Intégration d'AnyConnect 4.0 avec l'exemple de configuration de version 1.3 ISE

Contenu

Introduction

Ce document décrit la nouvelle fonctionnalité dans la version 1.3 du Logiciel Cisco Identity Services Engine (ISE) qui te permet pour configurer plusieurs modules sécurisés de client de mobilité d'AnyConnect et pour provision les automatiquement au point final. Ce document présente comment configurer des modules VPN, de gestionnaire d'accès au réseau (NAM), et de posture sur ISE et les pousser à l'utilisateur en entreprise.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiements, authentification, et autorisation ISE
- Configuration des contrôleurs LAN Sans fil (WLCs)
- La connaissance de base VPN et de 802.1x

- La configuration des profils VPN et NAM avec AnyConnect profilent des éditeurs

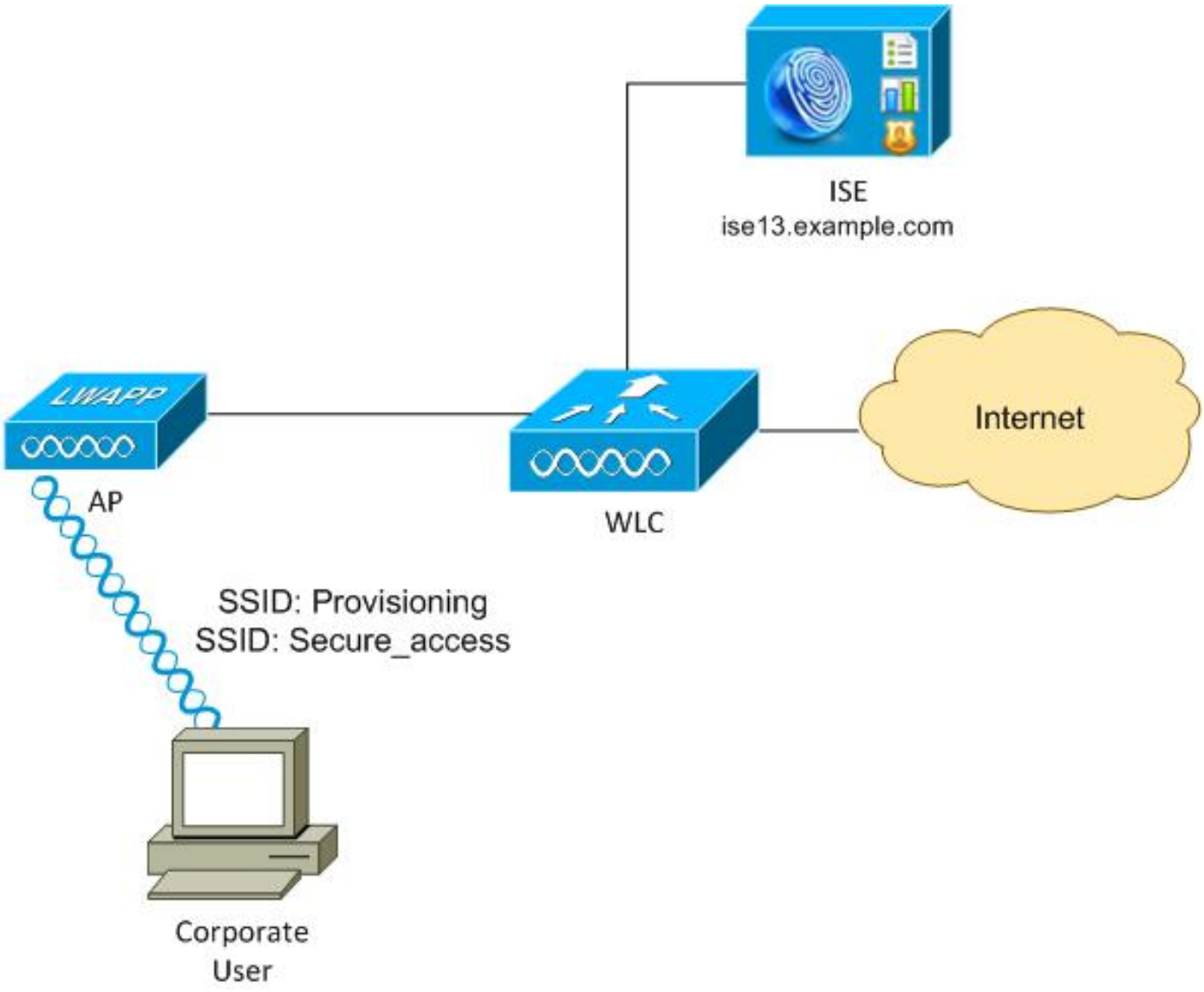
Composants utilisés

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

- Microsoft Windows 7
- Version 7.6 et ultérieures de Cisco WLC
- Logiciel de Cisco ISE, versions 1.3 et ultérieures

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Topologie et écoulement



Voici l'écoulement :

Étape 1. Identifiant SSID (Service Set Identifier) d'acceses d'utilisateur en entreprise :

Ravitaillement. Exécute l'authentification de 802.1x avec l'EAP Protocol-protégé par authentification extensible (EAP-PEAP). La règle d'autorisation de **ravitaillement** est produite sur ISE et l'utilisateur est réorienté pour le ravitaillement d'AnyConnect (par l'intermédiaire du ravitaillement de client Protal). Si AnyConnect n'est pas détecté sur l'ordinateur, tous les modules configurés sont installés (VPN, NAM, posture). Avec ce profil, la configuration pour chaque module est poussée.

Étape 2. Une fois qu'AnyConnect est installé, l'utilisateur doit redémarrer le PC. Après que la réinitialisation, AnyConnect fonctionne et le SSID correct est automatiquement utilisé selon le profil configuré NAM (Secure_access). EAP-PEAP est utilisé (comme exemple, le Protocol-transport Layer Security (EAP-TLS) d'authentification extensible pourrait être également utilisé). En même temps, le module de posture vérifie si la station est conforme (vérifie l'existence du **fichier de c:\test.txt**).

Étape 3. Si l'état de posture de station est inconnu (aucun état de module de posture), il est encore réorienté pour le ravitaillement, parce que la règle d'Authz d'**inconnu** est produite sur ISE. Une fois que la station est conforme, ISE envoie une modification de l'autorisation (CoA) au contrôleur LAN Sans fil, qui déclenche la ré-authentification. Une deuxième authentification se produit, et la règle **conforme** est frappée sur ISE, qui fournira à l'utilisateur l'accès complet au réseau.

En conséquence, l'utilisateur provisioned avec AnyConnect VPN, NAM, et modules de posture qui tiennent compte de l'accès unifié au réseau. La fonctionnalité semblable peut être utilisée sur l'appliance de sécurité adaptable (ASA) pour l'accès VPN. Actuellement, ISE peut faire la même chose pour n'importe quel type d'accès avec une approche très granulaire.

Cette fonctionnalité n'est pas limitée aux utilisateurs en entreprise, mais elle est probablement la plus commune pour la déployer pour ce groupe d'utilisateurs.

Configurer

WLC

Le WLC est configuré avec deux SSID :

- Ravitaillement - [WPA + WPA2][Auth(802.1X)]. Ce SSID est utilisé pour le ravitaillement d'AnyConnect.
- Secure_access - [WPA + WPA2][Auth(802.1X)]. Ce SSID est utilisé pour l'accès sécurisé après que le point final provisioned avec le module NAM qui est configuré pour ce SSID.

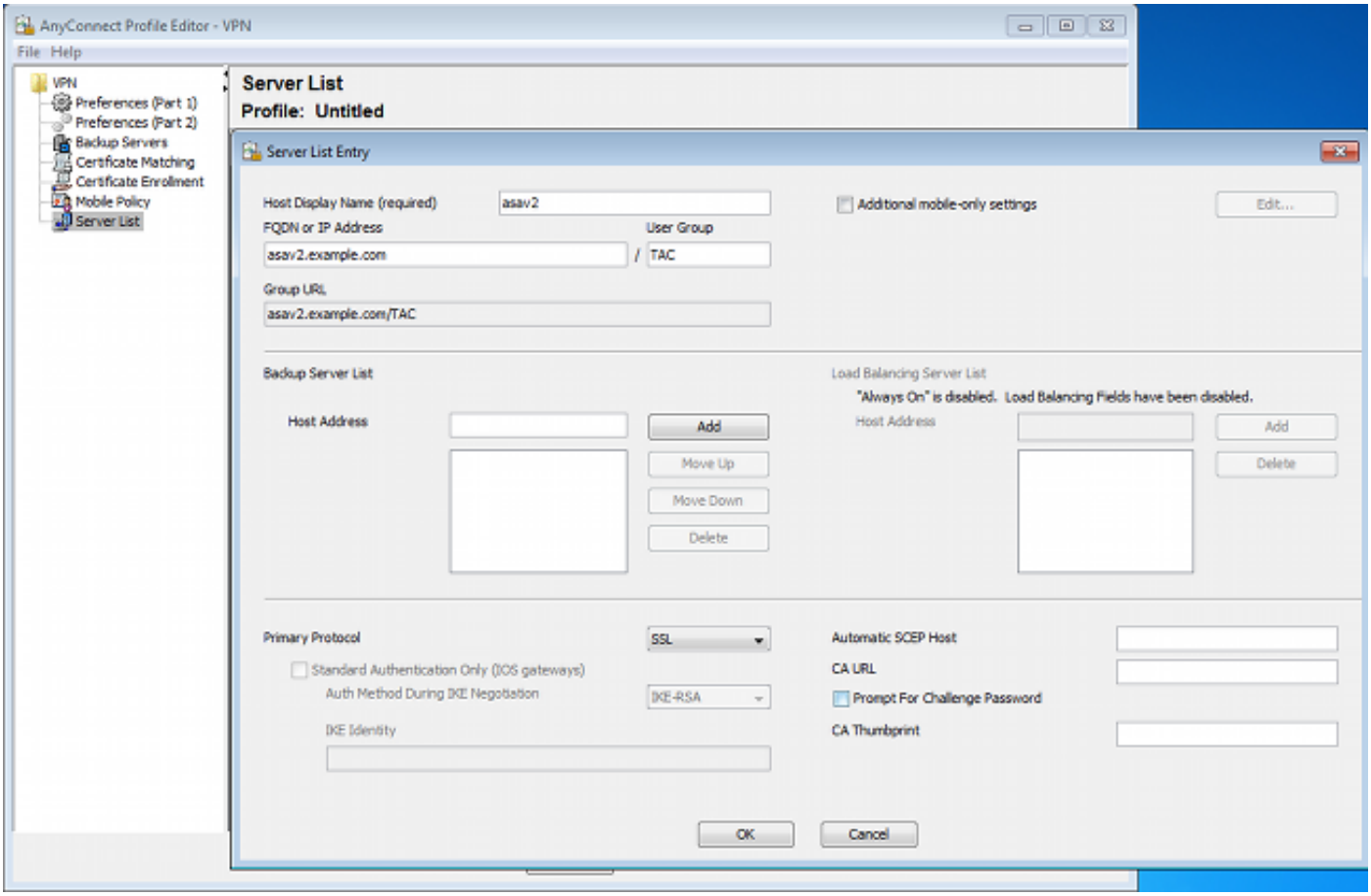
ISE

Étape 1. Ajoutez le WLC

Ajoutez le WLC aux périphériques de réseau sur ISE.

