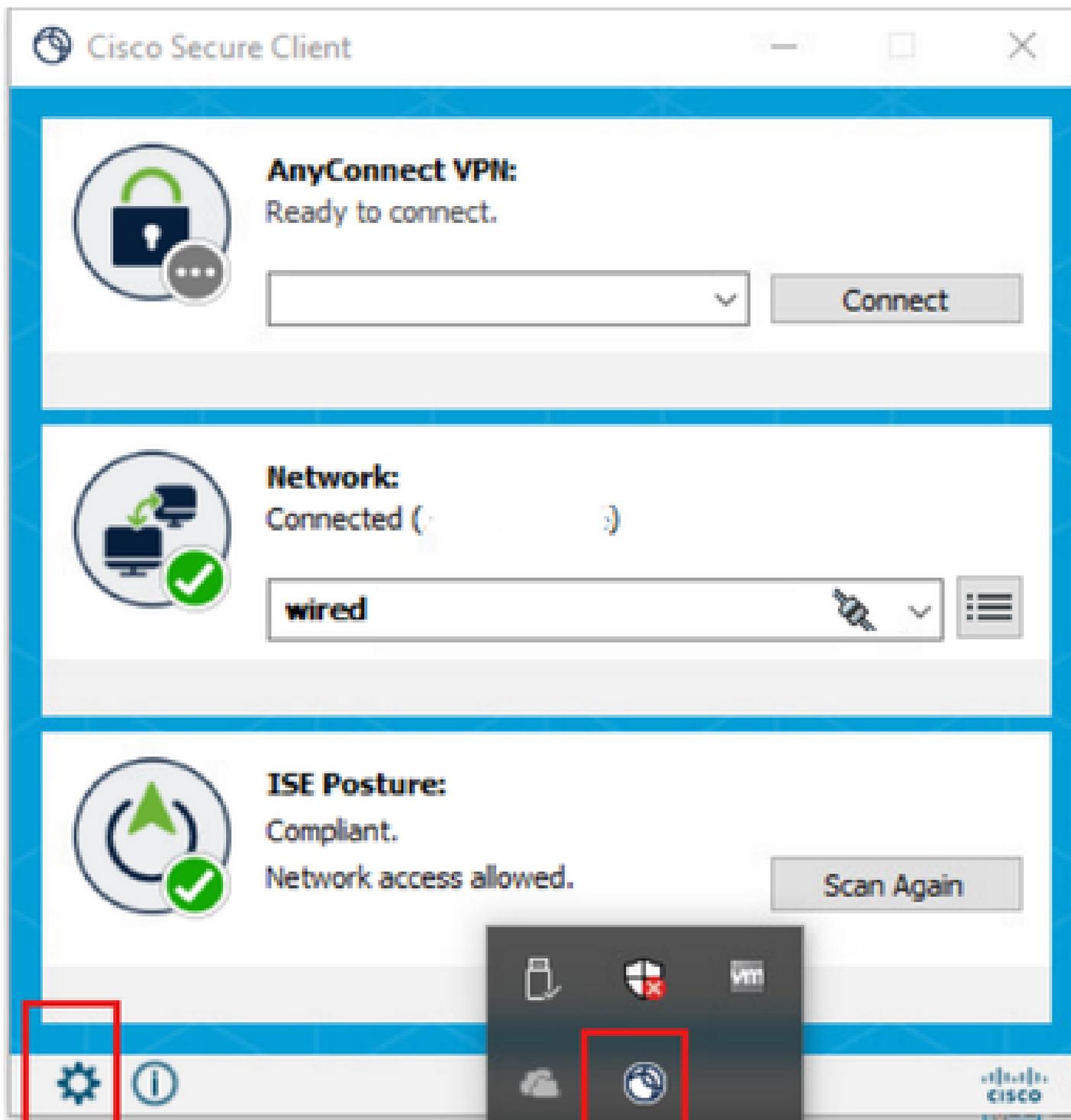


The screenshot shows a Windows File Explorer window with the address bar displaying the path: > This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > Network Access Manager > system. The main area shows a list of files with columns for Name, Date modified, Type, and Size. The 'configuration' file is highlighted with a red box.

Name	Date modified	Type	Size
configuration	7/26/2024 4:53 PM	XML Document	7 KB
internalConfiguration	7/27/2024 12:27 AM	XML Document	3 KB
userConfiguration	7/27/2024 12:27 AM	XML Document	1 KB

