

# AnyConnect 4.0 Integratie met ISE versie 1.3

## Configuratievoorbeeld

### Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Topologie en stroom](#)

[Configureren](#)

[WLC](#)

[ISE](#)

[Stap 1. Voeg de WLC toe](#)

[Stap 2. Het VPN-profiel configureren](#)

[Stap 3. Het NAM-profiel configureren](#)

[Stap 4. Installeer de applicatie](#)

[Stap 5. Installeer het VPN/NAM-profiel](#)

[Stap 6. Instellen van de posterijen](#)

[Stap 7. Configureer AnyConnect](#)

[Stap 8. Clientprovisioningregels](#)

[Stap 9. Verificatieprofielen](#)

[Stap 10. Vergunningsregels](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

### Inleiding

Dit document beschrijft nieuwe functionaliteit in Cisco Identity Services Engine (ISE) versie 1.3 waarmee u meerdere AnyConnect Secure Mobility Client-modules kunt configureren en automatisch aan het eindpunt kunt leveren. Dit document presenteert hoe u VPN-, Network Access Manager (NAM)- en Postmodules op ISE kunt configureren en naar de zakelijke gebruiker kunt duwen.

### Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE-implementaties, verificatie en autorisatie
- Configuratie van draadloze LAN-controllers (WLC's)
- Basiskennis van VPN en 802.1x

- Configuratie van VPN- en NAM-profielen met AnyConnect-profielredacteuren

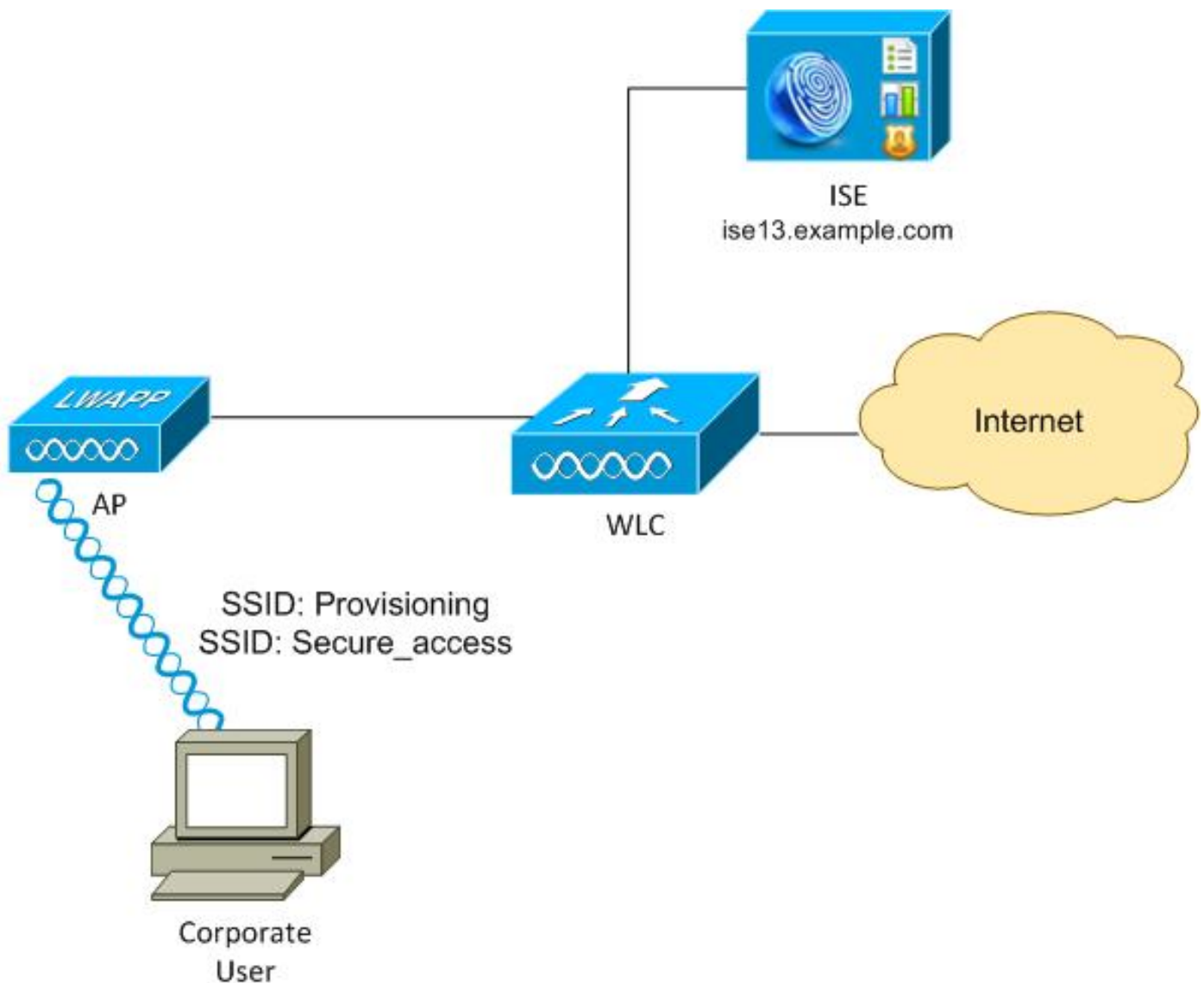
## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Cisco WLC versie 7.6 en hoger
- Cisco ISE-software, versie 1.3 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Topologie en stroom