Étape 2. Configurez le profil VPN

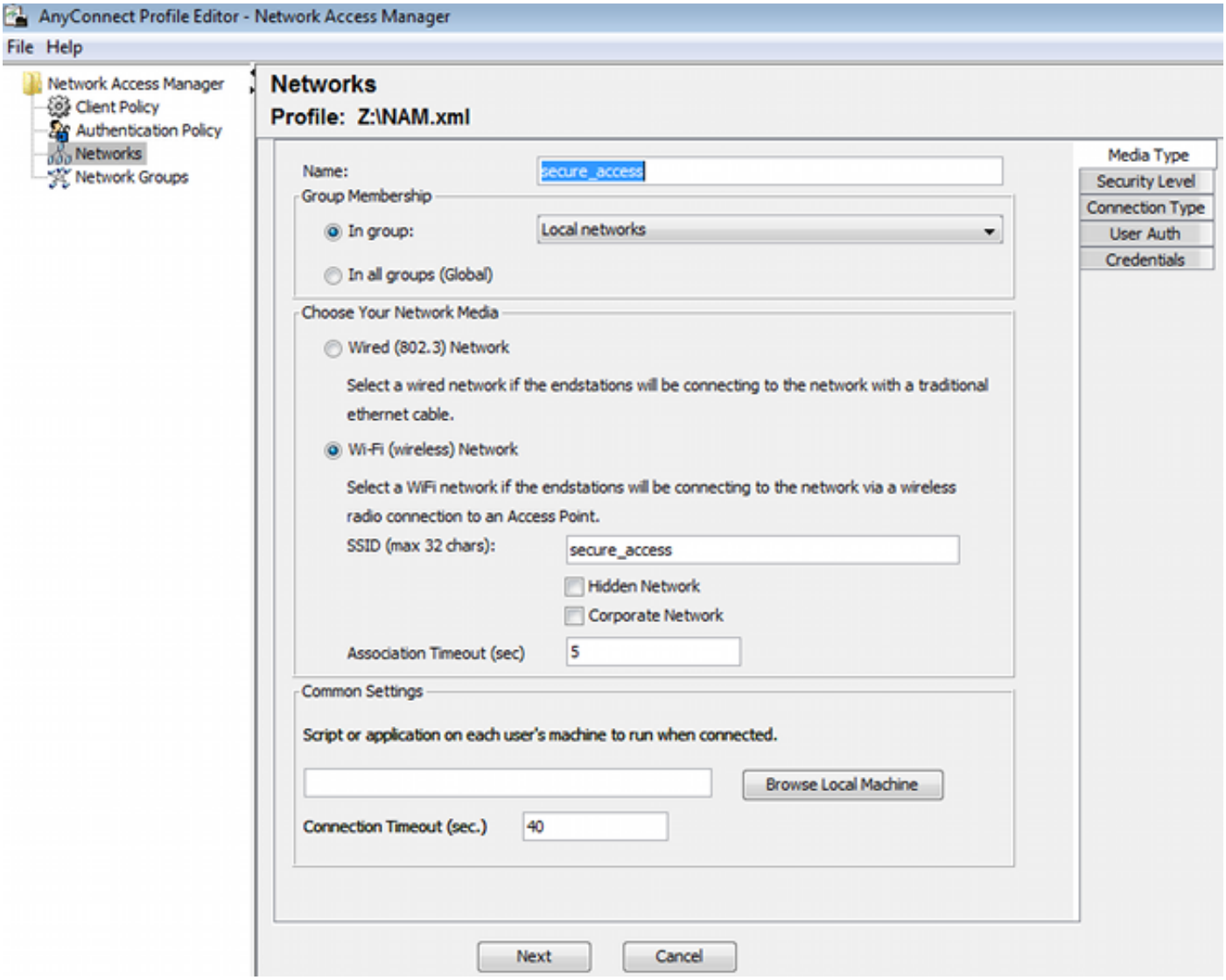
Configurez le profil VPN avec l'éditeur de profil d'AnyConnect pour le VPN.



Seulement une entrée a été ajoutée pour l'accès VPN. Sauf que fichier XML à **VPN.xml.**

Étape 3. Configurez le profil NAM

Configurez le profil NAM avec l'éditeur de profil d'AnyConnect pour NAM.



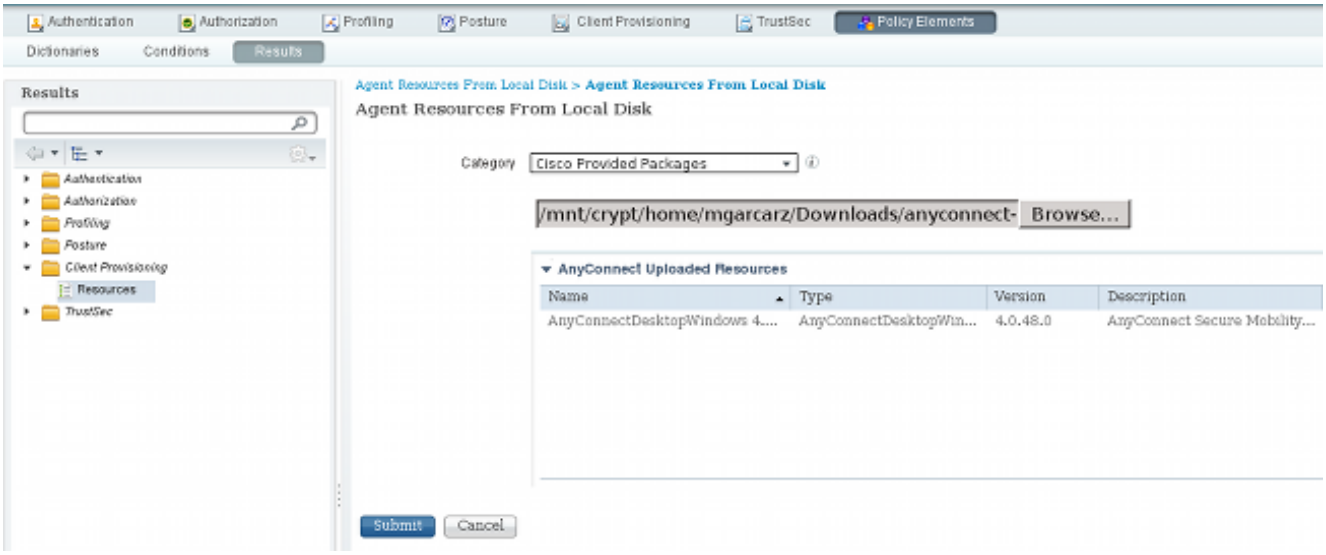
Seulement un SSID a été configuré : **secure_access**. Sauf que fichier XML à **NAM.xml.**

Étape 4. Installez l'application

1. Téléchargez l'application manuellement de Cisco.com.

   anyconnect-win-4.0.00048-k9.pkganyconnect-win-compliance-3.6.9492.2.pkg

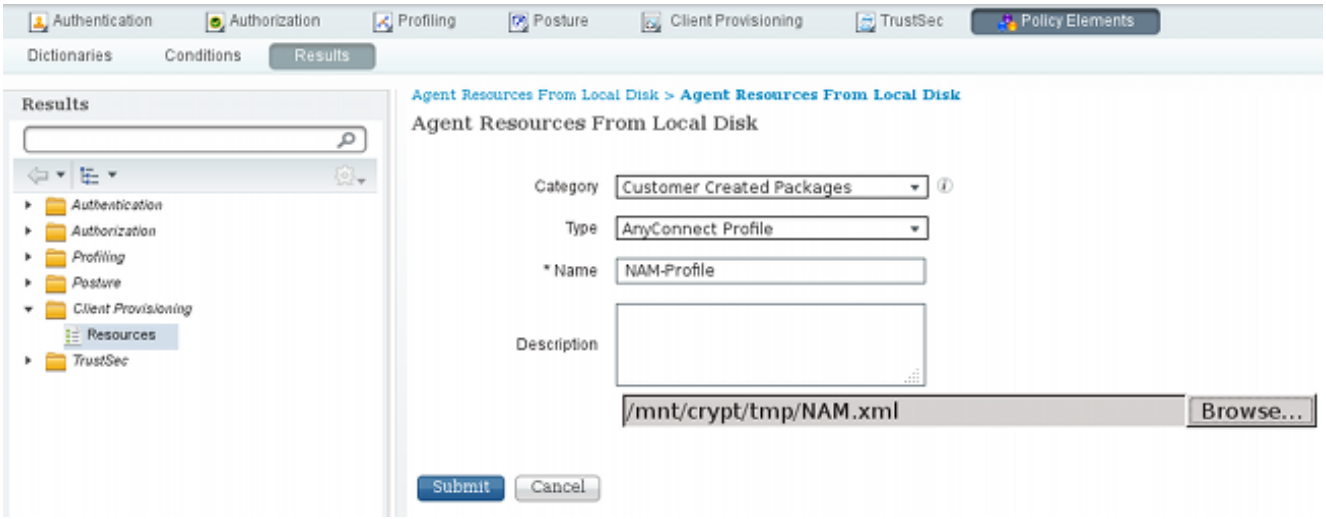
2. Sur ISE, naviguez vers la **stratégie > les résultats > le ravitaillement > les ressources de client**, et ajoutez les ressources en agent à partir du disque local.
3. Choisissez Cisco a fourni des modules et sélectionne l'**anyconnect-win-4.0.00048-k9.pkg** :



