Configuration du profil NAM du client sécurisé sous Windows à l'aide d'ISE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configuration
  - Diagramme du réseau
  - Flux de données
  - Configurer le commutateur
  - Télécharger le package Secure Client
- 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 la configuration de l'agent
  - Étape 6. Politique de provisionnement du client
  - Étape 7. Politique de posture
  - Étape 8. Ajout d'un périphérique réseau
  - Étape 9. Profil d'autorisation
  - Étape 10. Protocoles autorisés
  - Étape 11. Active Directory
  - Étape 12. Ensembles de politiques
- Validation
  - Étape 1 : téléchargement et installation du module NAM/Secure Client Posture à partir d'ISE
  - Étape 2. EAP-FAST
  - Étape 3. Analyse de la posture
- Dépannage
  - Étape 1. Profil NAM
  - Étape 2. Journalisation étendue du 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).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Politique de posture
- Moteur du service de vérification des identités (ISE)
- AnyConnect NAM et Éditeur de profil
- 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 :

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

---

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

Informations générales

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-

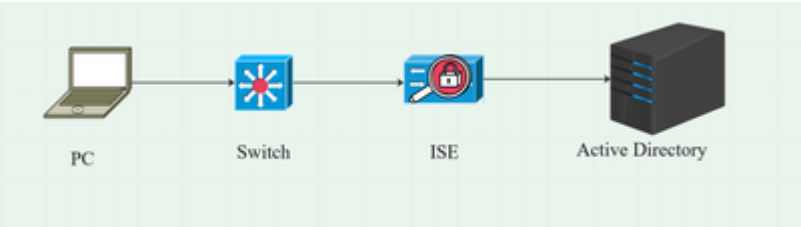
Length-Values (TLV) afin d'établir un tunnel protégé. Ces objets TLV sont utilisés pour transmettre des données liées à l'authentification entre le client et le serveur. Une fois le tunnel établi, la deuxième phase commence avec le client et le noeud ISE qui engagent d'autres conversations pour établir 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 NAM avec vérification 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.