Hier is de stroom:

**Stap 1** . Servicesinstellingen voor zakelijke gebruikers (SSID's): Provisioning. Voer 802.1x-verify uit met Extensible Authentication Protocol-Protected EAP (EAP-PEAP). De

vergunningsregel voor **provisioning** wordt op ISE aangetroffen en de gebruiker wordt opnieuw gericht op AnyConnect Provisioning (via het clientprovisioningprogramma). Als AnyConnect niet op de machine wordt gedetecteerd, worden alle geconfigureerde modules geïnstalleerd (VPN, NAM, Posture). Samen met dat profiel wordt de configuratie voor elke module geduwd.

**Stap 2** . Zodra AnyConnect is geïnstalleerd, moet de gebruiker de pc opnieuw opstarten. Na de herstart wordt AnyConnect uitgevoerd en de juiste SSID wordt automatisch gebruikt volgens het geconfigureerde NAM-profiel (Secure\_access). EAP-PEAP wordt gebruikt (als voorbeeld kan ook de beveiliging van de uitgebreide verificatieprotocol-transportlaag (EAP-TLS) worden gebruikt). Tegelijkertijd controleert de Postmodule of het station voldoet (controles op het bestaan van **c:\test.txt-bestand**).

**Stap 3**. Als de status van het station onbekend is (geen rapport van Postmodule), wordt het nog steeds opnieuw gericht op voorziening, omdat de **Onbekende** Auditregel op ISE is aangetroffen. Zodra het station compatibel is, stuurt ISE een Wijzigen van de Vergunning (CoA) naar de Draadloze LAN controller waardoor opnieuw verificatie wordt gestart. Een tweede authenticatie treedt op, en de **conformerende** regel wordt op ISE toegepast, die de gebruiker volledige toegang tot het netwerk zal geven.

Als resultaat hiervan is de gebruiker voorzien van AnyConnect VPN, NAM en Posture modules die Unified access to het netwerk mogelijk maken. Gelijkaardige functionaliteit kan worden gebruikt op de Adaptieve Security Appliance (ASA) voor VPN-toegang. Momenteel kan ISE hetzelfde doen voor elk type toegang met een zeer granulaire benadering.

Deze functionaliteit is niet beperkt tot zakelijke gebruikers, maar het is mogelijk het meest gebruikelijk om deze voor die groep gebruikers in te zetten.

## Configureren

### WLC

De WLC is ingesteld met twee SSID's:

- Provisioning - [WAP + WAP2][Auth(802.1X)]. Deze SSID wordt gebruikt voor AnyConnect-provisioning.
- Secure\_access - [WAP + WAP2][Auth(802.1X)]. Deze SSID wordt gebruikt voor beveiligde toegang nadat het eindpunt met de NAM module is bevoorrad die voor die SSID is ingesteld.