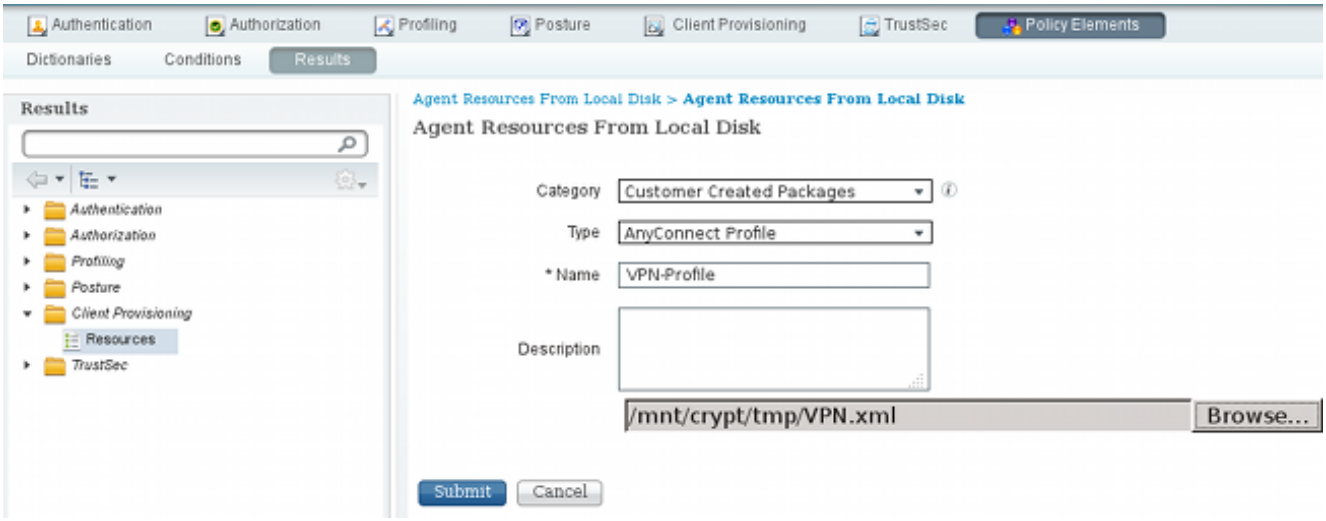
4. Répétez l'étape 4 pour le module de conformité.

Étape 5. Installez le profil VPN/NAM

1. Naviguez vers la **stratégie > les résultats > le ravitaillement > les ressources de client**, et ajoutez les ressources en agent à partir du disque local.
2. Choisissez les modules et le **profil d'AnyConnect** créés par client de type. Sélectionnez le profil précédemment créé NAM (fichier XML) :



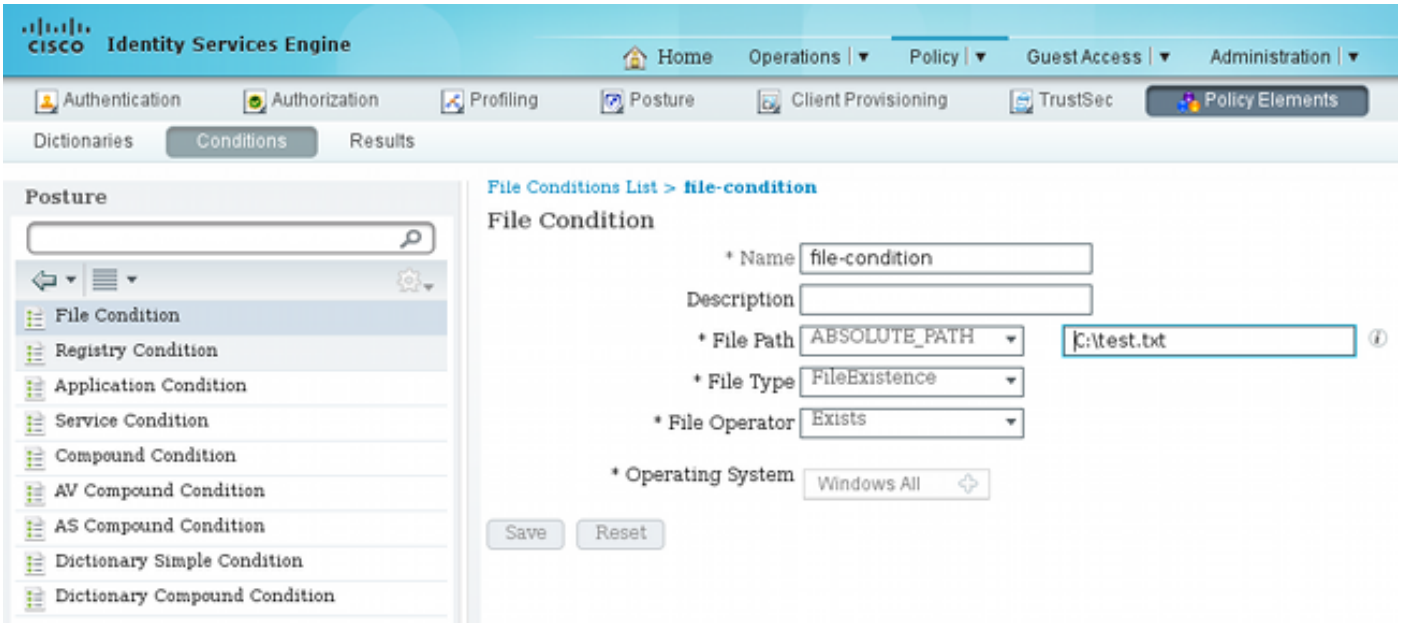
3. Étapes semblables de répétition pour le profil VPN :



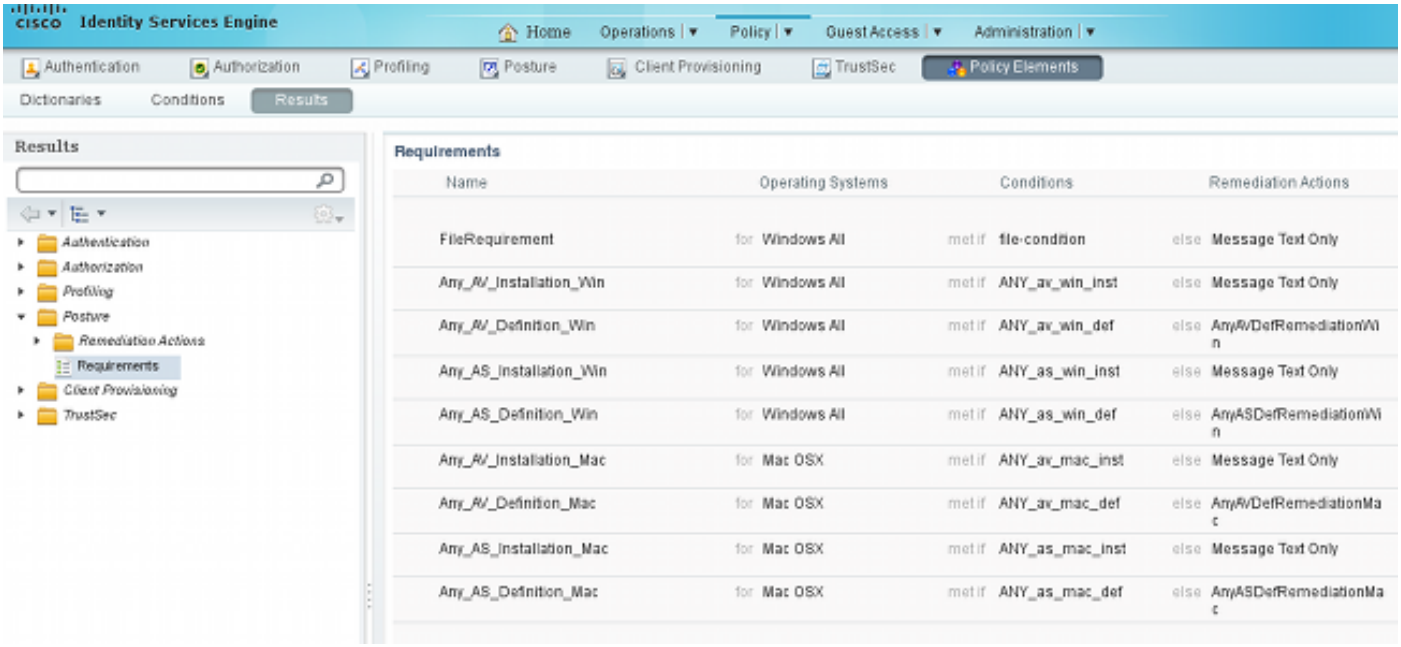
Étape 6. Configurez la posture

Des profils NAM et VPN doivent être configurés extérieurement avec l'éditeur de profil d'AnyConnect et être importés dans ISE. Mais la posture est saturée sur ISE.

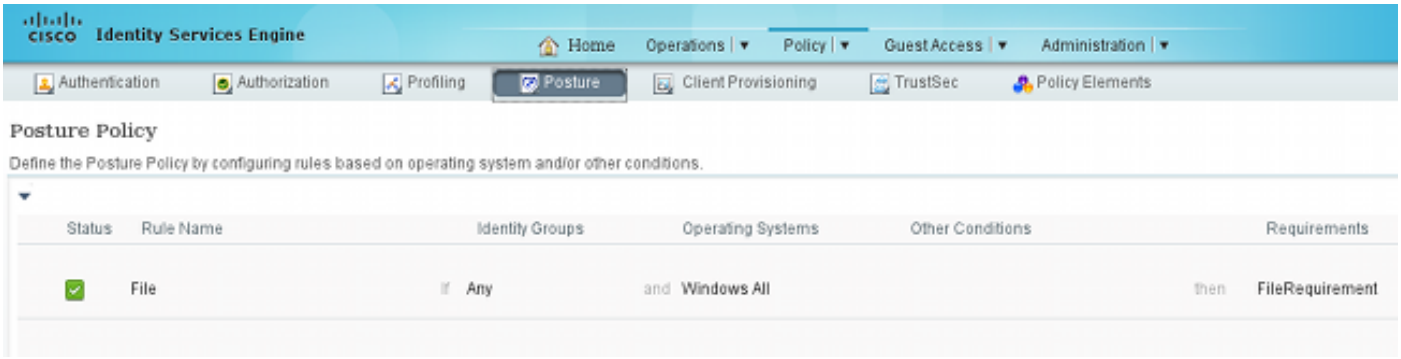
Naviguez vers la **stratégie > les conditions > la posture > le fichier Condition.You** peut voir qu'un état simple pour l'existence de fichier a été créé. Vous devez avoir ce fichier afin d'être conforme avec la stratégie vérifiée par le module de posture :



Cette condition est utilisée pour une condition requise :



Et la condition requise est utilisée dans la stratégie de posture pour des systèmes de Microsoft Windows :