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 l'ordinateur est redirigé vers la page d'approvisionnement 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 le profil Posture et le profil NAM est configuré 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 Redirect pour rediriger les utilisateurs vers le portail d'approvisionnement du client ISE :

```
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 Secure Client

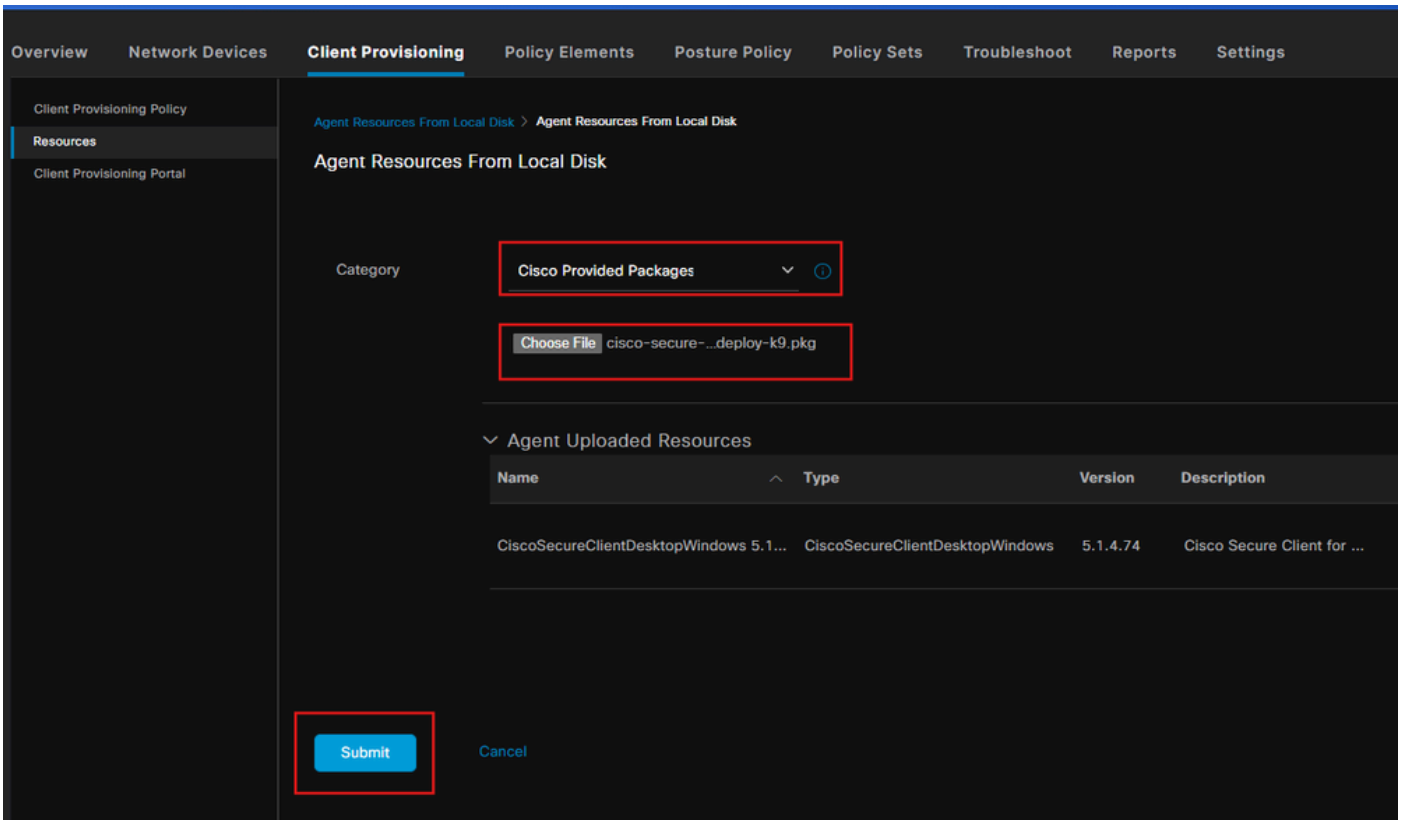
Téléchargez manuellement les fichiers de déploiement Web de l'Éditeur de profil, de Secure Client Windows et du Module de conformité à partir de la page de téléchargement de logiciels Cisco. Dans la barre de recherche du nom du produit, tapez Secure Client 5. Downloads Home > Security > Endpoint Security > Secure Client (y compris AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software

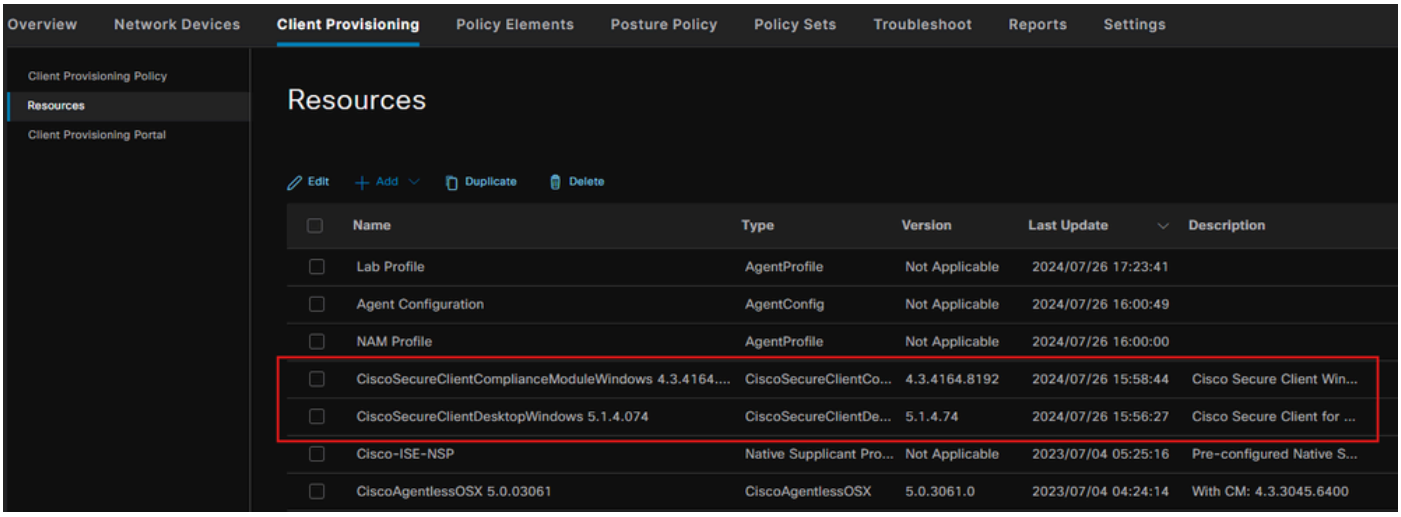
- cisco-secure-client-win-5.1.x-webdeploy-k9.pkg
- cisco-secure-client-win-4.3.x-isecompliance-webdeploy-k9.pkg
- tools-cisco-secure-client-win-5.1.x-profileeditor-k9.msi

Configuration ISE

Étape 1. Télécharger le package sur ISE

1. 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.


Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Client Provisioning Policy
Resources
Client Provisioning Portal
Agent Resources From Local Disk > Agent Resources From Local Disk
Agent Resources From Local Disk
Category
Cisco Provided Packages
Choose File
cisco-secure-...deploy-k9.pkg
Agent Uploaded Resources
Name
Type
Version
Description
CiscoSecureClientDesktopWindows 5.1...
CiscoSecureClientDesktopWindows
5.1.4.74
Cisco Secure Client for ...
Submit
Cancel

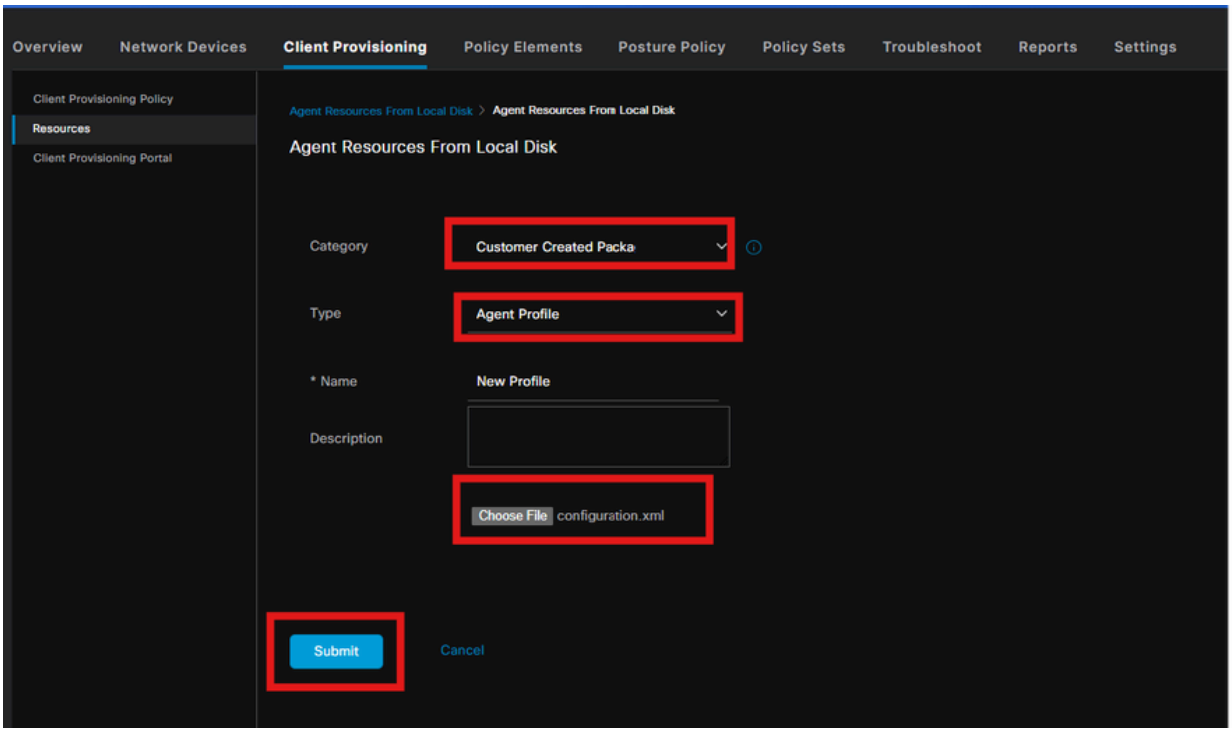

Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Client Provisioning Policy
Resources
Client Provisioning Portal
Resources
Edit
Add
Duplicate
Delete
Name
Type
Version
Last Update
Description
Lab Profile
AgentProfile
Not Applicable
2024/07/26 17:23:41
Agent Configuration
AgentConfig
Not Applicable
2024/07/26 16:00:49
NAM Profile
AgentProfile
Not Applicable
2024/07/26 16:00:00