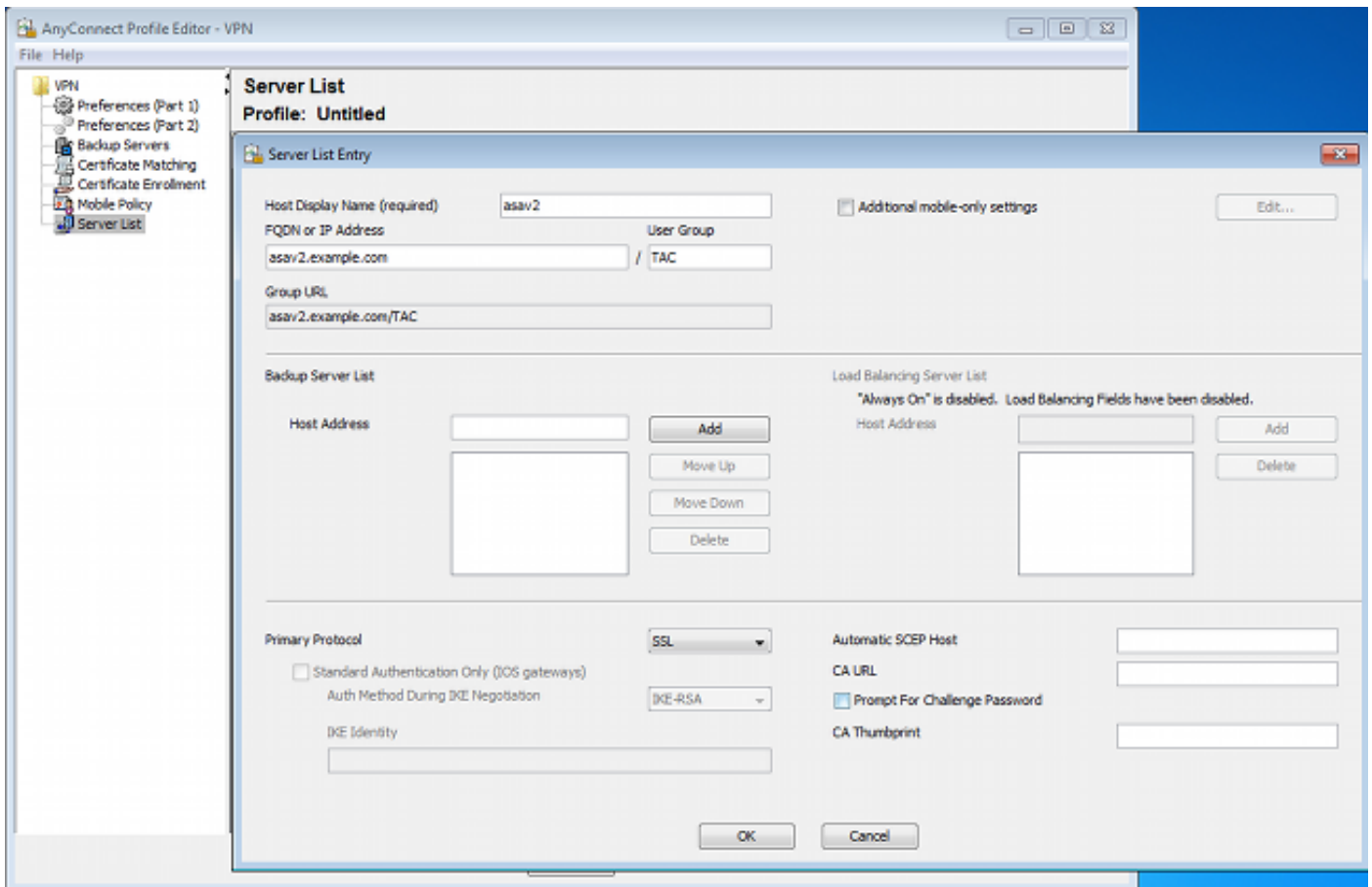
### ISE

#### Stap 1. Voeg de WLC toe

Voeg de WLC aan het Netwerkkapparaat in ISE toe.