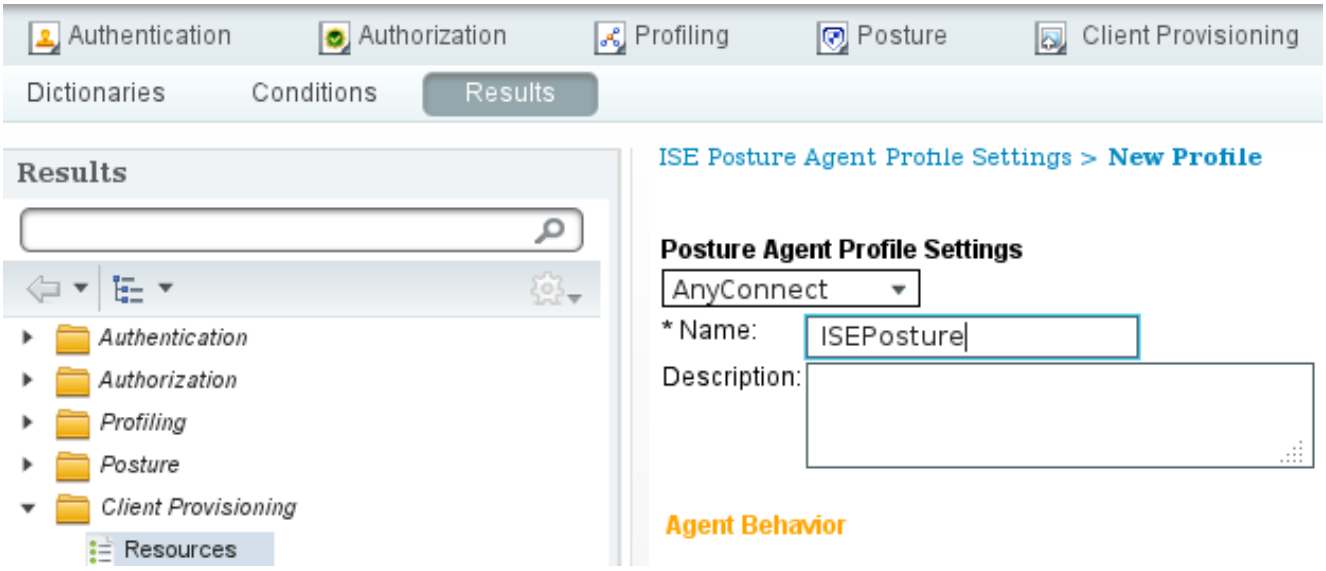


Pour plus d'informations sur la configuration de posture, référez-vous aux [services de posture sur le guide de configuration de Cisco ISE].

Une fois que la stratégie de posture est prête, il est temps d'ajouter la configuration d'agent intermédiaire.

1. Naviguez vers la **stratégie > les résultats > le ravitaillement > les ressources de client** et ajoutez le profil de posture d'agent de Contrôle d'admission au réseau (NAC) ou d'agent d'AnyConnect.

2. AnyConnect choisi (un nouveau module de posture de version 1.3 ISE a été utilisé au lieu du vieil agent NAC) :



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

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

4. Si le champ de règles de nom du serveur est parti vide, ISE ne sauvegarde pas des configurations et signale cette erreur :

```
Server name rules: valid value is required
```

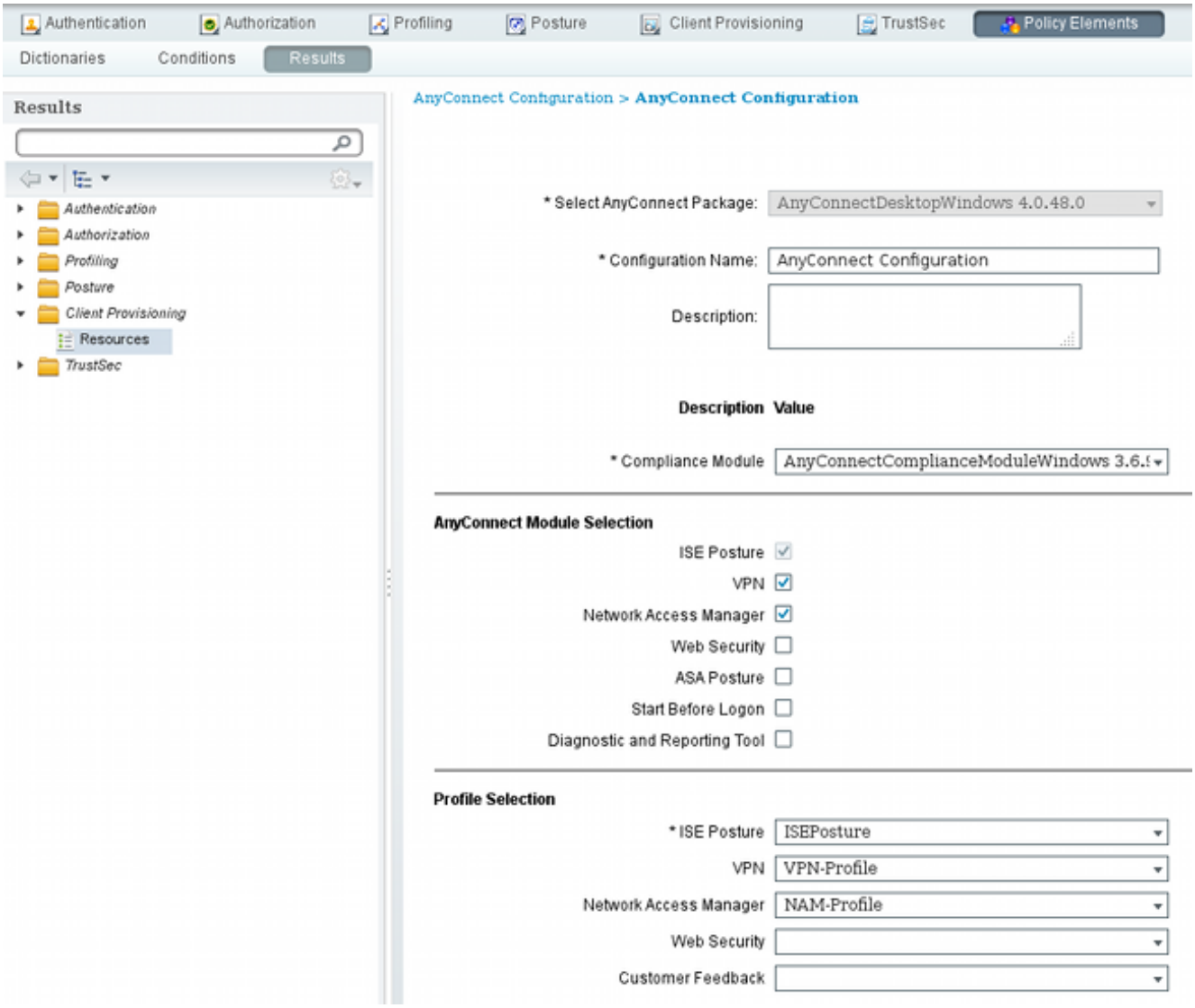
Étape 7. Configurez AnyConnect

Àce stade, toutes les applications (AnyConnect) et la configuration de profil pour tous les modules (VPN, NAM, et posture) ont été configurées. Il est temps de le lier ensemble.

1. Naviguez vers la **stratégie > les résultats > le ravitaillement > les ressources de client**, et ajoutez la configuration d'AnyConnect.

2. Configurez le nom et sélectionnez le module de conformité et tous modules requis d'AnyConnect (VPN, NAM, et posture).

3. Dans la sélection de profil, choisissez le profil configuré plus tôt pour chaque module.



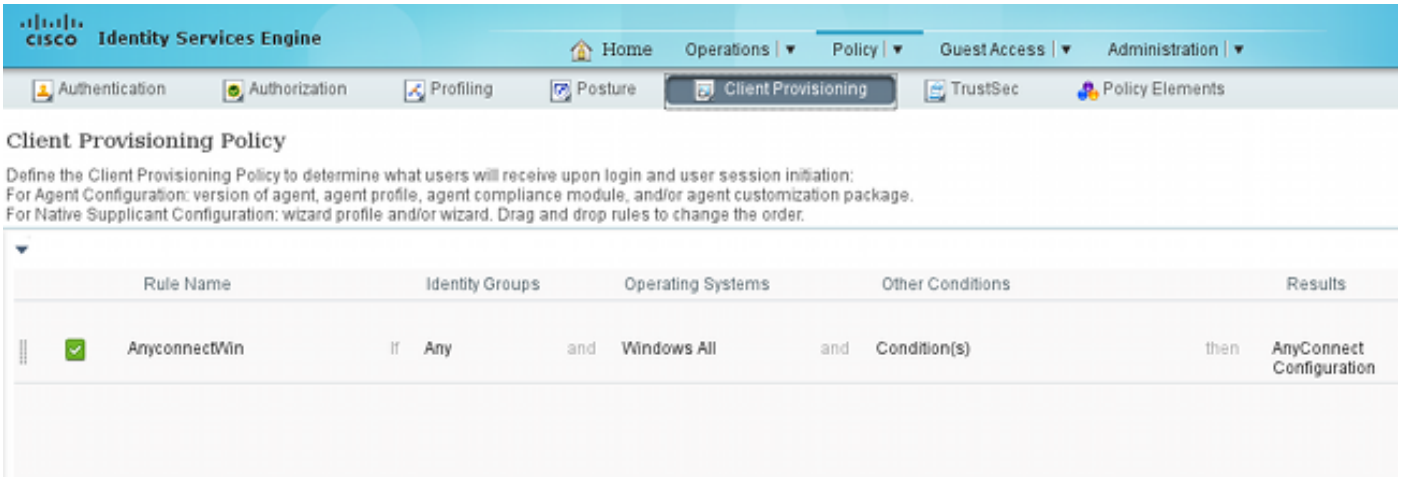
4. Il est obligatoire pour que tous autres modules fonctionnent le module VPN corrrectly. Même si le module VPN n'est pas sélectionné pour l'installation, il sera poussé et installé sur le client. Si vous ne voulez pas utiliser le VPN, il y a une possibilité pour configurer un profil spécial pour le VPN qui masque l'interface utilisateur pour le module VPN. Ces lignes devraient être ajoutées au **fichier VPN.xml :**

```
 <ClientInitialization>
<ServiceDisable>true</ServiceDisable>
</ClientInitialization>
```

5. Ce genre de profil est également installé quand vous utilisez **Setup.exe du** module ISO (anyconnect-win-3.1.06073-pre-deploy-k9.iso**).** Puis, le **profil** VPNDisable_ServiceProfile.xml pour le VPN est installé avec la configuration, qui désactive l'interface utilisateur pour le module VPN.