CiscoSecureClientComplianceModuleWindows 4.3.4164....
CiscoSecureClientCo...
4.3.4164.8192
2024/07/26 15:58:44
Cisco Secure Client Win...
CiscoSecureClientDesktopWindows 5.1.4.074
CiscoSecureClientDe...
5.1.4.74
2024/07/26 15:56:27
Cisco Secure Client for ...
Cisco-ISE-NSP
Native Supplicant Pro...
Not Applicable
2023/07/04 05:25:16
Pre-configured Native S...
CiscoAgentlessOSX 5.0.03061
CiscoAgentlessOSX
5.0.3061.0
2023/07/04 04:24:14
With CM: 4.3.3045.6400

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

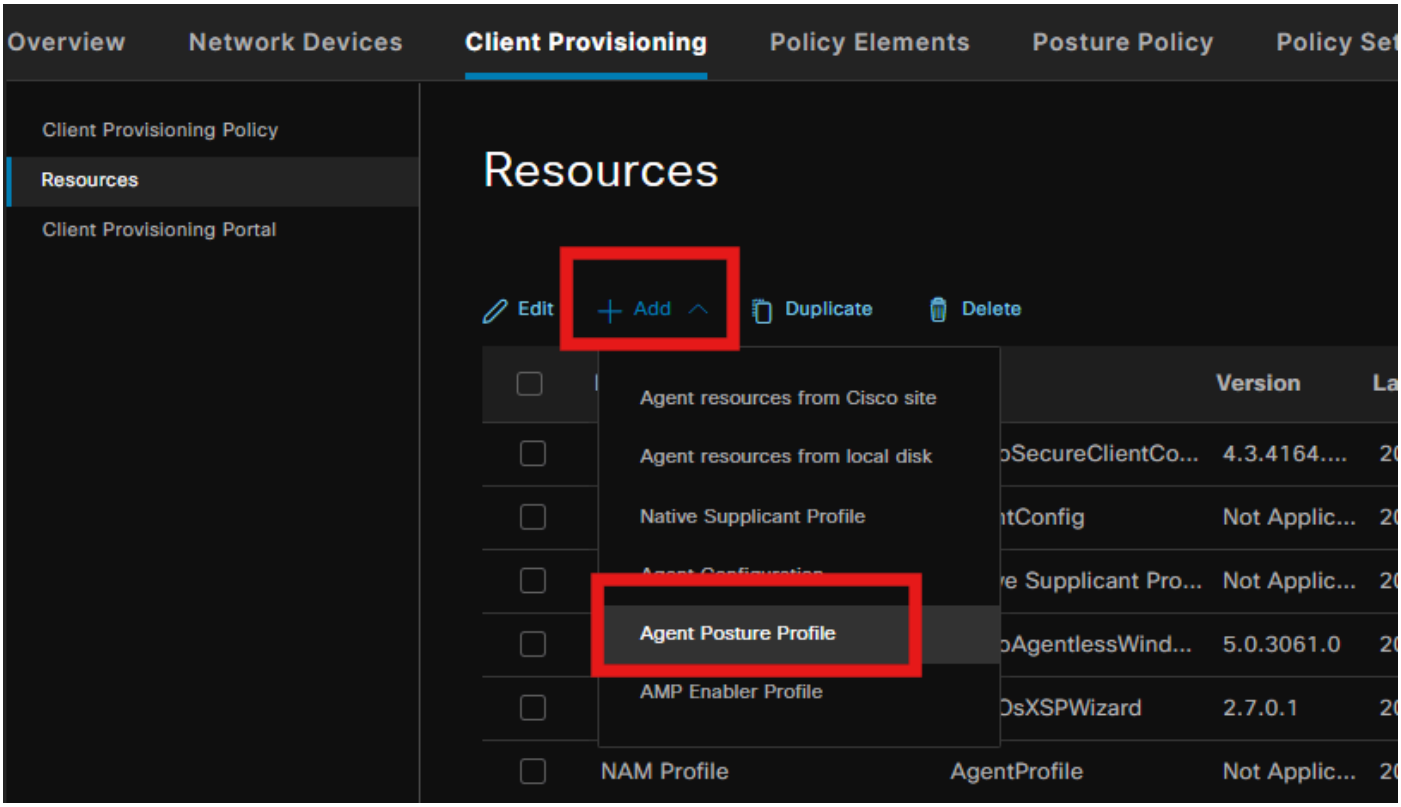
Pour plus d'informations sur la façon de configurer un profil NAM, référez-vous au guide Configure Secure Client NAM for Dot1x Using Windows and ISE 3.2.

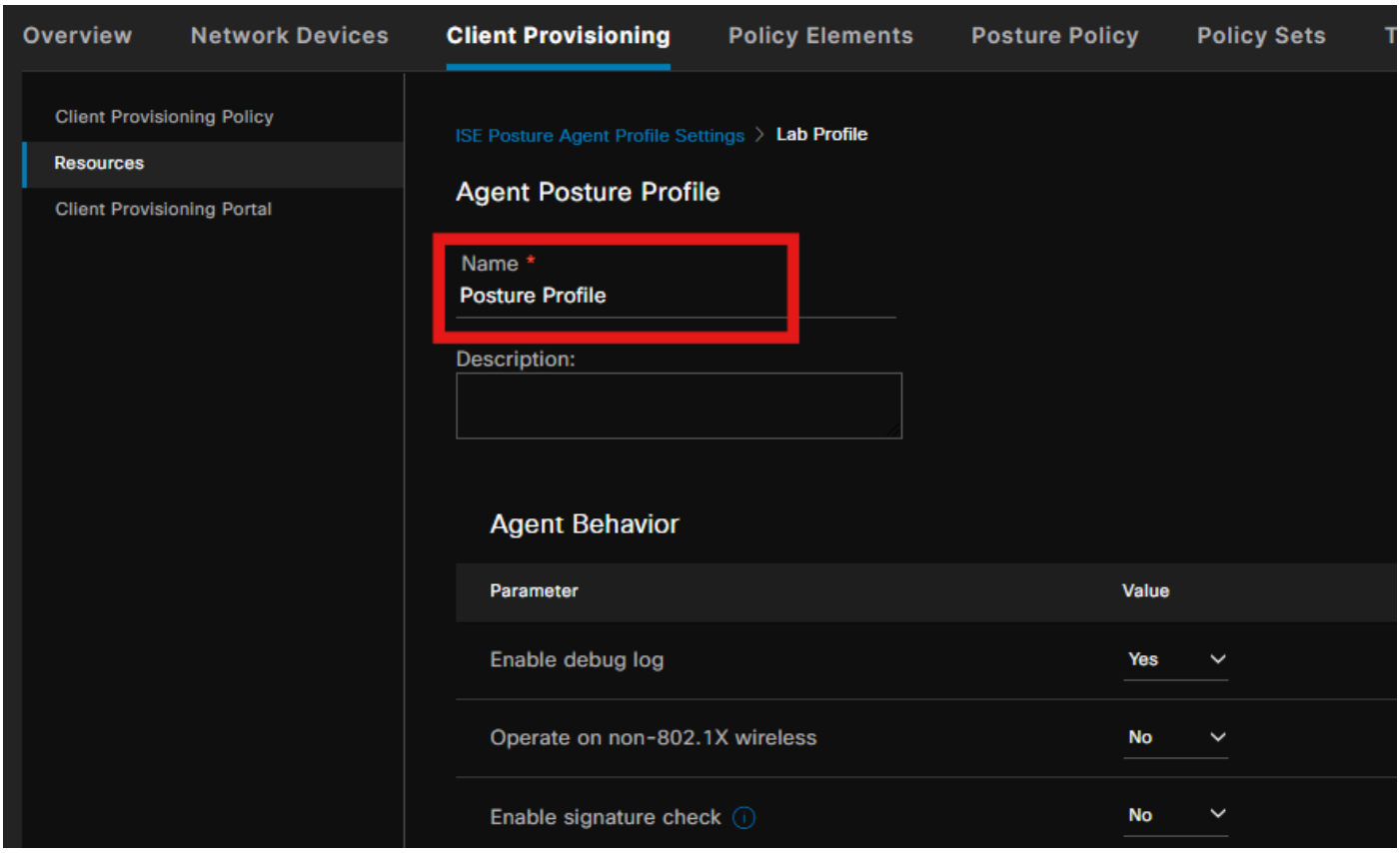
Étape 3. Télécharger le profil NAM sur ISE

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



Étape 4. Créer un profil de posture

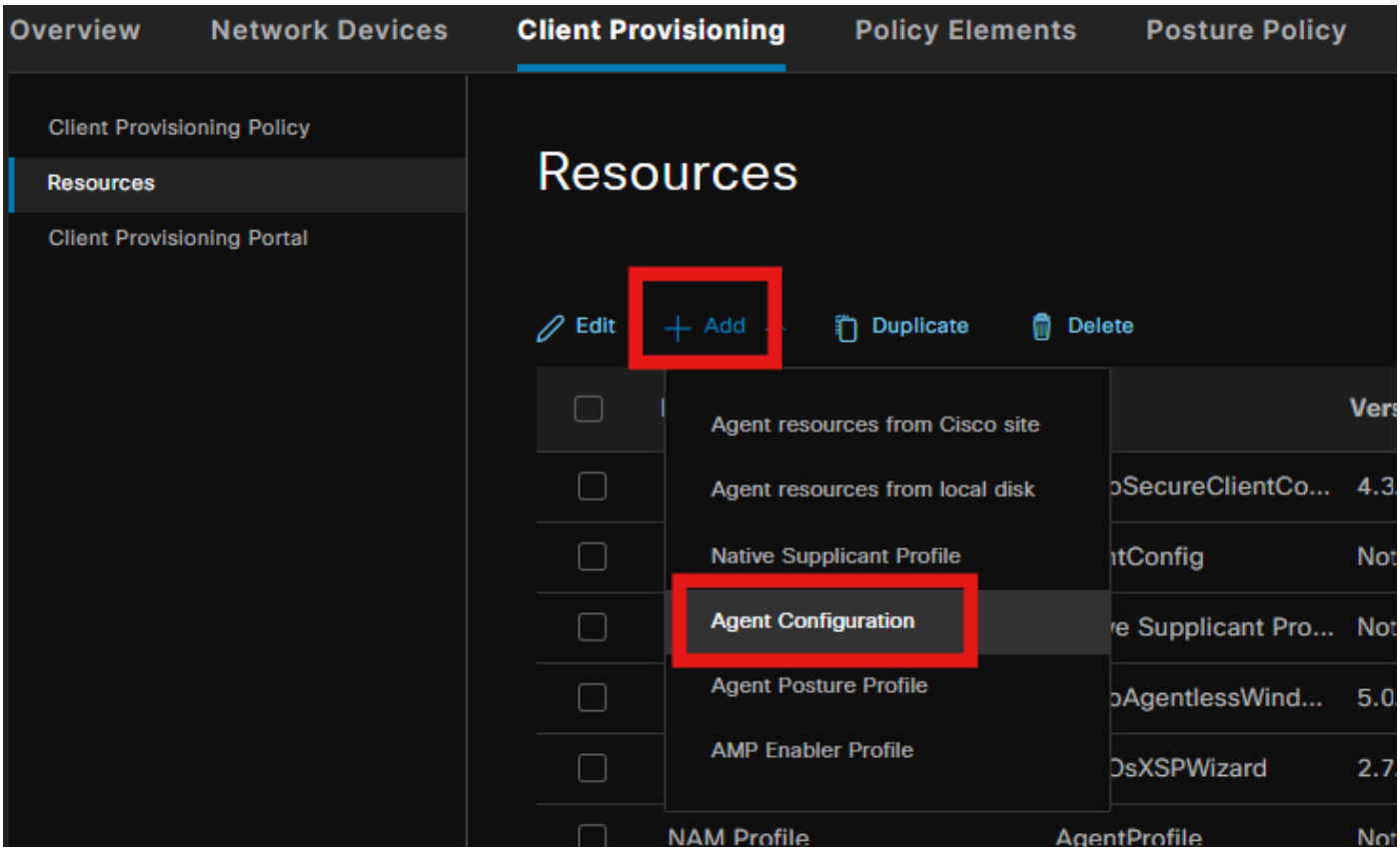




---

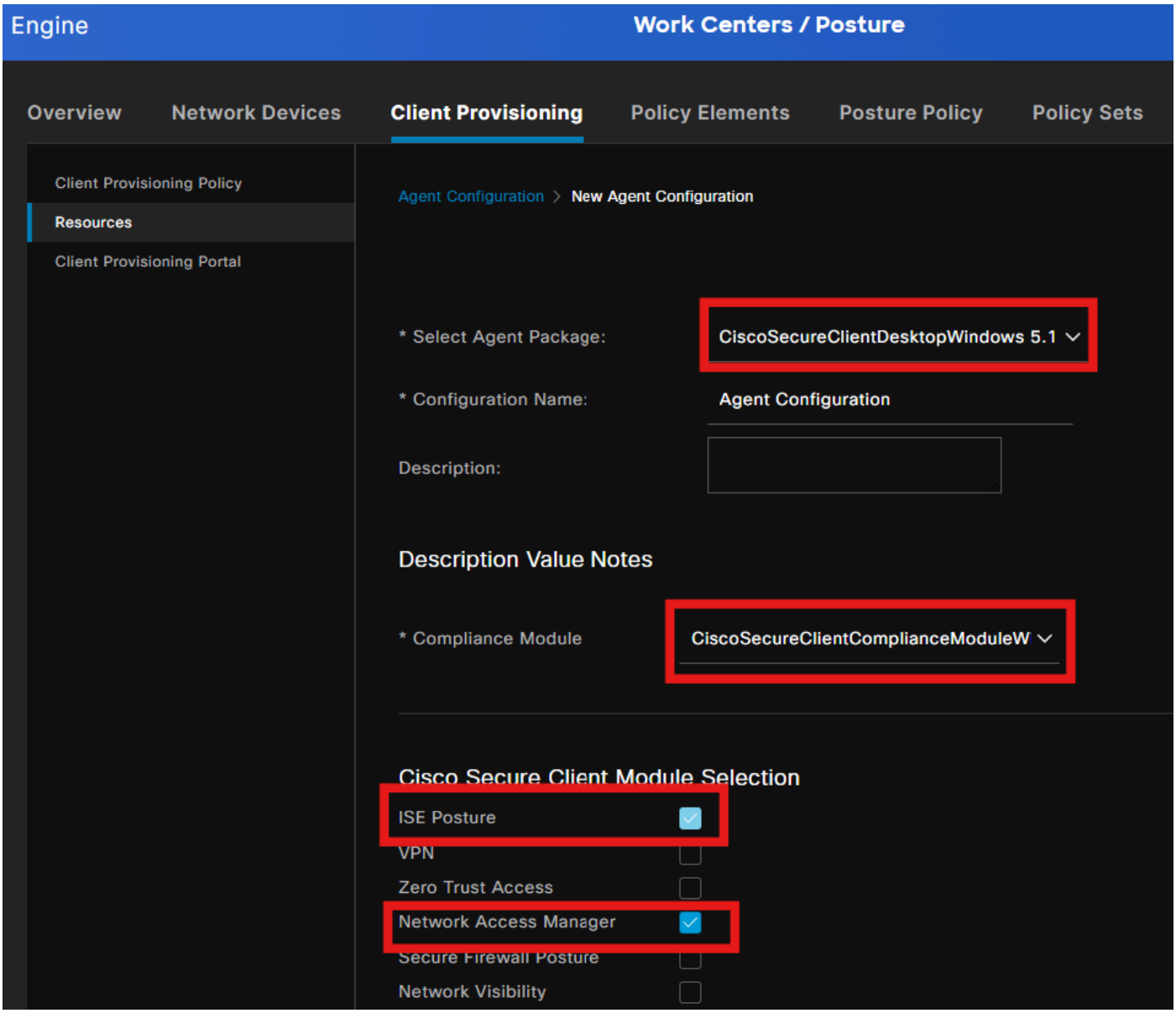
1. Dans la section Protocole de posture, n'oubliez pas d'ajouter un astérisque (*) pour permettre à l'agent de se connecter à tous les serveurs.

Étape 5. Créer la configuration de l'agent

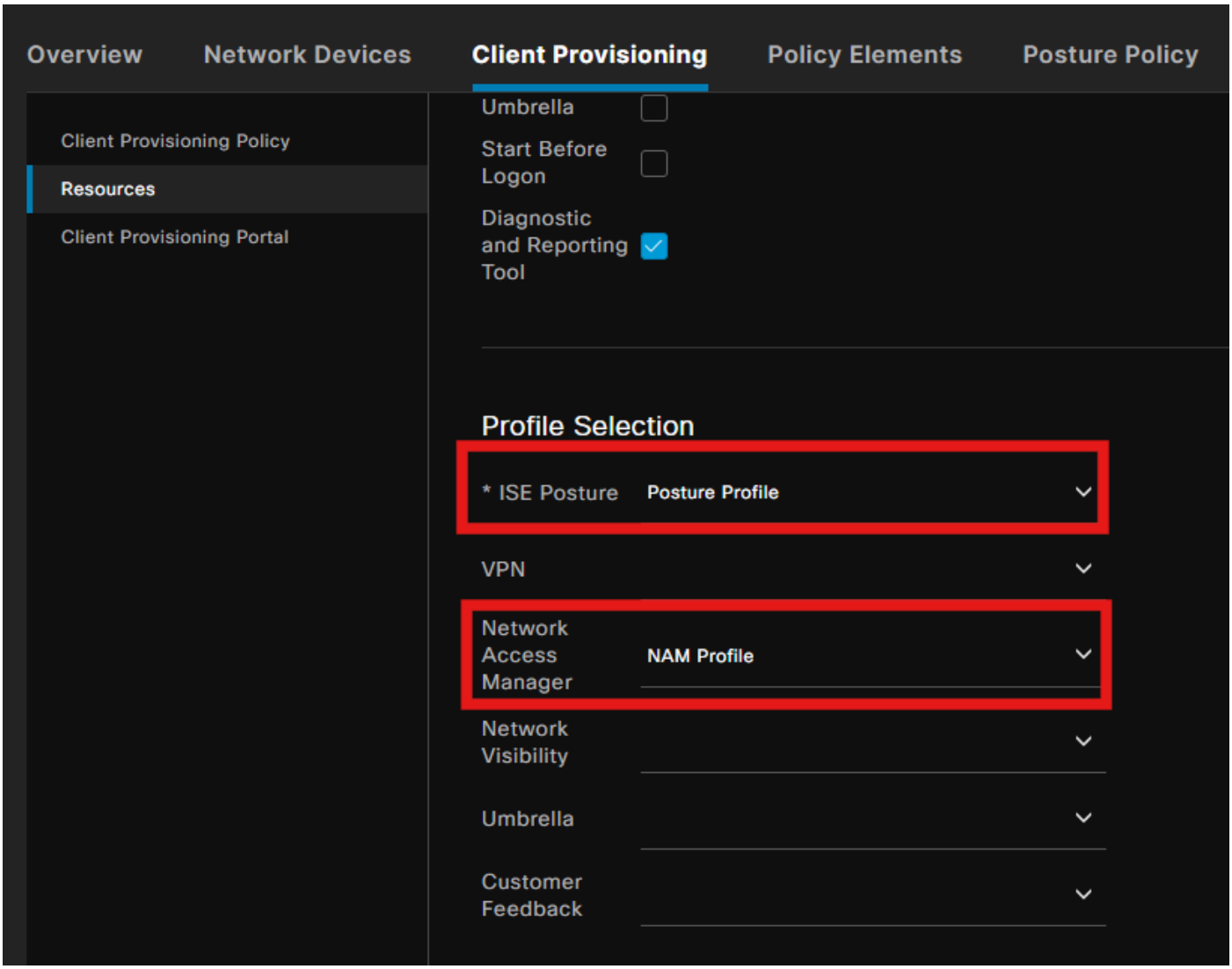


---

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

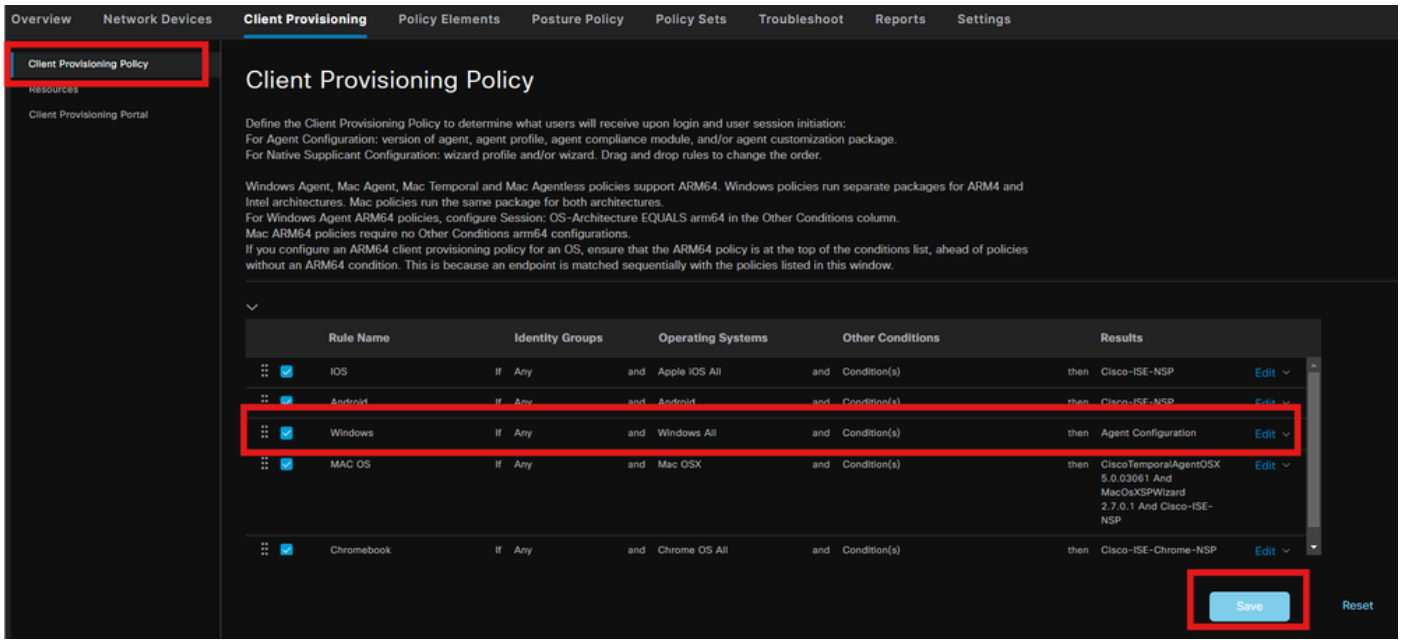


2. Sous Profile Selection, choisissez Posture et NAM Profile, puis cliquez sur Submit.


Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Client Provisioning Policy
Resources
Client Provisioning Portal
Umbrella
Start Before Logon
Diagnostic and Reporting Tool
Profile Selection
* ISE Posture
Posture Profile
VPN
Network Access Manager
NAM Profile
Network Visibility
Umbrella
Customer Feedback

Étape 6. Politique de provisionnement du client

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

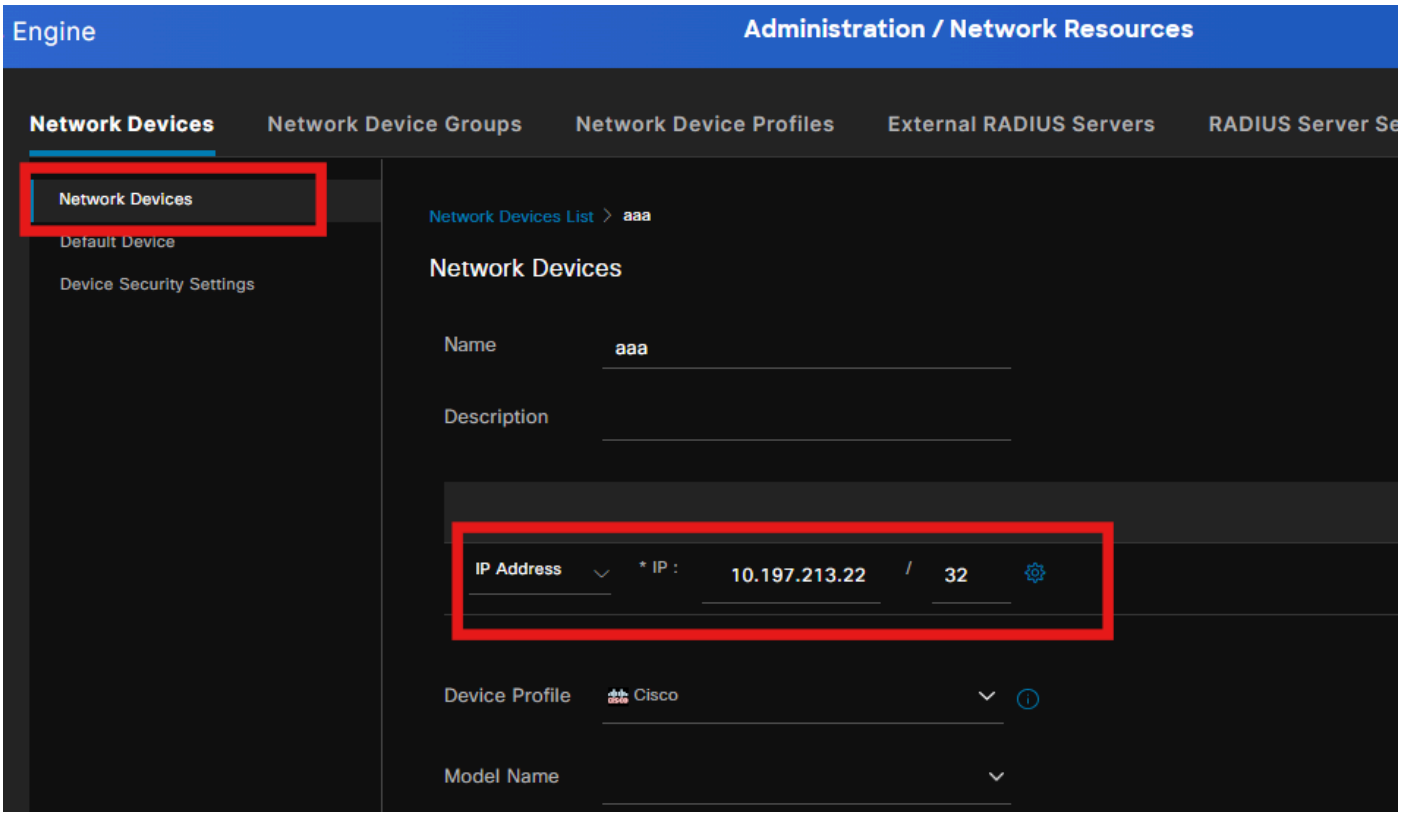


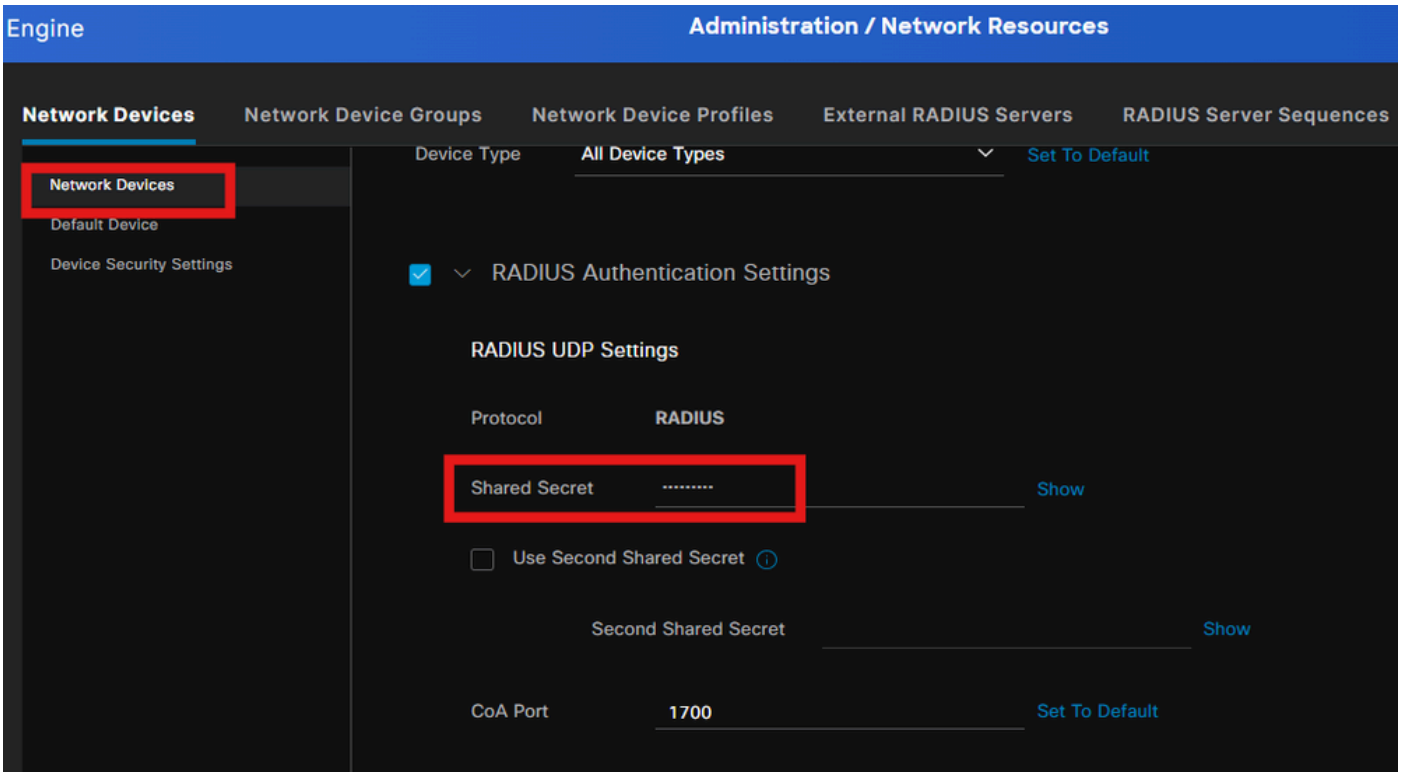
Étape 7. Politique de posture

Pour plus d'informations sur la façon de créer la politique de posture et les conditions, référez-vous au Guide de déploiement prescriptif de posture ISE.