#### Stap 2. Het VPN-profiel configureren

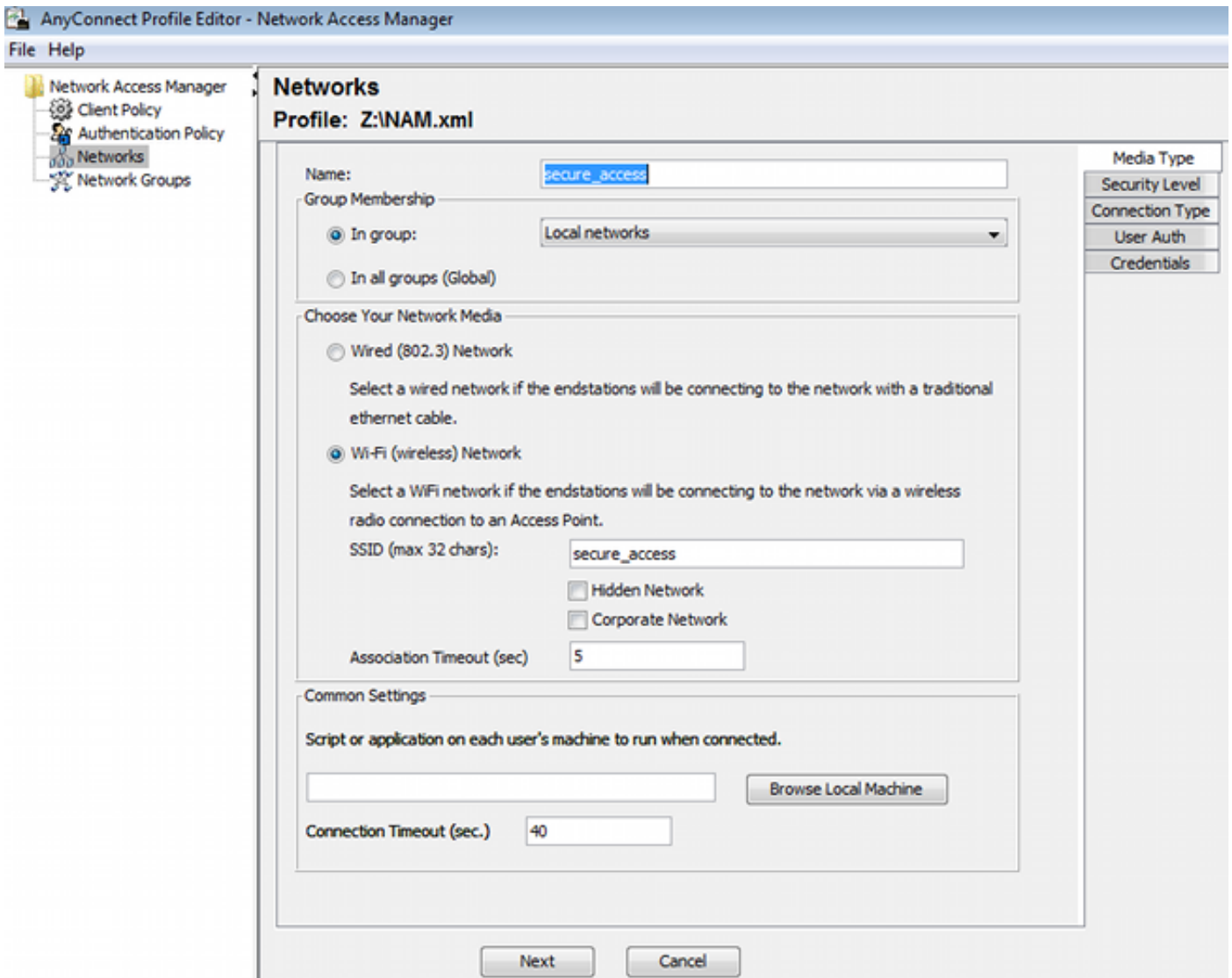
Configureer het VPN-profiel met de AnyConnect Profile Editor voor VPN.



Er is slechts één ingang toegevoegd voor VPN-toegang. Sla dat XML-bestand op in **VPN.xml**.

### Stap 3. Het NAM-profiel configureren

Configureer het NAM-profiel met de AnyConnect Profile Editor voor NAM.



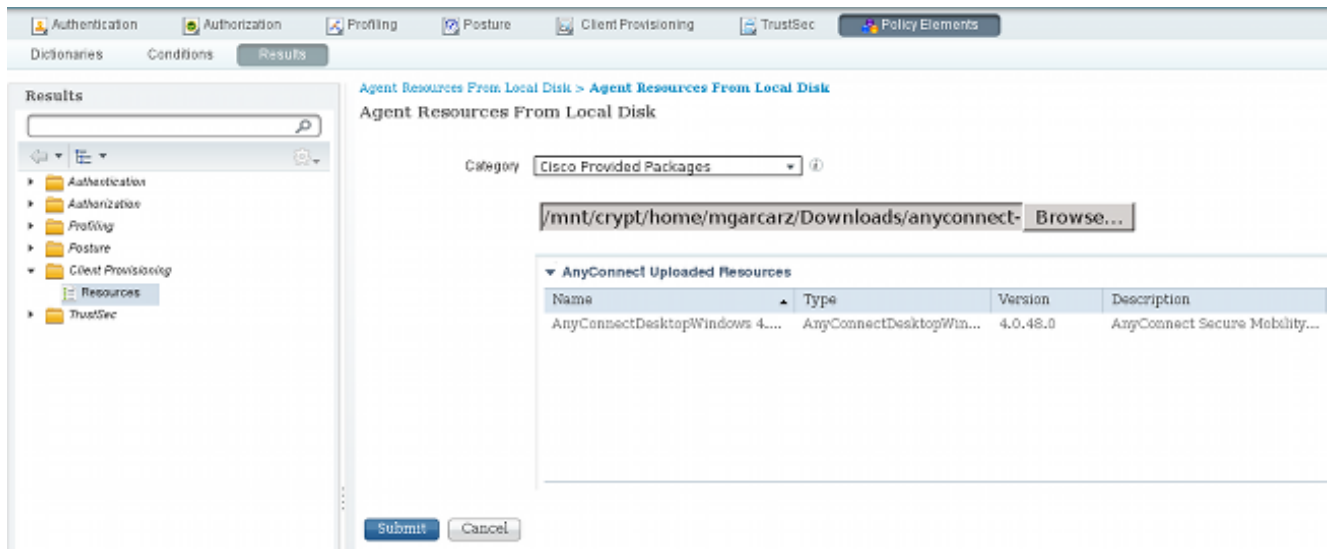
Slechts één SSID is geconfigureerd: **Secure\_access**. Sla dat XML-bestand op in **NAM.xml**.