Étape 8. Règles de ravitaillement de client

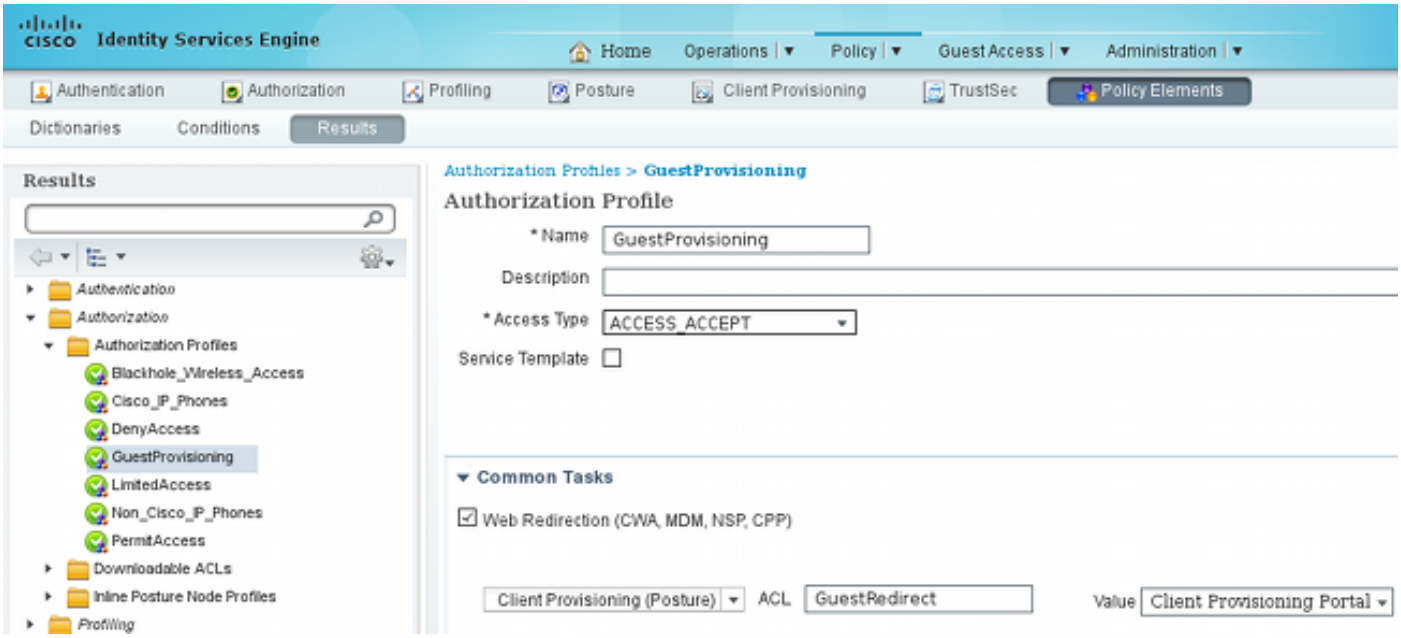
La configuration d'AnyConnect créée dans l'étape 7 devrait être mise en référence dans les règles de ravitaillement de client :



Les règles de ravitaillement de client décident quelle application sera poussée au client. Seulement une règle est nécessaire ici avec le résultat qui indique la configuration créée dans l'étape 7. De cette façon, tous les points finaux de Microsoft Windows qui sont réorientés pour le ravitaillement de client utilisera la configuration d'AnyConnect avec tous les modules et profils.

Étape 9. Profils d'autorisation

Le profil d'autorisation pour le ravitaillement de client doit être créé. Le portail par défaut de ravitaillement de client est utilisé :



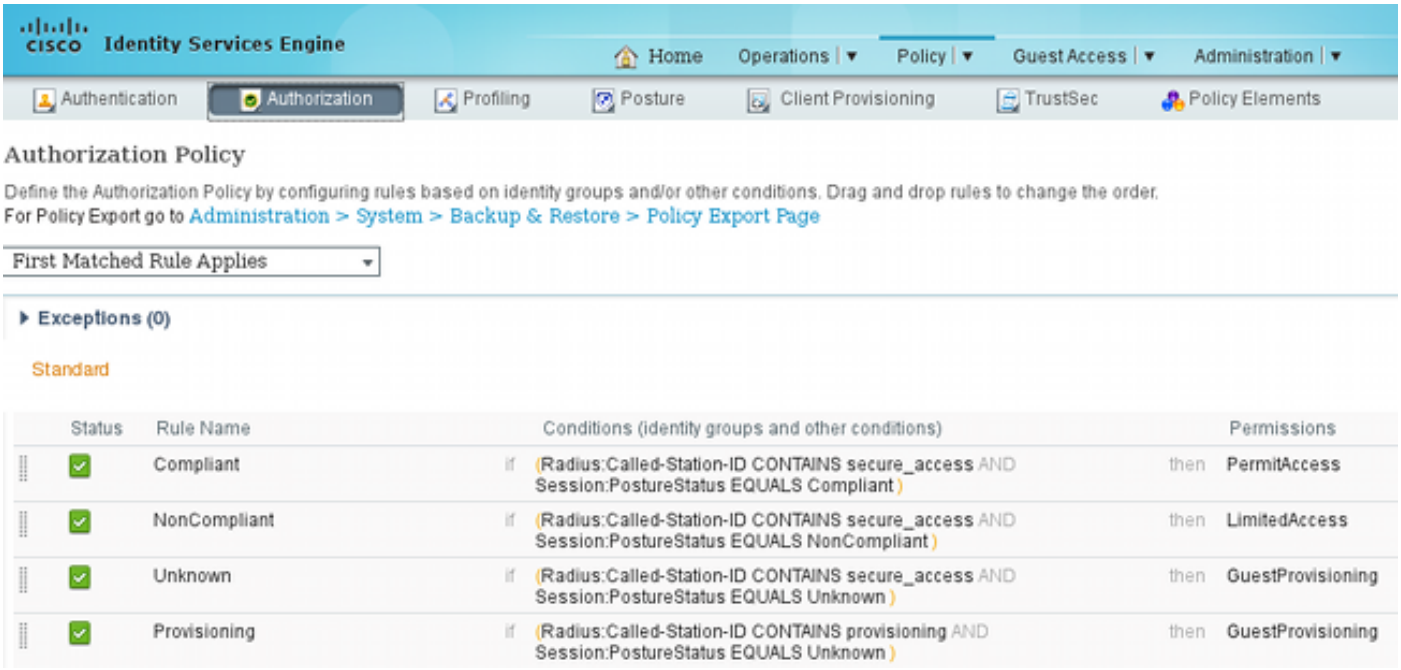
Ce profil force les utilisateurs à réorienter pour le ravitaillement au portail par défaut de ravitaillement de client. Ce portail évalue la stratégie de Provisiong de client (règles créées dans étape 8). Les profils d'autorisation sont les résultats des règles d'autorisation configurées dans l'étape 10.

La liste de contrôle d'accès de GuestRedirect (ACL) est le nom de l'ACL défini sur le WLC. Cet ACL décide ce que le trafic devrait être réorienté à ISE. Le pour en savoir plus, se rapportent à l'[authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine].

Il y a également un autre profil d'autorisation qui fournit l'accès au réseau limité (DACL) pour les utilisateurs non-conformes (appelés LimitedAccess).

Étape 10. Règles d'autorisation

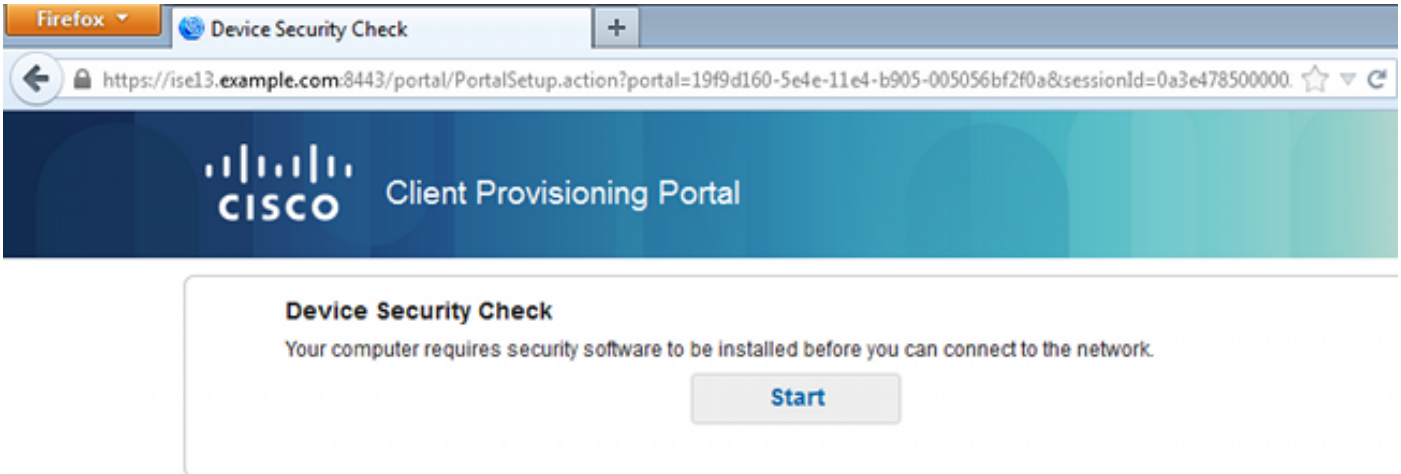
Tout ceux sont combinés dans quatre règles d'autorisation :