Étape 8. Ajout d’un périphérique réseau

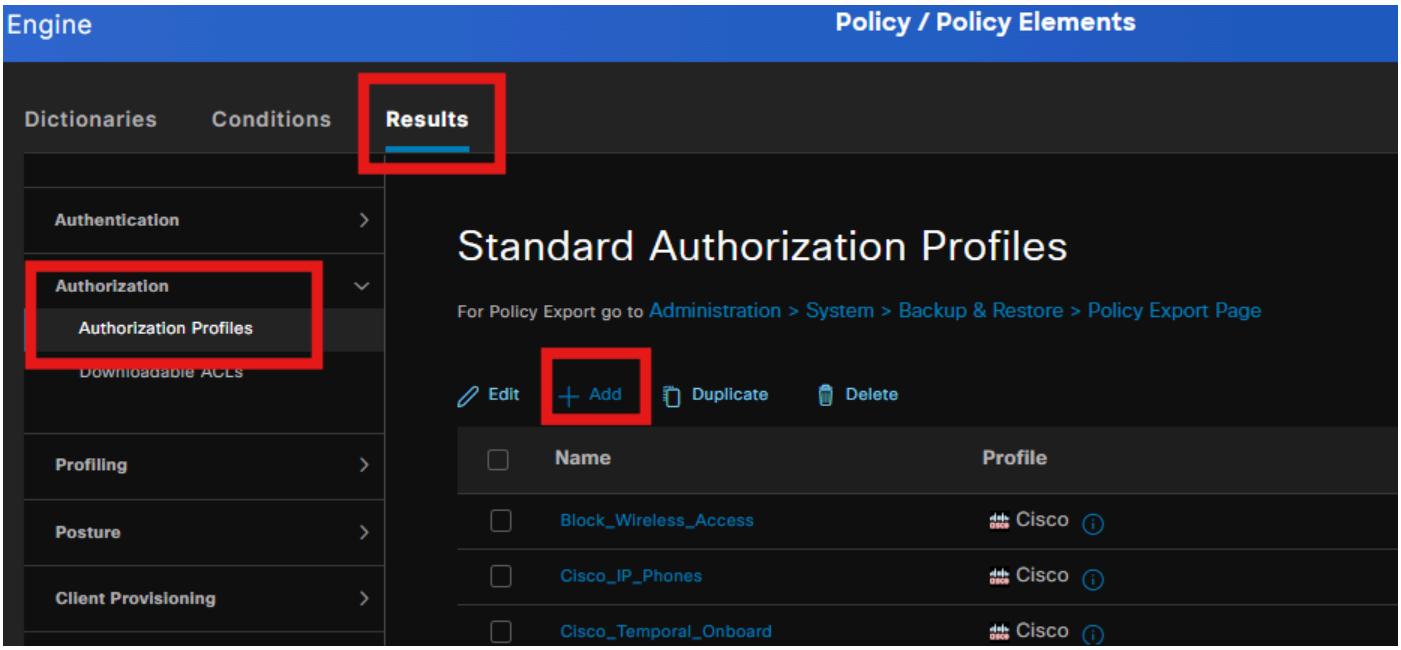
Pour ajouter l'adresse IP du commutateur et la clé secrète partagée radius, accédez à Administration > Network Resources.





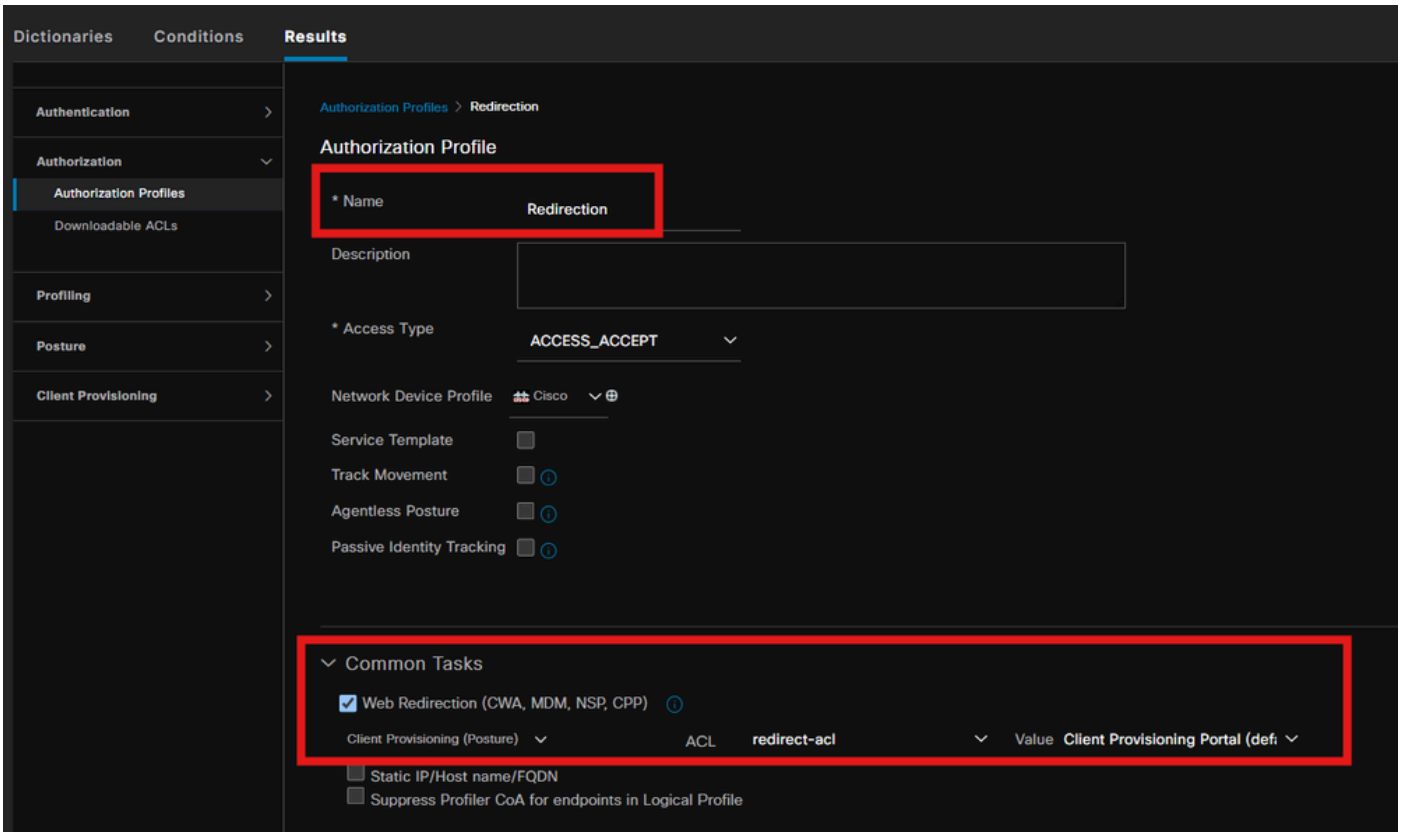
Étape 9. Profil d’autorisation

1. Pour créer un profil de redirection de position, accédez à Politique > Éléments de politique > Résultats.



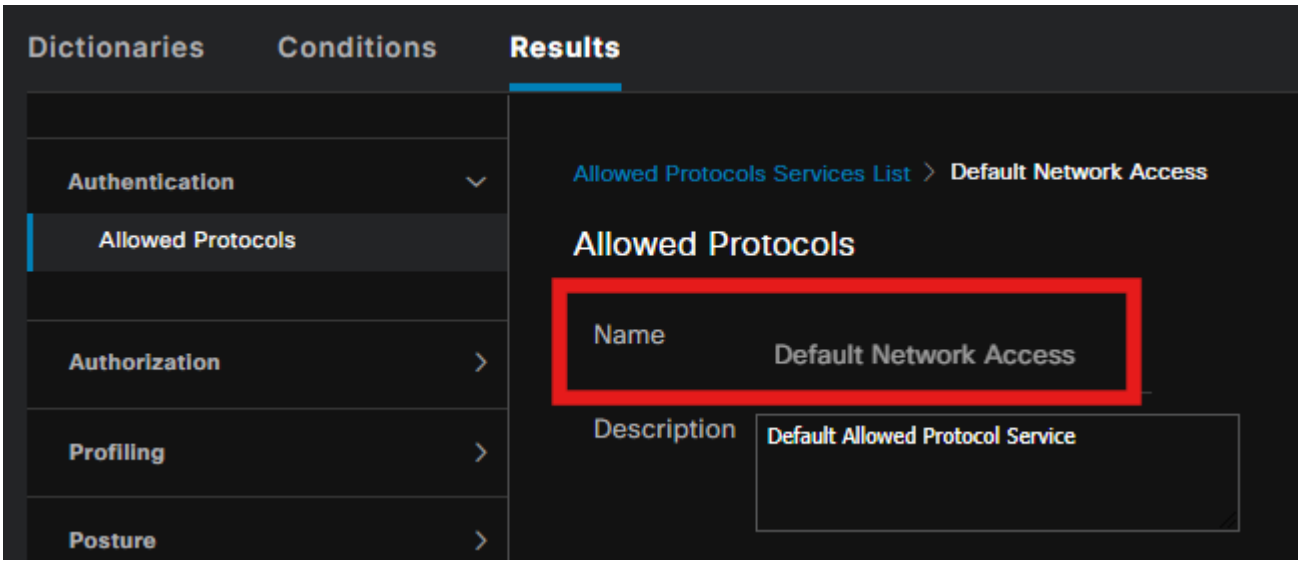
---

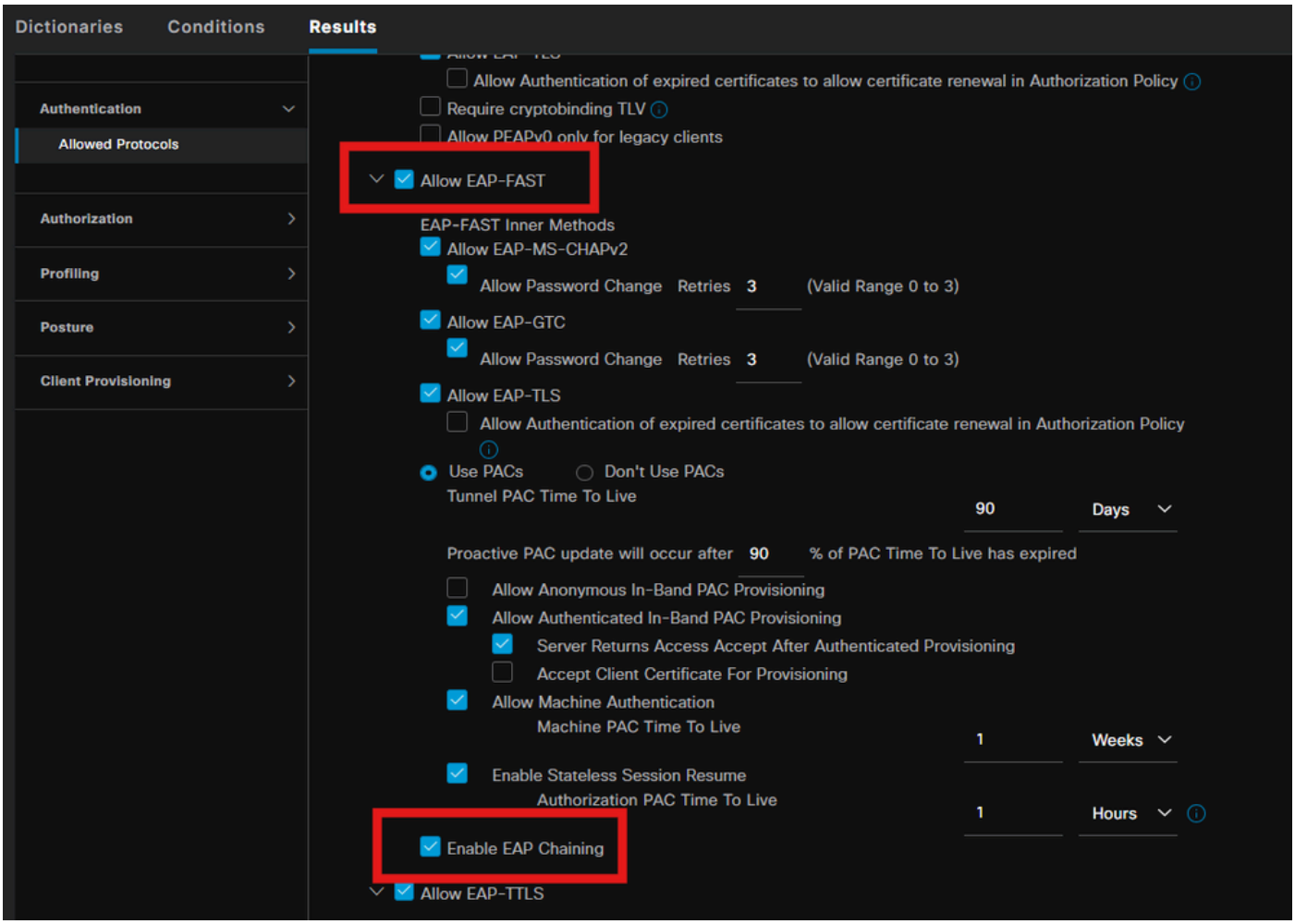
2. Sous Tâches courantes, sélectionnez Portail d'approvisionnement client avec ACL de redirection.



Étape 10. Protocoles autorisés

1. Accédez à Policy > Policy Elements > Results > Authentication > Allowed Protocols, sélectionnez les paramètres de chaînage EAP.


Dictionaries
Conditions
Results
Authentication
Allowed Protocols
Authorization
Profiling
Posture
Allowed Protocols Services List > Default Network Access
Allowed Protocols
Name
Default Network Access
Description
Default Allowed Protocol Service

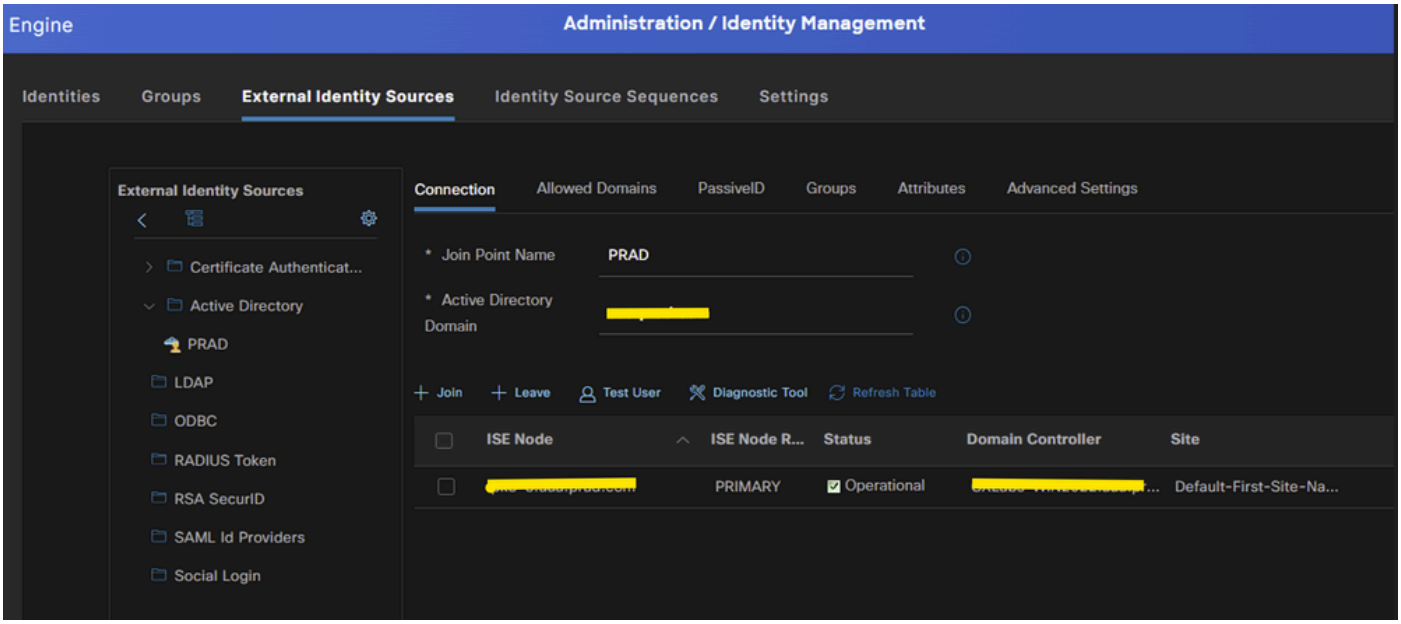

Dictionaries
Conditions
Results
Authentication
Allowed Protocols
Authorization
Profiling
Posture
Client Provisioning
Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
Require cryptobinding TLV
Allow PEAPv0 only for legacy clients
Allow EAP-FAST
EAP-FAST Inner Methods
Allow EAP-MS-CHAPv2
Allow Password Change Retries 3 (Valid Range 0 to 3)
Allow EAP-GTC
Allow Password Change Retries 3 (Valid Range 0 to 3)
Allow EAP-TLS
Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
Use PACs
Don't Use PACs
Tunnel PAC Time To Live
90
Days
Proactive PAC update will occur after 90 % of PAC Time To Live has expired
Allow Anonymous In-Band PAC Provisioning
Allow Authenticated In-Band PAC Provisioning
Server Returns Access Accept After Authenticated Provisioning
Accept Client Certificate For Provisioning
Allow Machine Authentication
Machine PAC Time To Live
1
Weeks
Enable Stateless Session Resume
Authorization PAC Time To Live
1
Hours
Enable EAP Chaining
Allow EAP-TTLS

Étape 11. Active Directory

1. La validation d'ISE est jointe au domaine Active Directory et des groupes de domaines sont sélectionnés, si nécessaire pour les conditions d'autorisation.