#### Stap 4. Installeer de applicatie

1. Download de toepassing handmatig van Cisco.com.

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

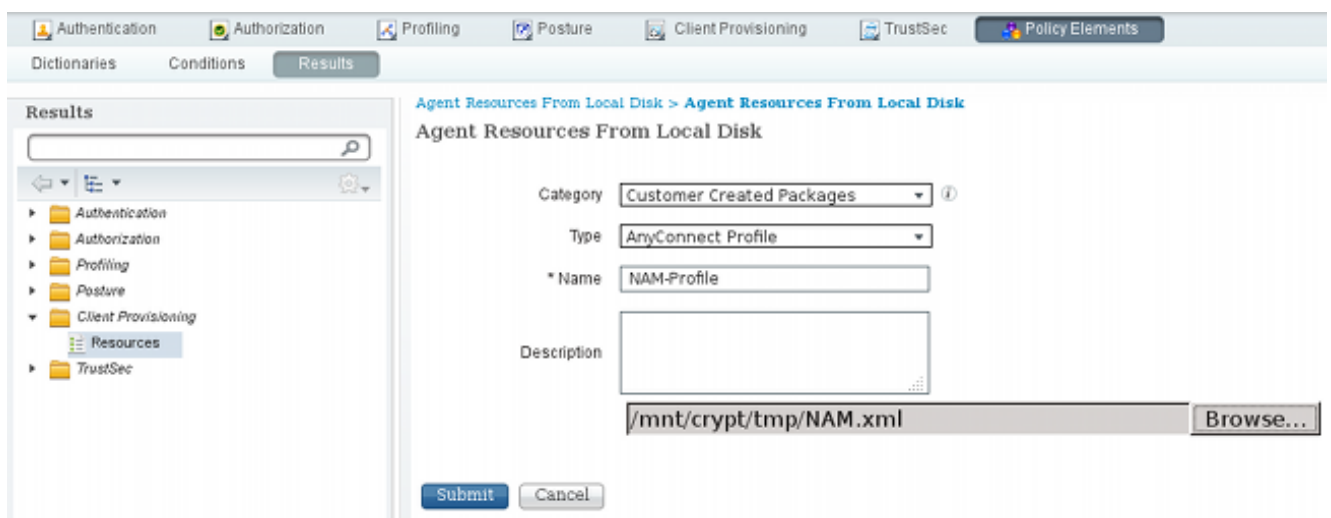
2. Op ISE, navigeer naar **Beleid > Resultaten > Clientprovisioning > Resources**, en voeg Agent Resources van lokale schijf toe.
3. Kies Cisco Provided Packages en selecteer de **anyconnect-win-4.0.0048-k9.pkg**:



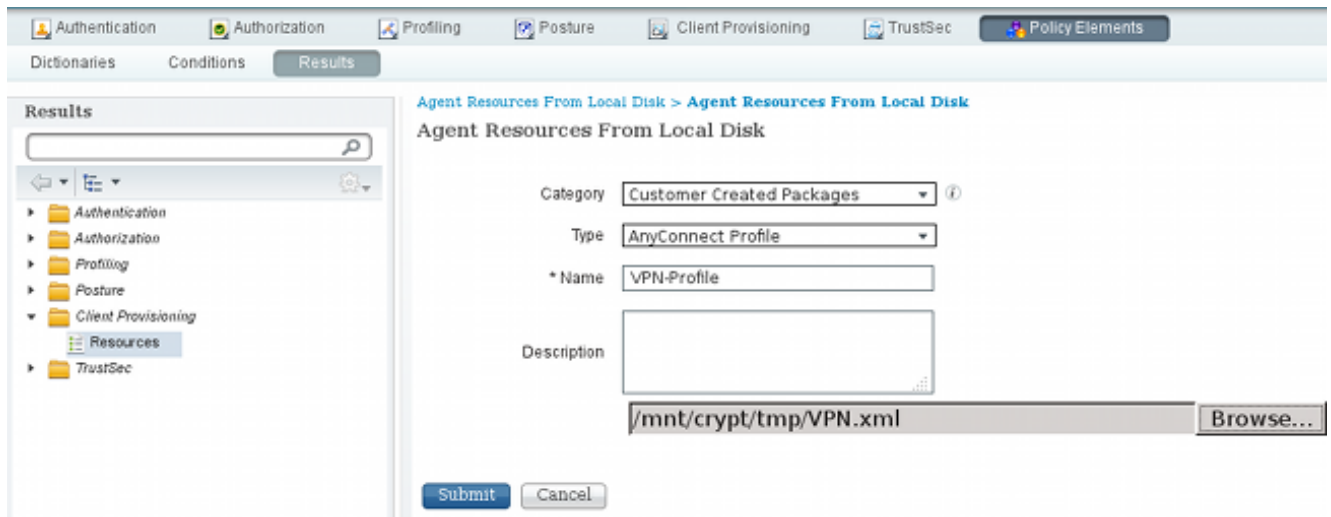
4. Herhaal stap 4 voor de nalevingsmodule.