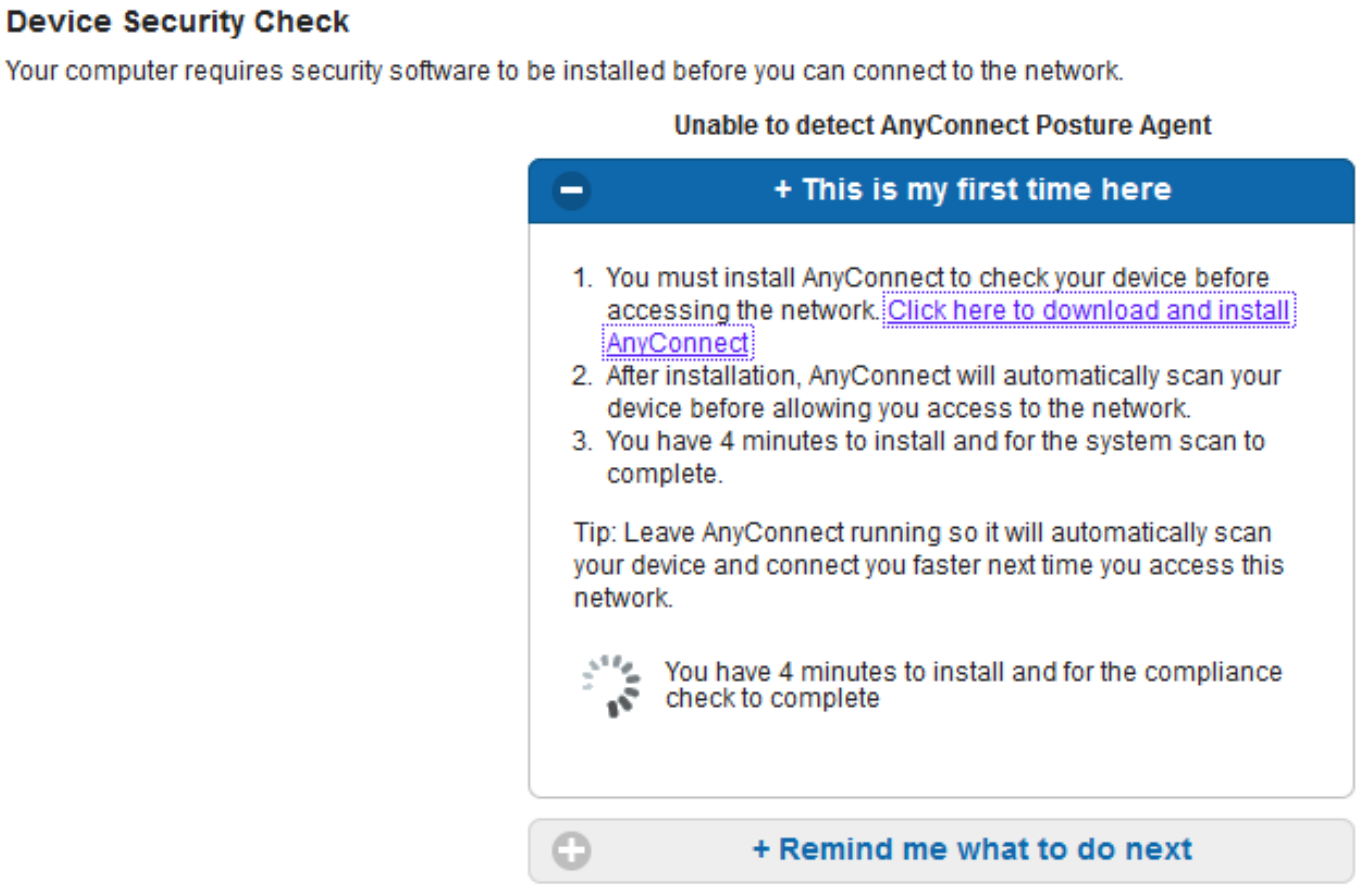
D'abord vous vous connectez au ravitaillement SSID et êtes réorienté pour le ravitaillement à un portail par défaut de ravitaillement de client (règle Provisioning Désigné). Une fois que vous vous connectez au **Secure_access** SSID, il réoriente toujours pour le ravitaillement si aucun état du module de posture n'est reçu par ISE (règle Unknown Désigné). Une fois que le point final est entièrement conforme, on accorde l'accès complet (nom de règle conforme). Si le point final est signalé comme non-conforme, il a limité l'accès au réseau (règle NonCompliant Désigné).

Vérifiez

Vous vous associez avec le ravitaillement SSID, essayez d'accéder à n'importe quelle page Web, et êtes réorienté au portail de ravitaillement de client :

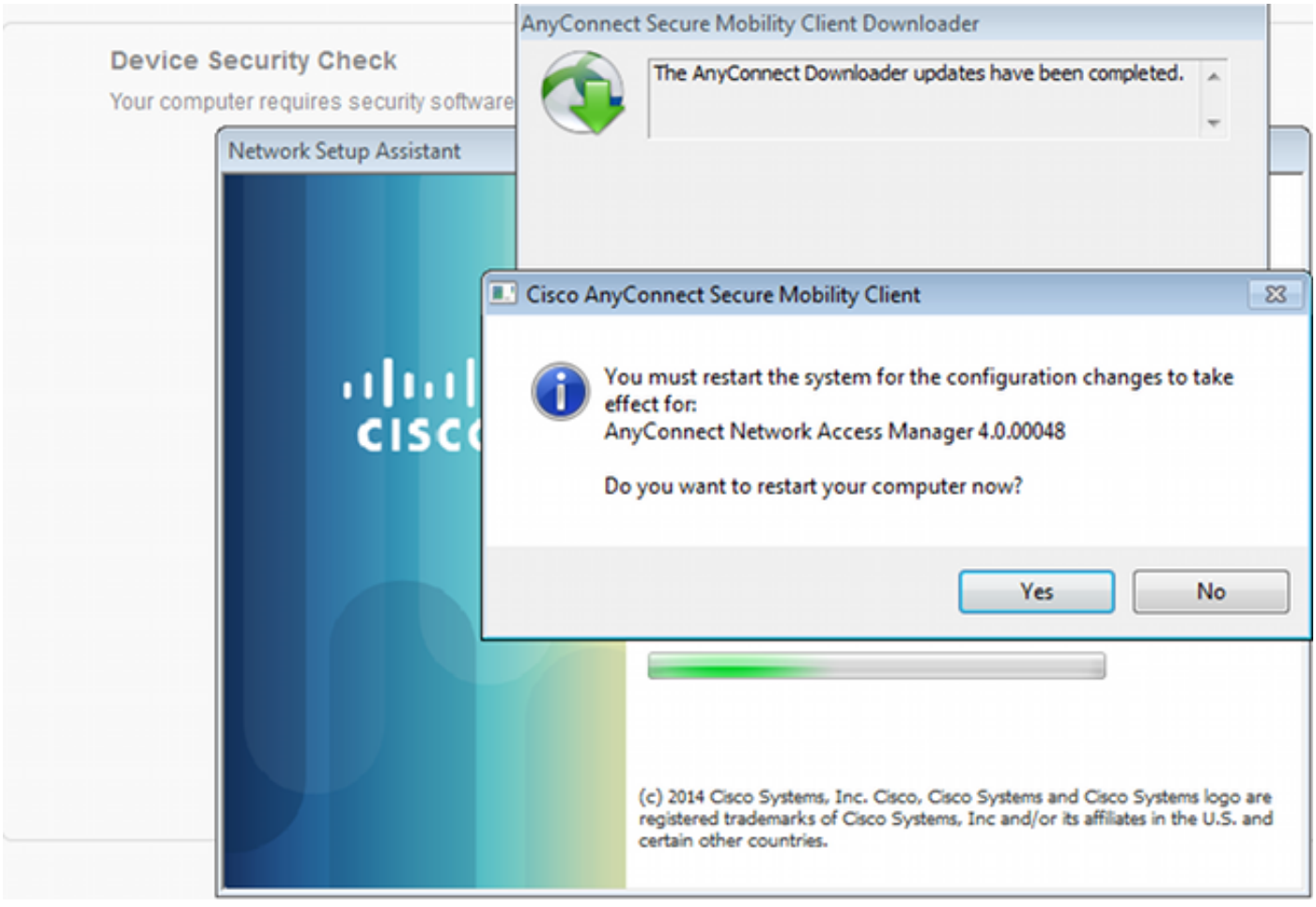


Puisqu'AnyConnect n'est pas détecté, vous êtes invité à l'installer :

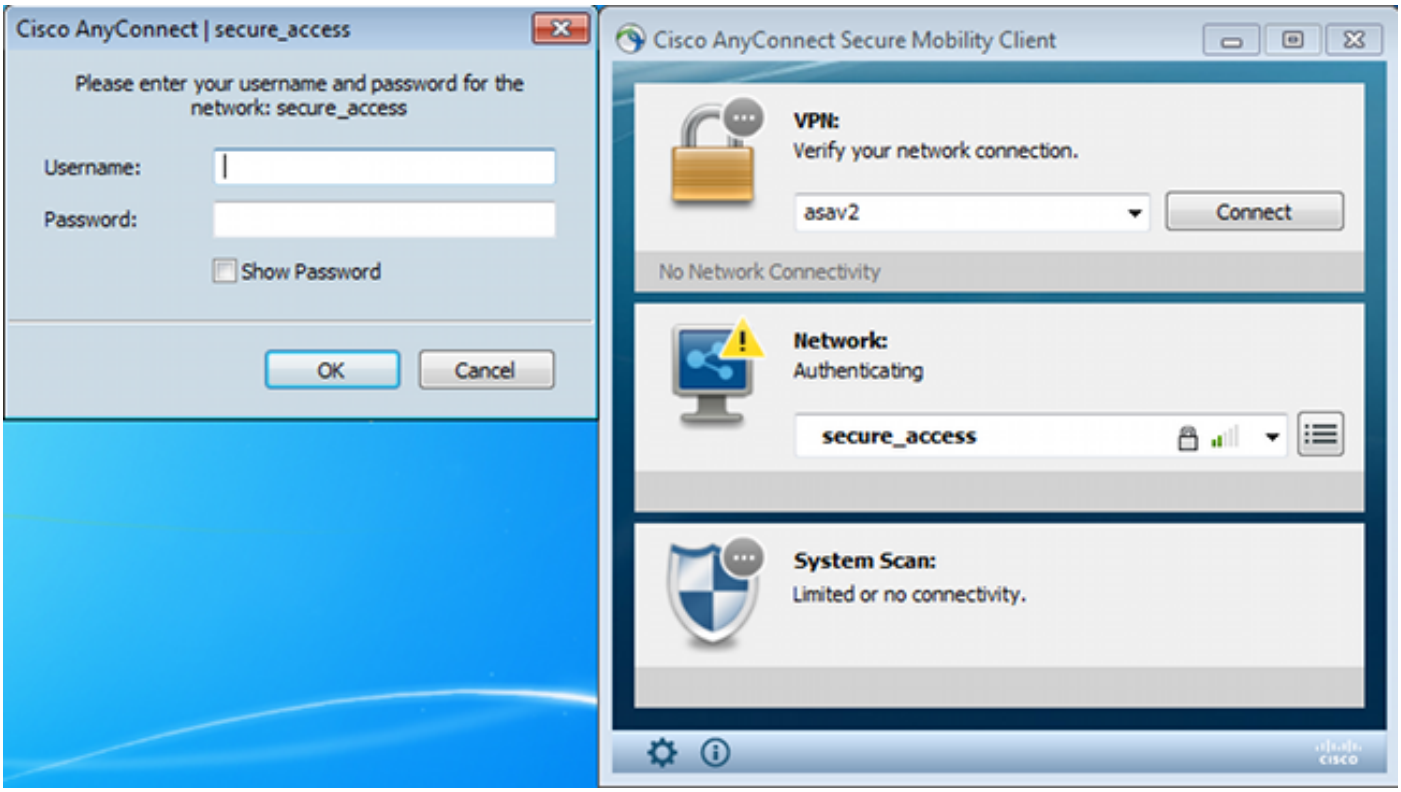


Un petit application a appelé l'assistant de configuration réseau, qui est responsable du processus d'installation entier, est téléchargé. Notez qu'il est différent que l'assistant de configuration réseau dans la version 1.2.