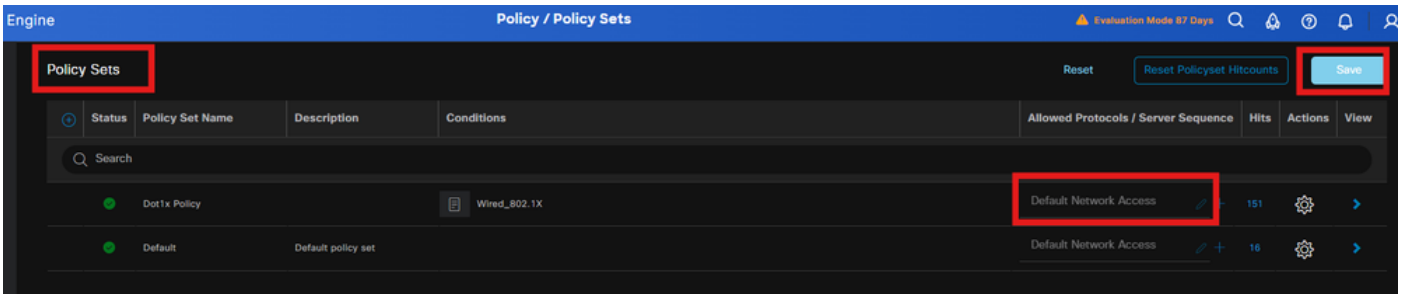
Administration > Gestion des identités > Sources d'identités externes > Active Directory

---



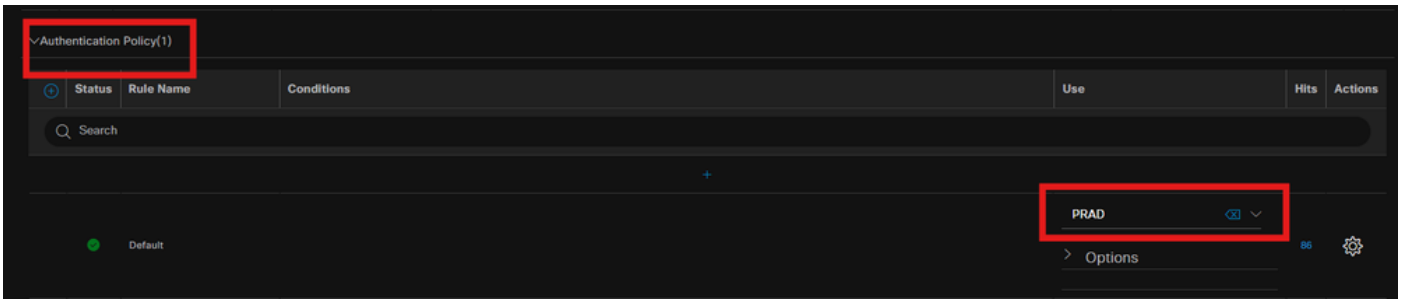
Étape 12. Ensembles de politiques

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



---

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

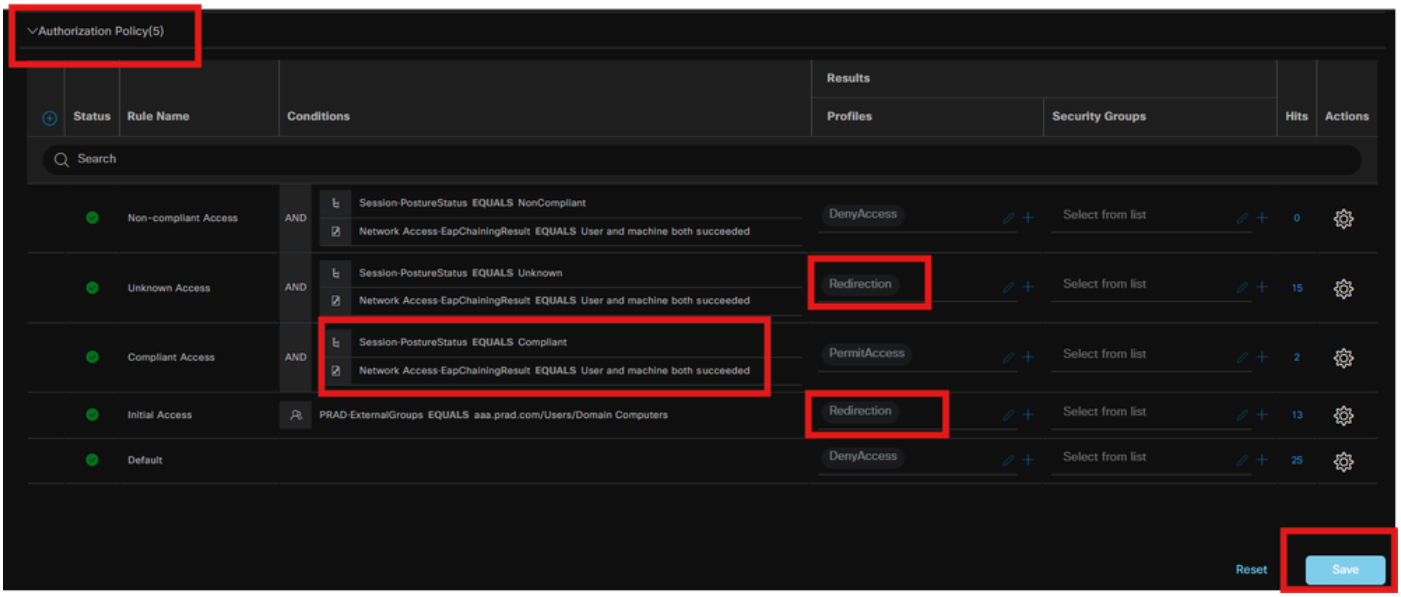


---

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

Dans ce cas d'utilisation :

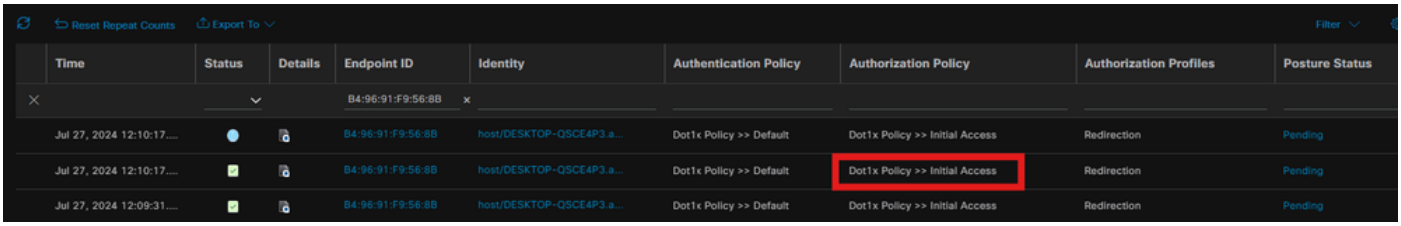
- Accès initial : Redirection vers le portail d'approvisionnement du client ISE pour installer l'agent client sécurisé et le profil NAM.
- Accès inconnu : Accès au portail d'approvisionnement du client pour la redirection basée sur la découverte de posture.
- Accès conforme : Accès réseau complet.
-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



Validation

Étape 1 : téléchargement et installation du module NAM/Secure Client Posture à partir d'ISE

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



2. Sur le commutateur, spécifiez l'URL de redirection et la liste de contrôle d'accès qui est appliquée pour le 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 : Inconnu
Adresse IPv4 : <IP-client>
Nom d'utilisateur : host/DESKTOP-xxxxxx.xxx
État : Autorisé
Domaine : DONNÉES
Mode hôte d’exploitation : hôte unique
Oper control dir : les deux
Expiration de session : S/O
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 : Doit sécuriser
État de sécurité : Liaison non sécurisée

Stratégies de serveur :
ACL de redirection URL : redirect-acl
Redirection URL :
https://ise33.xxxx:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39fd08-7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2
ACL ACS : xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3


Liste d'état de méthode :
Etat de méthode
dot1x Authc Success

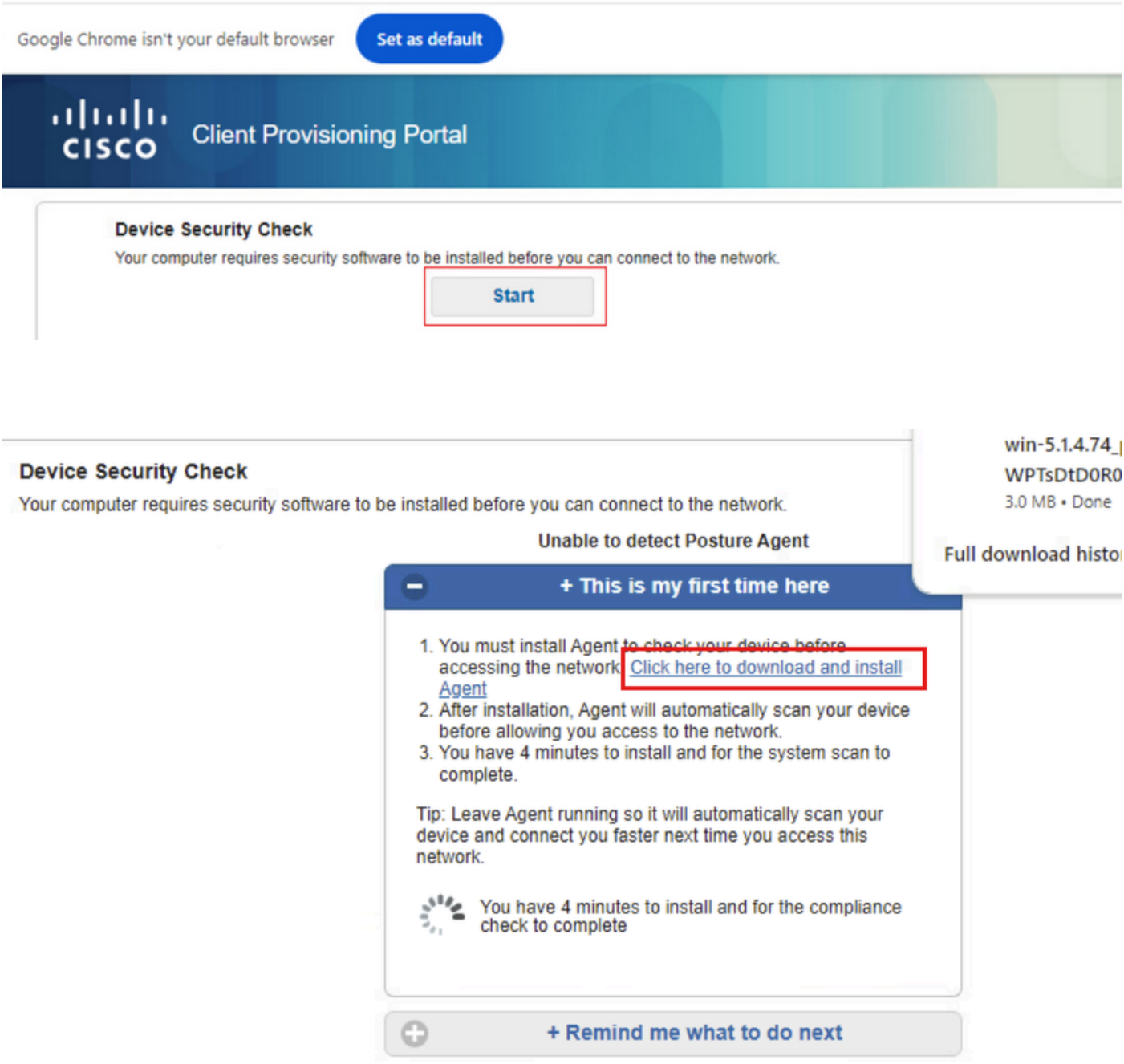
Switch#sh interface de base de données de suivi des périphériques te1/0/24

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
```