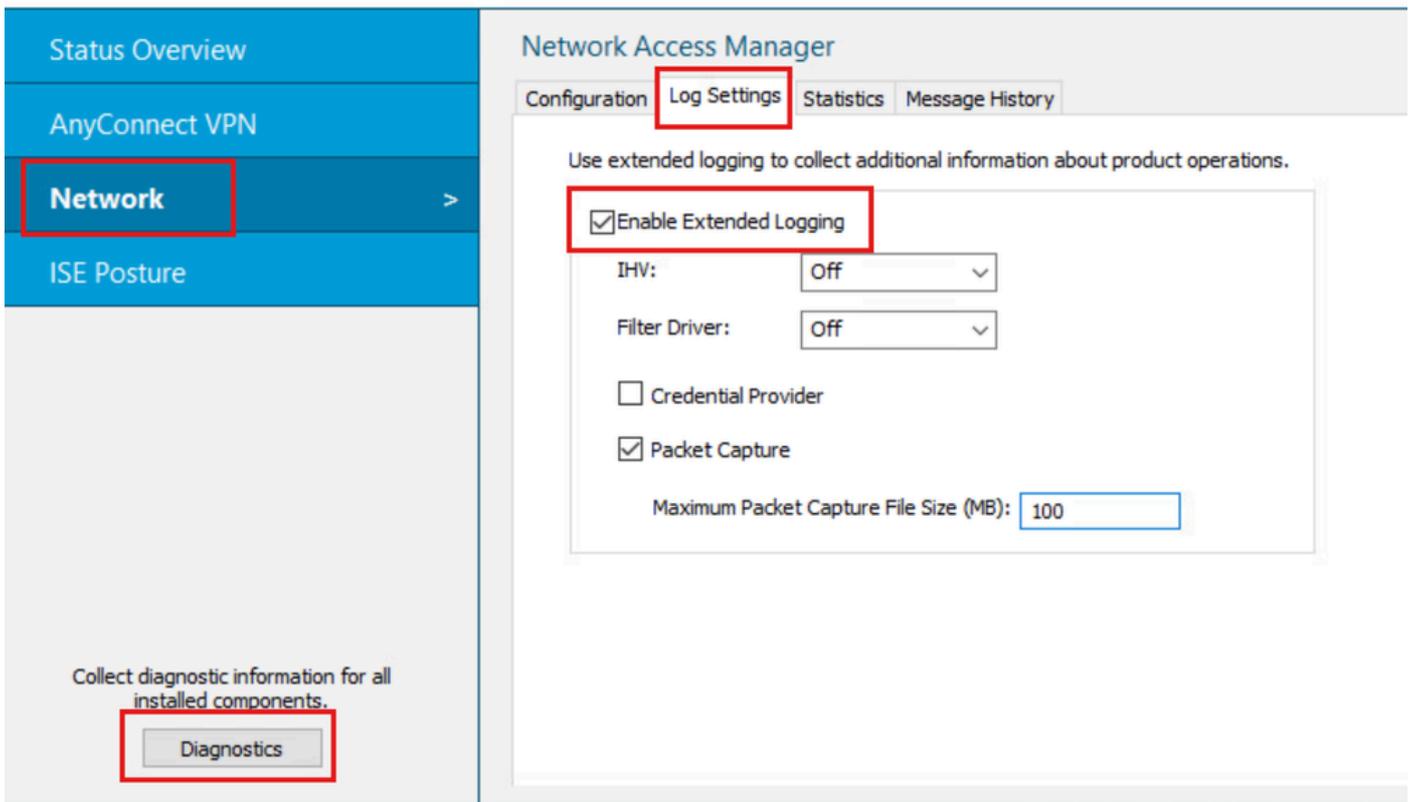
Étape 2. Journalisation étendue NAM

Cliquez sur l'icône Secure Client dans la barre des tâches et sélectionnez l'icône Settings (Paramètres).



Accédez à l'onglet Réseau > Paramètres du journal. Cochez la case Enable Extended Logging. Définissez la taille du fichier de capture de paquets sur 100 Mo.

Après avoir reproduit le problème, cliquez sur Diagnostics pour créer le bundle DART sur le terminal.



La section Historique des messages affiche les détails de chaque étape effectuée par NAM.

Étape 3. Débogages sur le commutateur

Activez ces débogages sur le commutateur pour dépanner dot1x et le flux de redirection.

```
debug ip http all
```

```
debug ip http transactions
```

```
debug ip http url
```

```
set platform software trace smd switch active R0 aaa debug  
set platform software trace smd switch active R0 dot1x-all debug  
set platform software trace smd switch active R0 radius debug  
set platform software trace smd switch active R0 auth-mgr-all debug  
set platform software trace smd switch active R0 eap-all debug  
set platform software trace smd switch active R0 epm-all debug
```

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

```
set platform software trace smd switch active R0 webauth-aaa debug
```

```
set platform software trace smd switch active R0 webauth-httpd debug
```

Pour afficher les journaux

```
show logging
```

```
show logging process smd internal
```

Étape 4. Débogages sur ISE

Collectez le bundle de support ISE avec ces attributs à définir au niveau du débogage :

- posture
- portail
- ravitaillement
- runtime-AAA
- nsf
- nsf-session
- suisse
- client-webapp

Informations connexes

[Configurer le NAM du client sécurisé](#)

[Guide de déploiement prescriptif de la position ISE](#)

[Dépannage de Dot1x sur les commutateurs Catalyst 9000](#)

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.