### Stap 5. Installeer het VPN/NAM-profiel

1. Navigeer naar **beleid > Resultaten > Clientprovisioning > Resources** en voeg Agent Resources uit lokale schijf toe.
2. Kies de klant gemaakte pakketten en type **AnyConnect Profile**. Selecteer het eerder gemaakte NAM profiel (XML bestand):



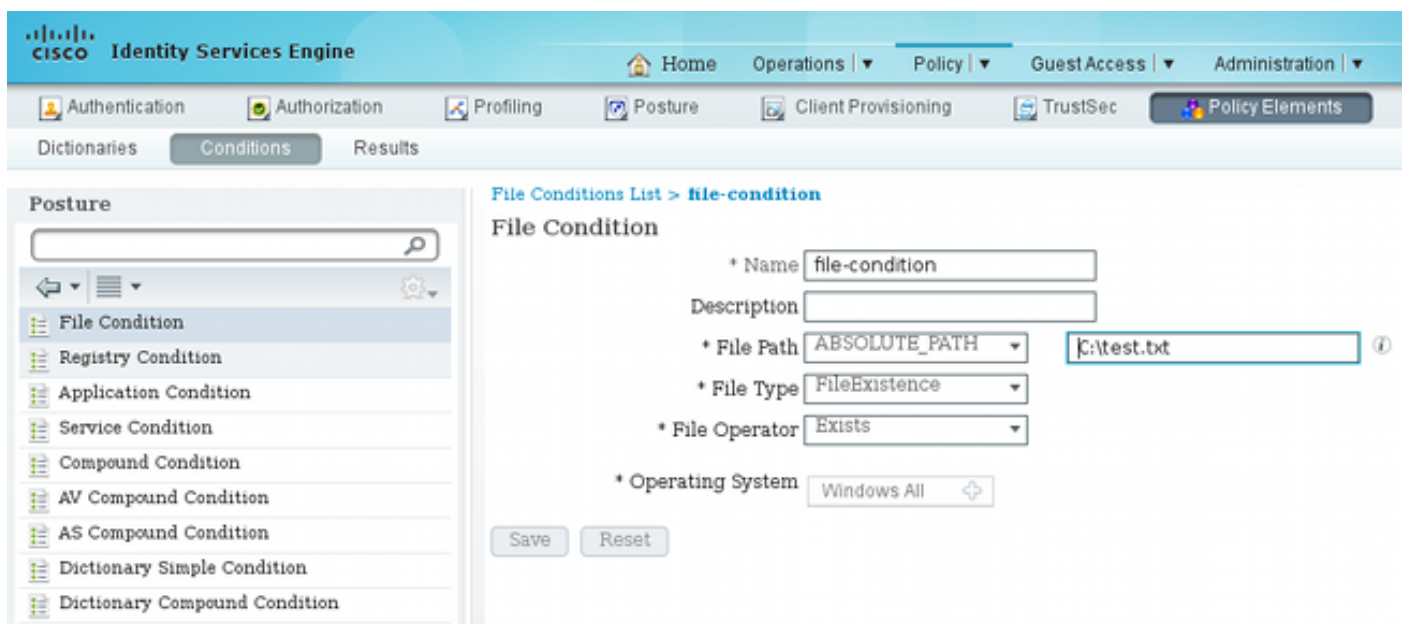
3. Herhaal soortgelijke stappen voor het VPN-profiel:



## Stap 6. Instellen van de posterijen

NAM- en VPN-profielen moeten extern met de AnyConnect-profieleditor worden geconfigureerd en in ISE worden geïmporteerd. Maar de Posture is volledig ingesteld op ISE.