---

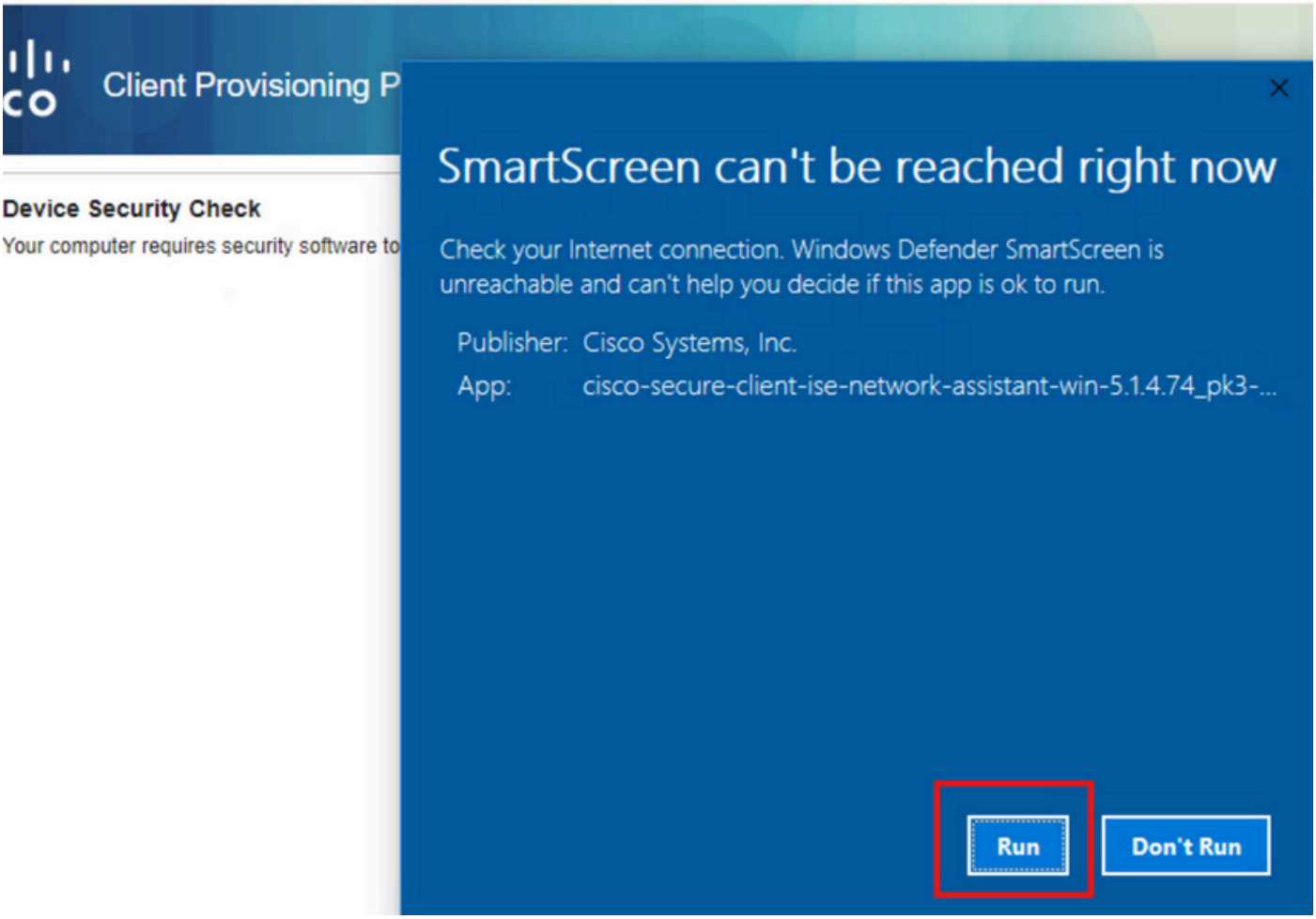
3. Sur le point de terminaison, vérifiez le trafic redirigé vers la posture ISE et cliquez sur Start pour

télécharger l'assistant de configuration réseau sur le point de terminaison.