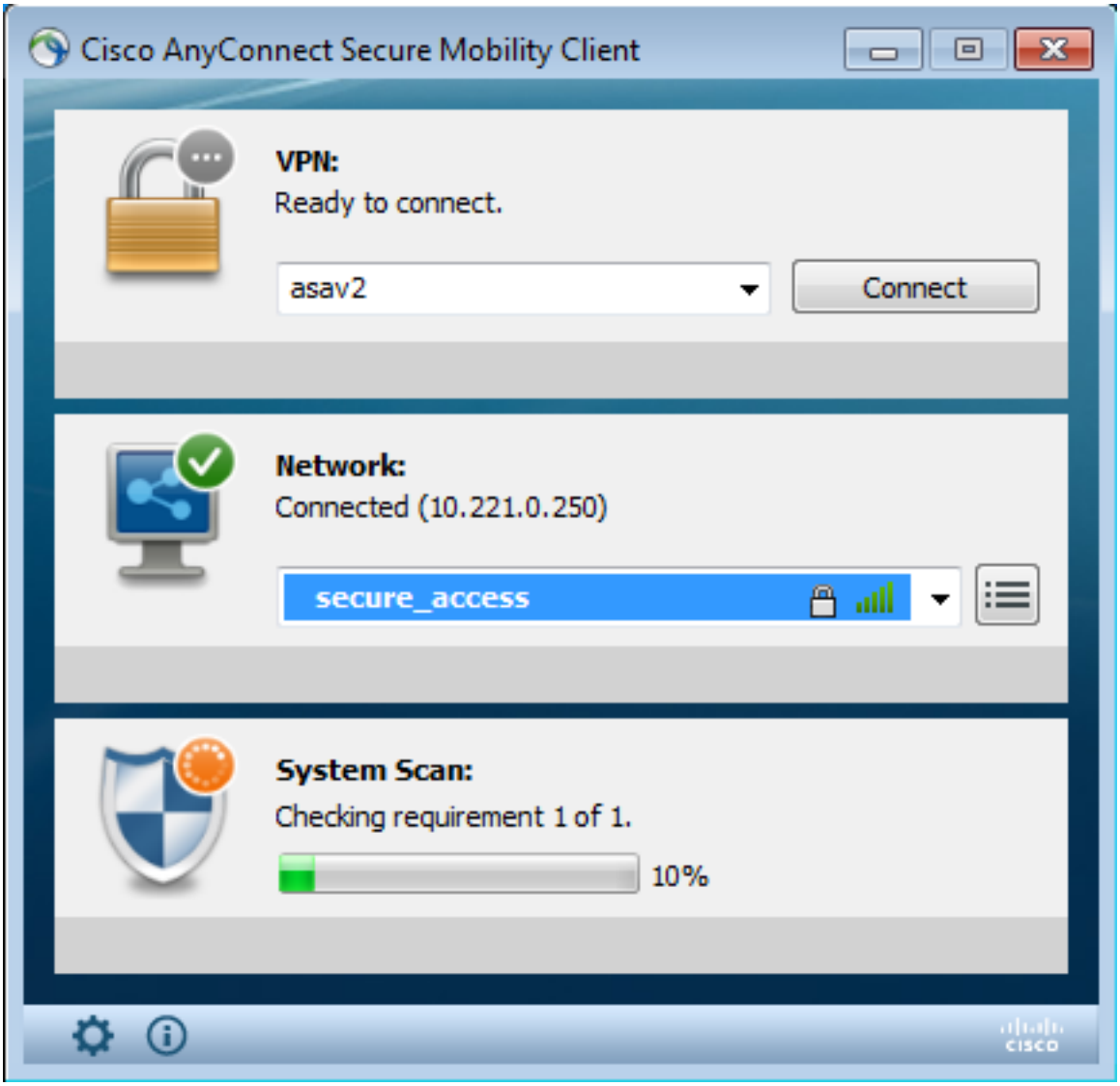
Tous les modules (VPN, NAM, et posture) sont installés et configurés. Vous devez redémarrer votre PC :



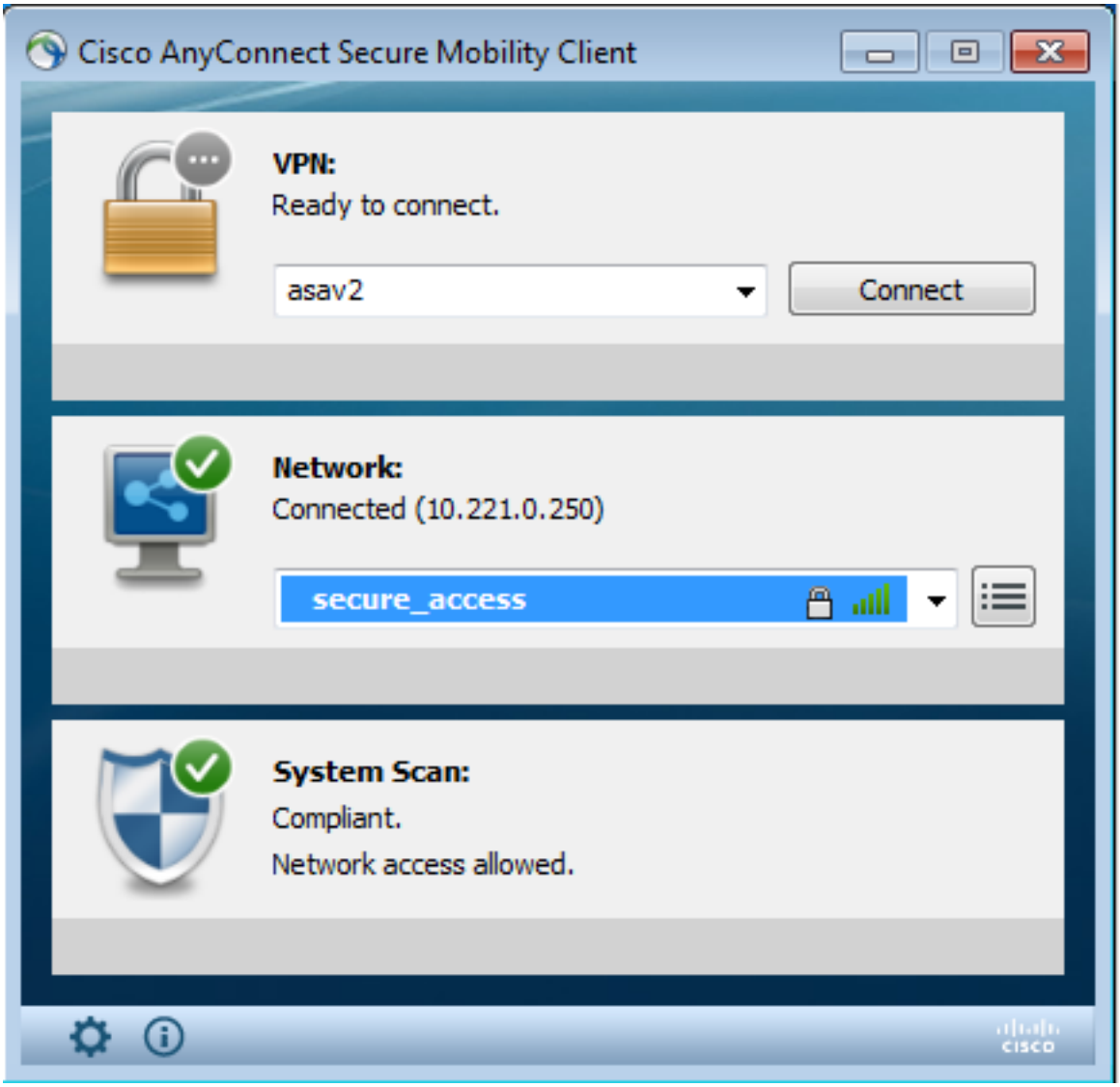
Après que la réinitialisation, AnyConnect soit automatiquement exécutée et essai NAM pour s'associer avec les secure_access SSID (selon le profil configuré). Notez que le profil VPN est correctement installé (entrée asav2 pour le VPN) :



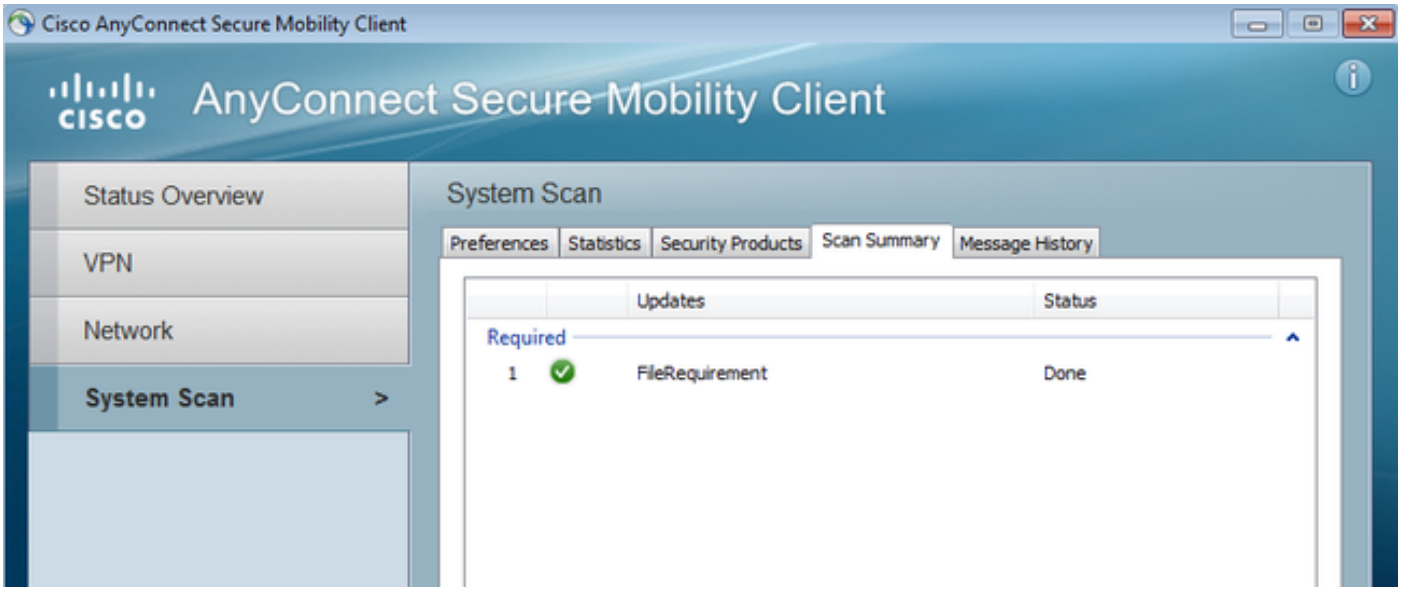
Après authentification, AnyConnect télécharge des mises à jour et pose également les règles pour lesquelles la vérification est exécutée :