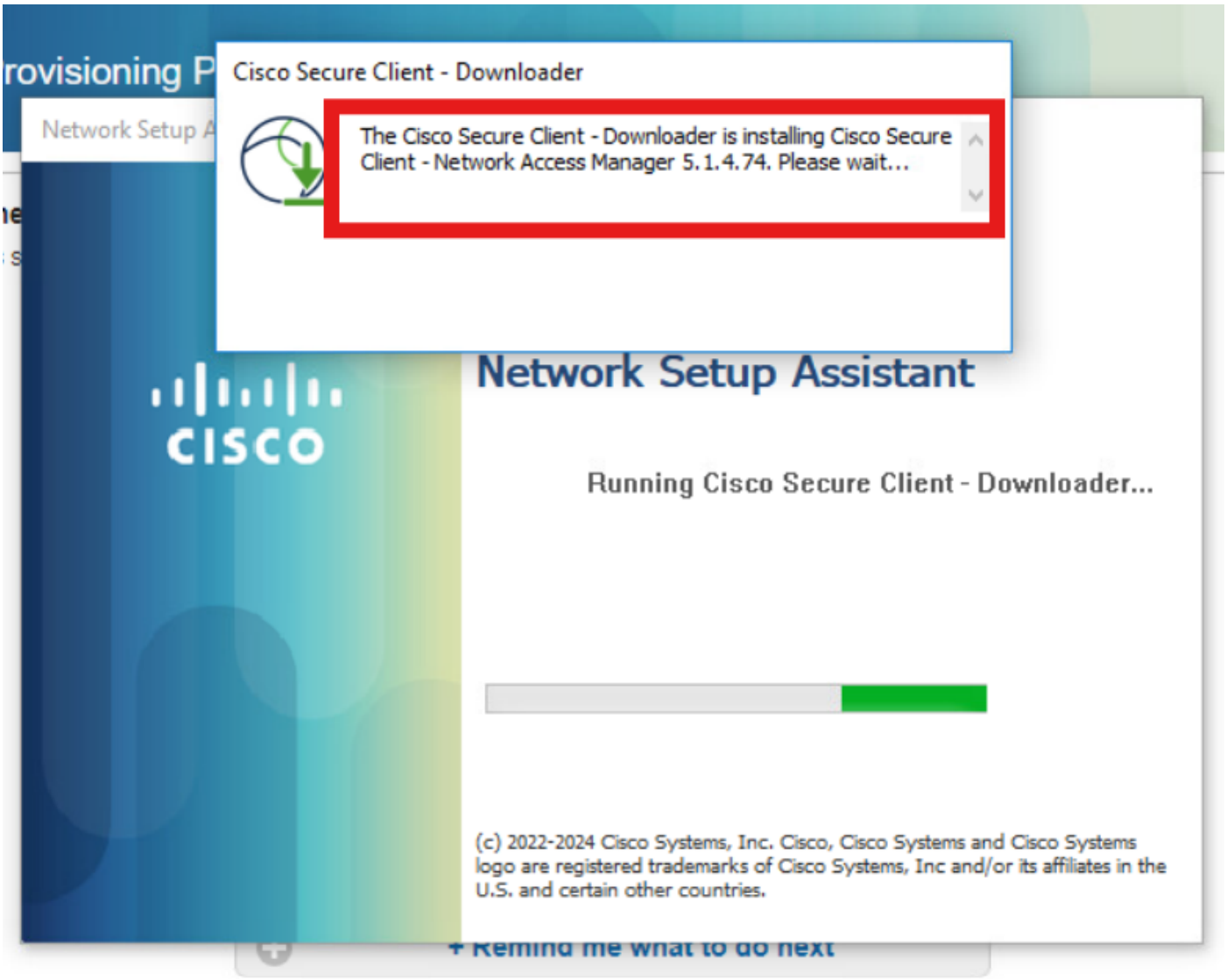
---

4. Cliquez sur Exécuter pour installer l'application NSA.



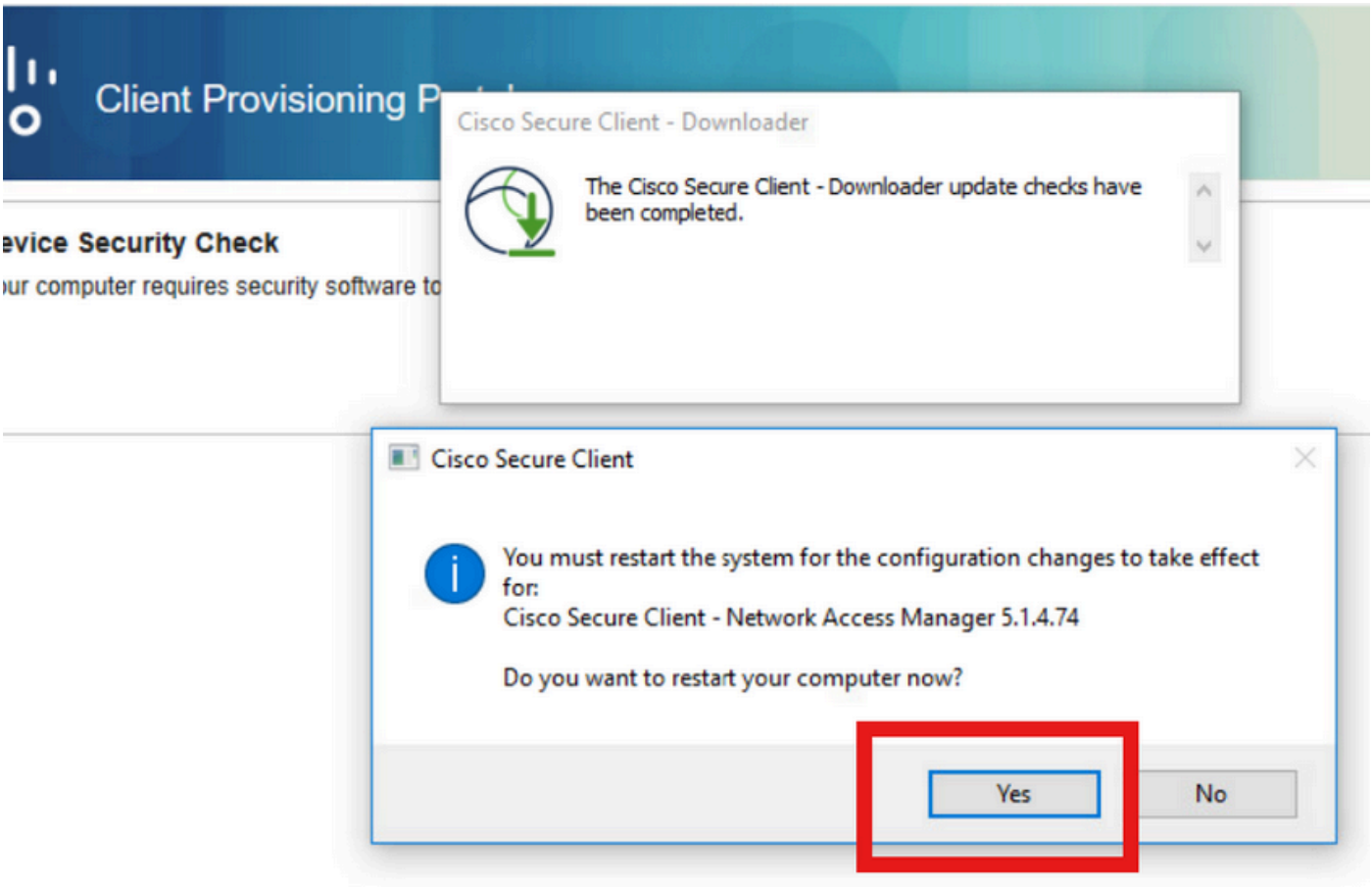
---

2. 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.



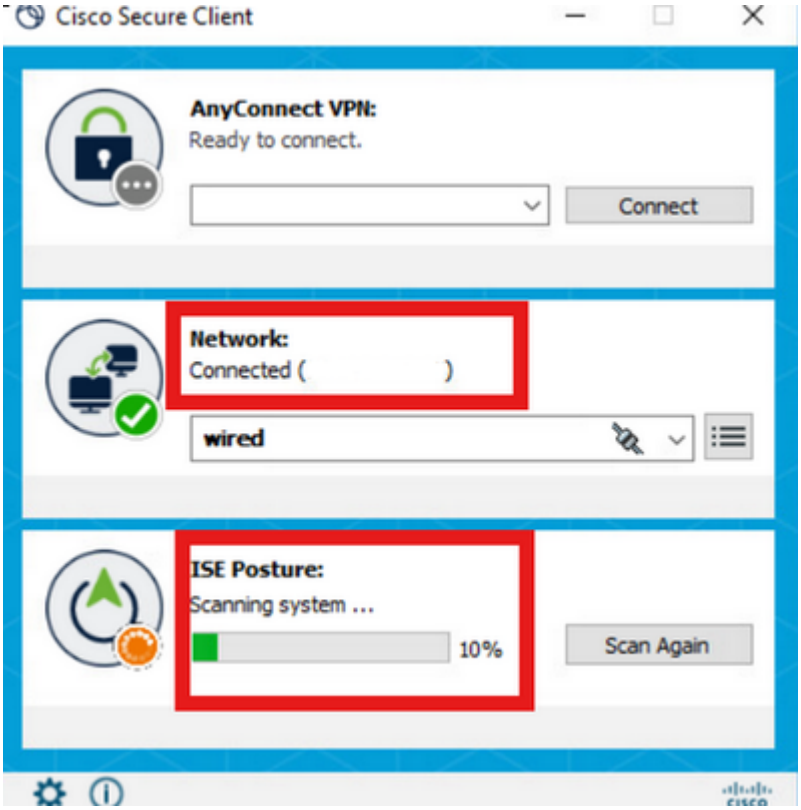
---

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



Étape 2. EAP-FAST

1. Une fois que le PC redémarre et que l'utilisateur se connecte, le NAM authentifie l'utilisateur et la machine via EAP-FAST. Si le point d'extrémité s'authentifie correctement, NAM affiche qu'il est connecté et le module Posture déclenche le balayage de posture.