Àce stade, il pourrait encore y avoir d'accès limité (vous rencontrez la règle inconnue d'autorisation sur ISE). Une fois que la station est conforme, cela est signalé par le module de posture :



Les détails peuvent être également vérifiés (le FileRequirement est satisfait) :

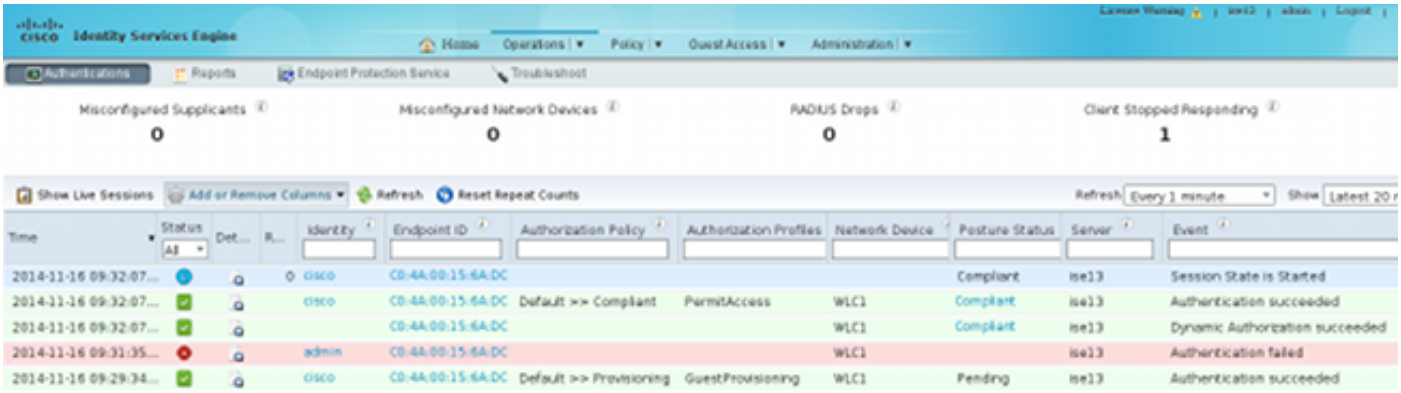


L'historique de message affiche les étapes détaillées :

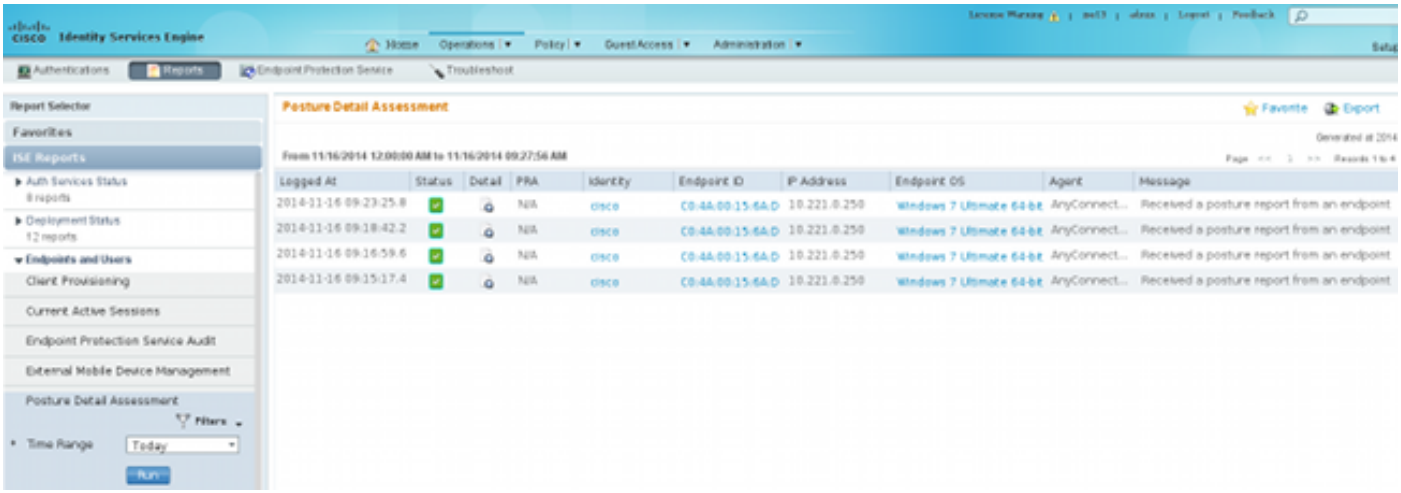
```
9:18:38 AM The AnyConnect Downloader is performing update checks...
9:18:38 AM Checking for profile updates...
9:18:38 AM Checking for product updates...
```

```
9:18:38 AM Checking for customization updates...
9:18:38 AM Performing any required updates...
9:18:38 AM The AnyConnect Downloader updates have been completed.
9:18:38 AM Update complete.
9:18:38 AM Scanning system ...
9:18:40 AM Checking requirement 1 of 1.
9:18:40 AM Updating network settings ...
9:18:48 AM Compliant.
```

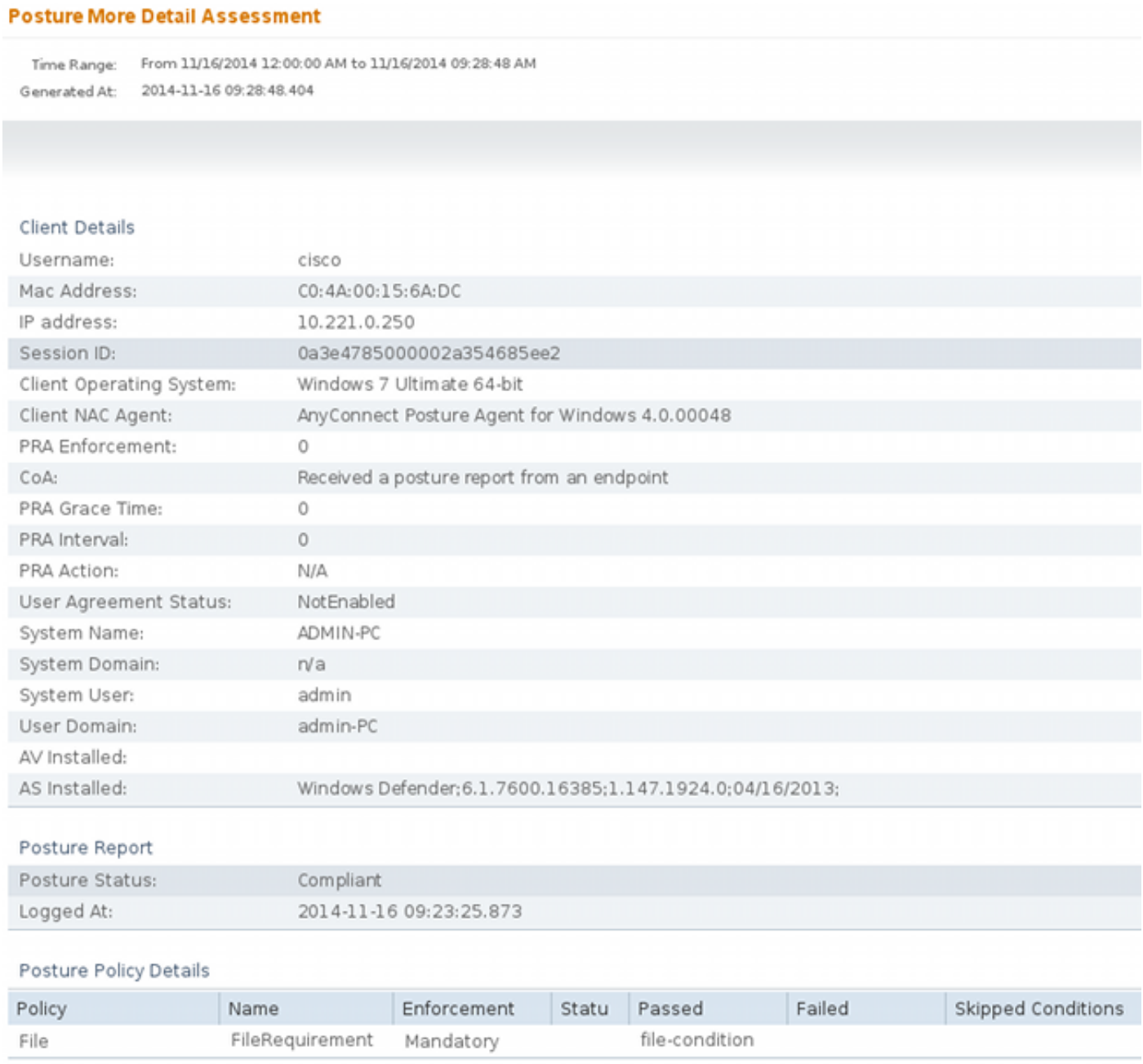
L'état réussi est envoyé à ISE, qui déclenche la modification de l'autorisation. La deuxième authentification rencontre la règle conforme et le plein accès au réseau est accordé. Si l'état de posture est envoyé tandis que toujours associé au ravitaillement SSID, ces logs sont vus sur ISE :



L'état de posture indique :



Les rapports détaillés affichent le FileRequirement qui est satisfait :



Posture More Detail Assessment

Time Range: From 11/16/2014 12:00:00 AM to 11/16/2014 09:28:48 AM
Generated At: 2014-11-16 09:28:48.404

Client Details

Username:	cisco
Mac Address:	C0:4A:00:15:6A:DC
IP address:	10.221.0.250
Session ID:	0a3e4785000002a354685ee2
Client Operating System:	Windows 7 Ultimate 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.0.00048
PRA Enforcement:	0
CoA:	Received a posture report from an endpoint
PRA Grace Time:	0
PRA Interval:	0
PRA Action:	N/A
User Agreement Status:	NotEnabled
System Name:	ADMIN-PC
System Domain:	n/a
System User:	admin
User Domain:	admin-PC
AV Installed:	
AS Installed:	Windows Defender;6.1.7600.16385;1.147.1924.0;04/16/2013;

Posture Report

Posture Status:	Compliant
Logged At:	2014-11-16 09:23:25.873

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
File	FileRequirement	Mandatory		file-condition		

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Services de posture sur le guide de configuration de Cisco ISE
- Guide d'administrateurs de Cisco ISE 1.3
- Support et documentation techniques - Cisco Systems