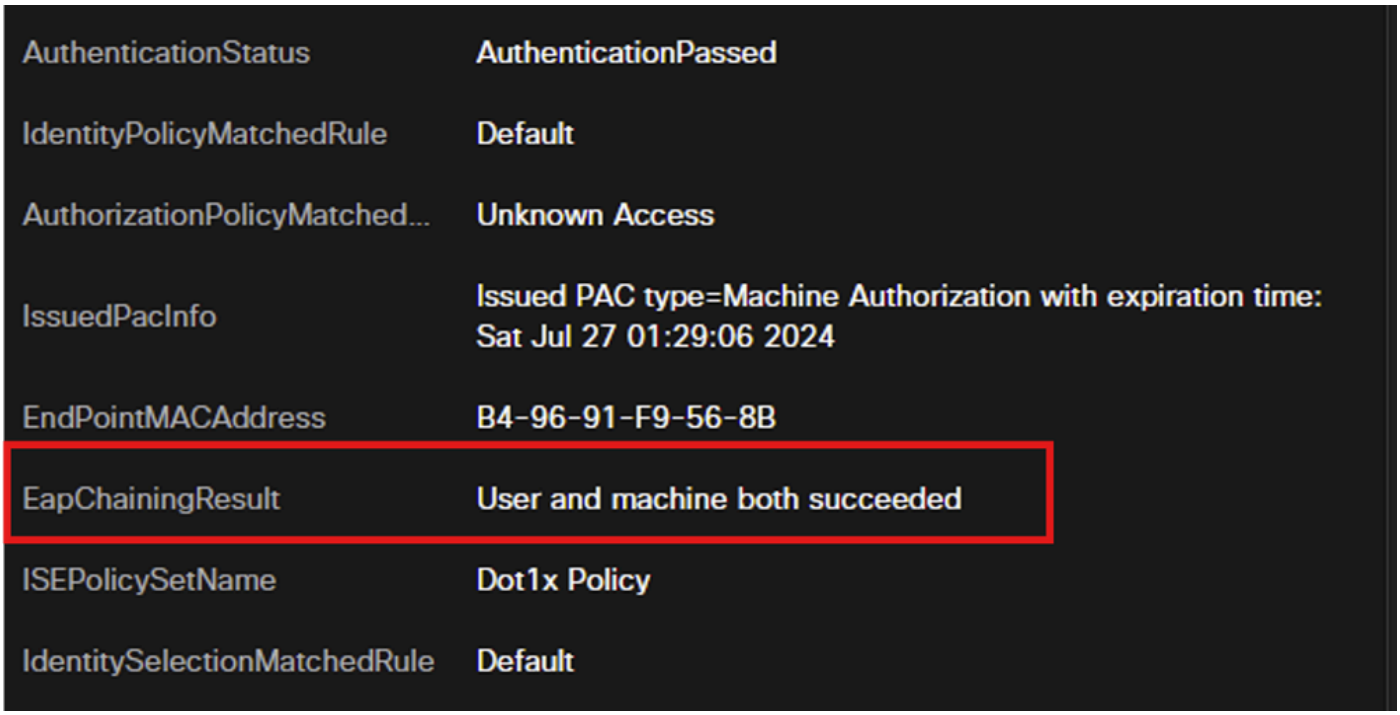
---

2. Sur les journaux en direct ISE, le point de terminaison atteint maintenant la règle d'accès inconnu.



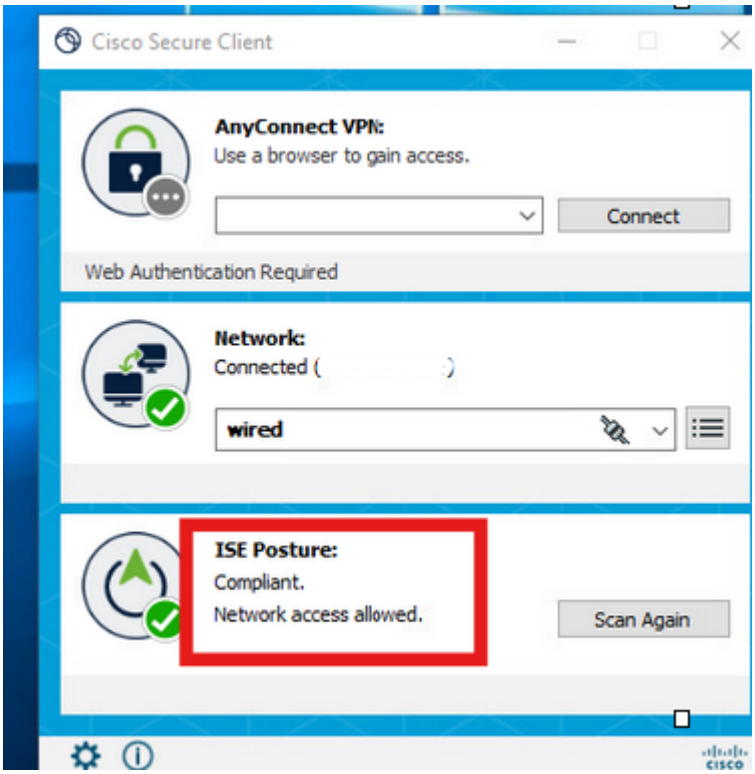
---

3. Maintenant, le protocole d’authentification est EAP-FAST en fonction de la configuration du profil NAM et le résultat du chaînage EAP est Succès.



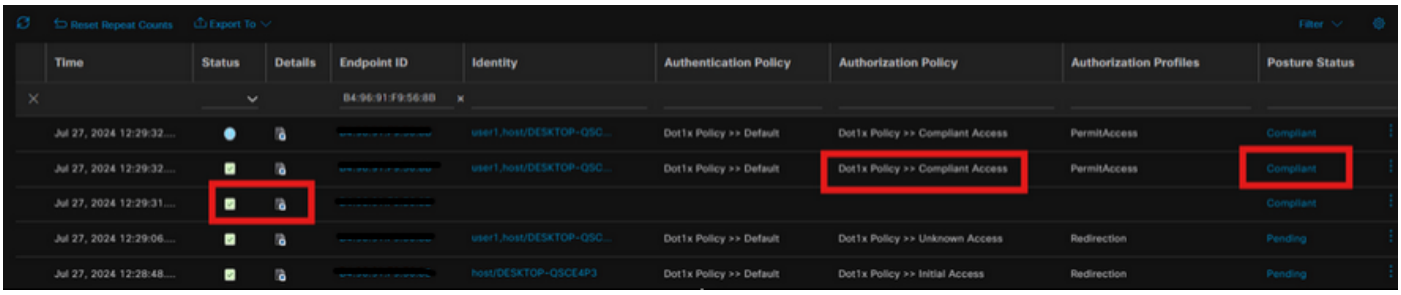
Étape 3. Analyse de la posture

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



---

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

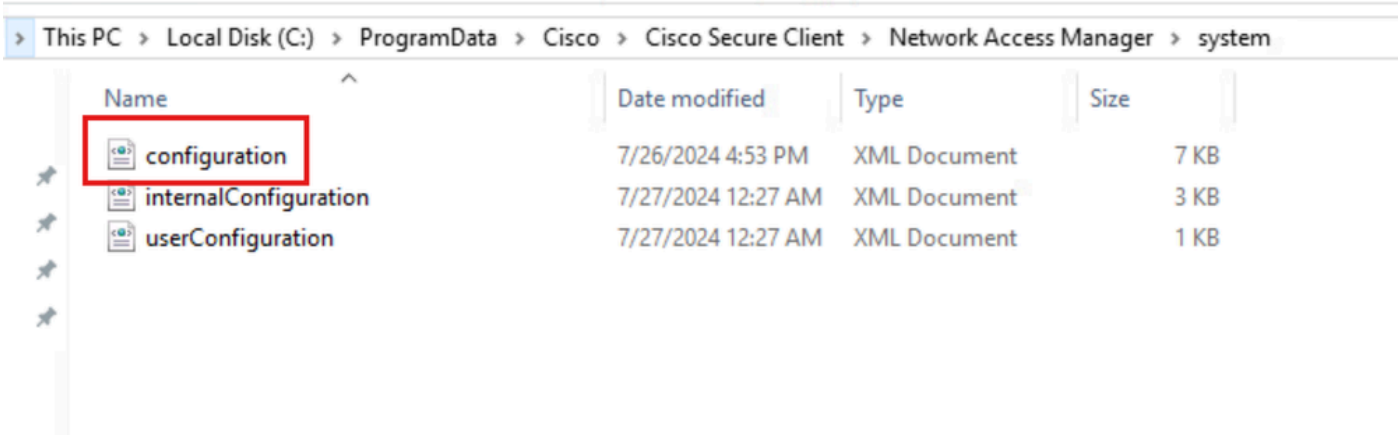


Dépannage

Étape 1. Profil NAM

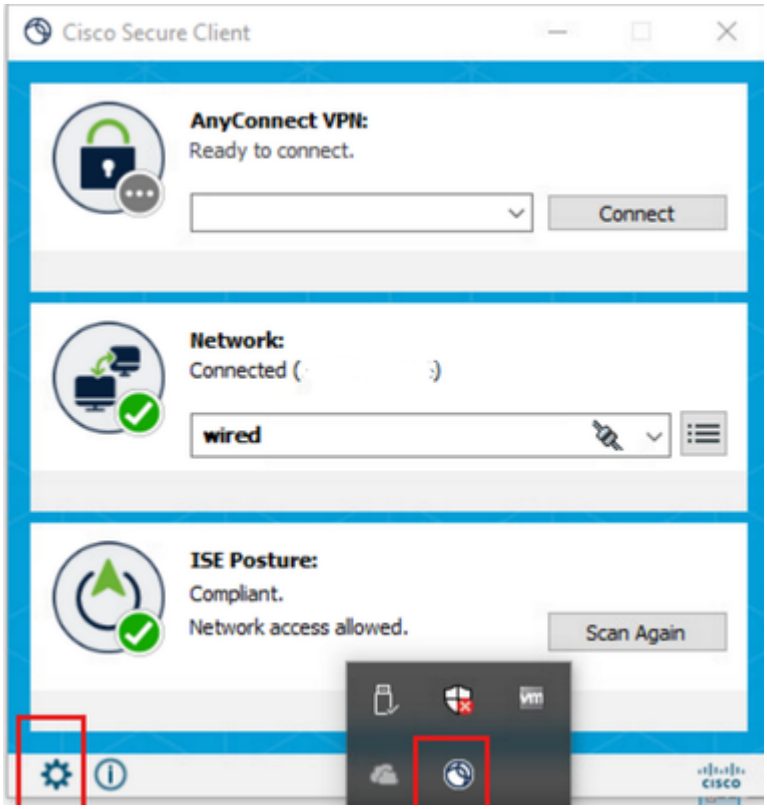
1. Vérifiez que le fichier configuration.xml du profil NAM figure dans le chemin suivant sur votre ordinateur après l'installation du module NAM : C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

---



Étape 2. Journalisation étendue du NAM

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

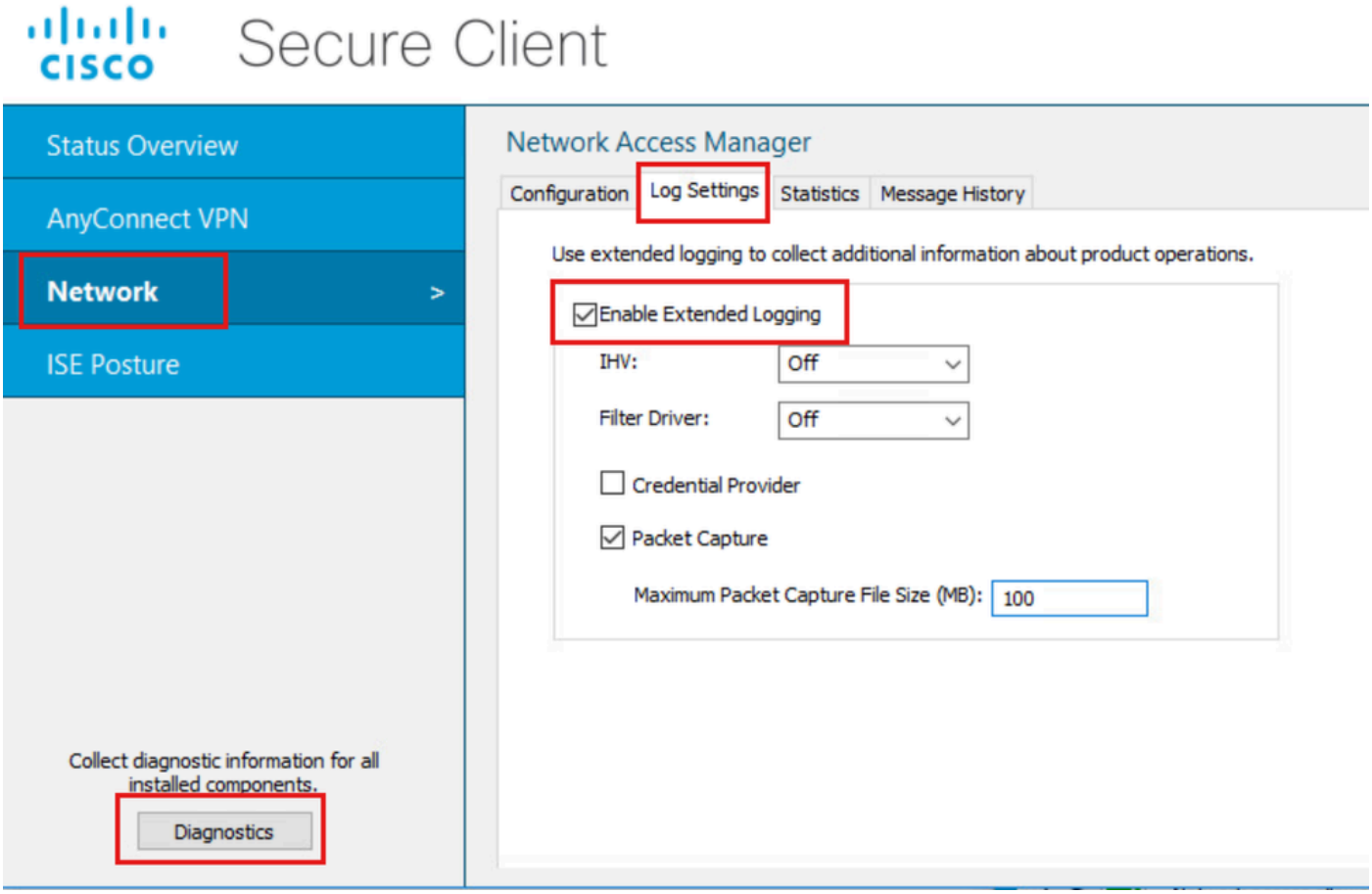


---

2. Accédez à l'onglet Réseau > Paramètres du journal. Cochez la case Enable Extended Logging.

---

3. Définissez la taille du fichier de capture de paquets sur 100 Mo. Après avoir reproduit le problème, cliquez sur Diagnostics pour créer l'offre groupée DART sur le terminal.



---

4. La section Historique des messages affiche les détails de chaque étape de NAM terminée.

Étape 3. Débogages sur le commutateur

1. 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

1. Recueillez l'offre groupée 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

- Configuration du NAM du client sécurisé pour Dot1x à l'aide de Windows et ISE 3.2
- Guide de déploiement prescriptif de la position ISE
- Dépannage de Dot1x sur les commutateurs Cisco IOS® XE 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.