Navigeer naar **beleid > Voorwaarden > Post > File Condition**. U kunt zien dat er een eenvoudige voorwaarde voor het bestaan van bestanden is gemaakt. U moet over dat bestand beschikken om te voldoen aan het door de Postmodule geverifieerde beleid:



Deze voorwaarde wordt gebruikt voor een vereiste:

Name	Operating Systems	Conditions	Remediation Actions
FileRequirement	for Windows All	met if file-condition	else Message Text Only
Any_AV_Installation_Win	for Windows All	met if ANY_av_win_inst	else Message Text Only
Any_AV_Definition_Win	for Windows All	met if ANY_av_win_def	else AnyAVDefRemediationWin
Any_AS_Installation_Win	for Windows All	met if ANY_as_win_inst	else Message Text Only
Any_AS_Definition_Win	for Windows All	met if ANY_as_win_def	else AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	met if ANY_av_mac_inst	else Message Text Only
Any_AV_Definition_Mac	for Mac OSX	met if ANY_av_mac_def	else AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	met if ANY_as_mac_inst	else Message Text Only
Any_AS_Definition_Mac	for Mac OSX	met if ANY_as_mac_def	else AnyASDefRemediationMac

En deze eis wordt gebruikt in het Posture-beleid voor Microsoft Windows-systemen:

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
✓	File	if Any	and Windows All		then FileRequirement

Raadpleeg voor meer informatie over de configuratie van de [posterijen](#) de [posteringservices van Cisco ISE Configuration Guide](#).

Zodra het Postbeleid klaar is, is het tijd om de configuratie van de Postmachine toe te voegen.

1. Navigeren in op **beleid > Resultaten > Clientprovisioning > Resources** en netwerktoegangscontrole (NAC) Agent of AnyConnect Agent Posture Profile.
2. Selecteer AnyConnect (er is een nieuwe Postmodule van ISE versie 1.3 gebruikt in plaats van de oude NAC Agent):



3. Vergeet niet om in het gedeelte Posture Protocol \* toe te voegen zodat de Agent een verbinding kan maken met alle servers.

#### Posture Protocol

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

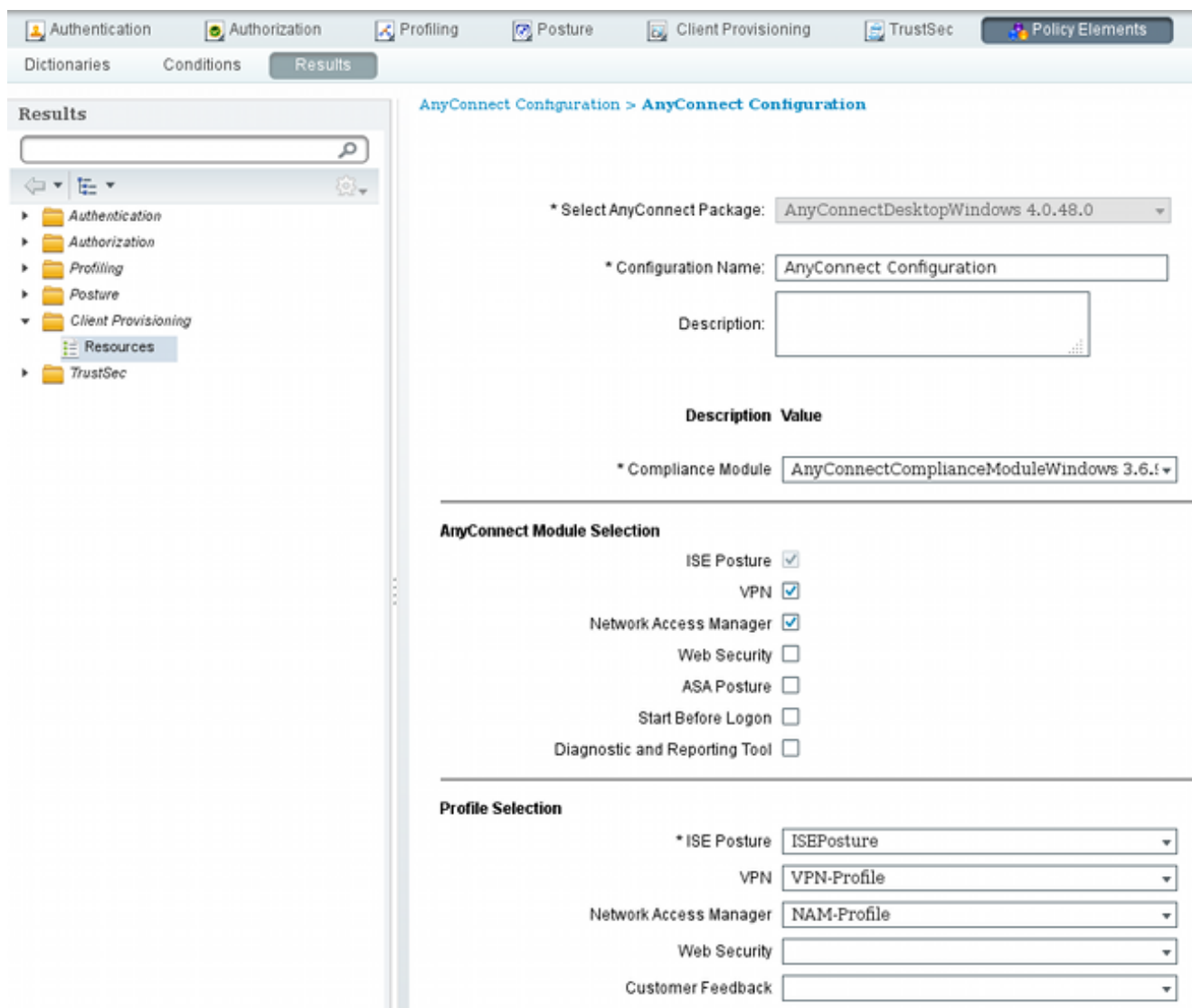
4. Als het veld servernaam leeg is, slaat ISE geen instellingen op en rapporteert u deze fout:

Server name rules: valid value is required

## Stap 7. Configureer AnyConnect

In deze fase zijn alle toepassingen (AnyConnect) en de profielconfiguratie voor alle modules (VPN, NAM en Posture) geconfigureerd. Het is tijd om het samen te binden.

1. Navigeer in op **beleid > Resultaten > Clientprovisioning > Resources** en voeg AnyConnect-configuratie toe.
2. Configuratie van de naam en selecteer de nalevingsmodule en alle vereiste modules van AnyConnect (VPN, NAM, en Posture).
3. Kies in de selectie van het profiel het profiel dat eerder voor elke module is ingesteld.



4. De VPN module is verplicht voor alle andere modules om correct te functioneren. Zelfs als de VPN-module niet is geselecteerd voor installatie, wordt deze op de client geduwd en geïnstalleerd. Als u VPN niet wilt gebruiken, is er een mogelijkheid om een speciaal profiel voor VPN te configureren dat de gebruikersinterface voor de VPN-module verbergt. Deze regels moeten worden toegevoegd aan het bestand **VPN.xml**:

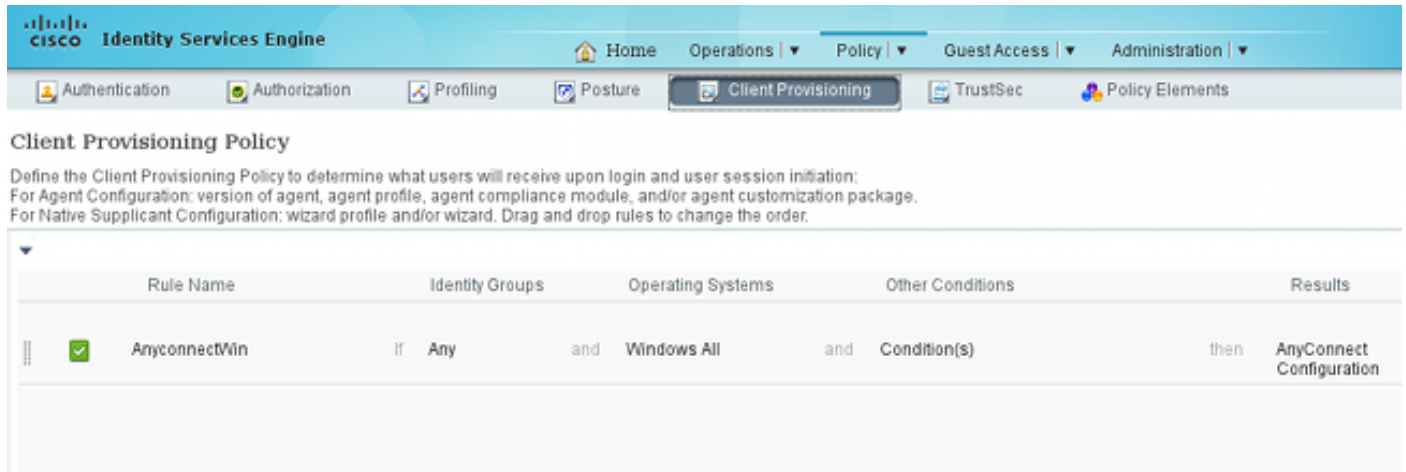
```
<ClientInitialization>
```

```
</ClientInitialization>
```

5. Dit type profiel wordt ook geïnstalleerd wanneer u **Setup.exe** gebruikt van het iso-pakket (**anyconnect-win-3.1.06073-pre-implementatie-k9.iso**). Vervolgens wordt het profiel **VPNDisable\_ServiceProfile.xml** samen met de configuratie geïnstalleerd, dat de gebruikersinterface voor de VPN-module schakelt.

## Stap 8. Clientprovisioningregels

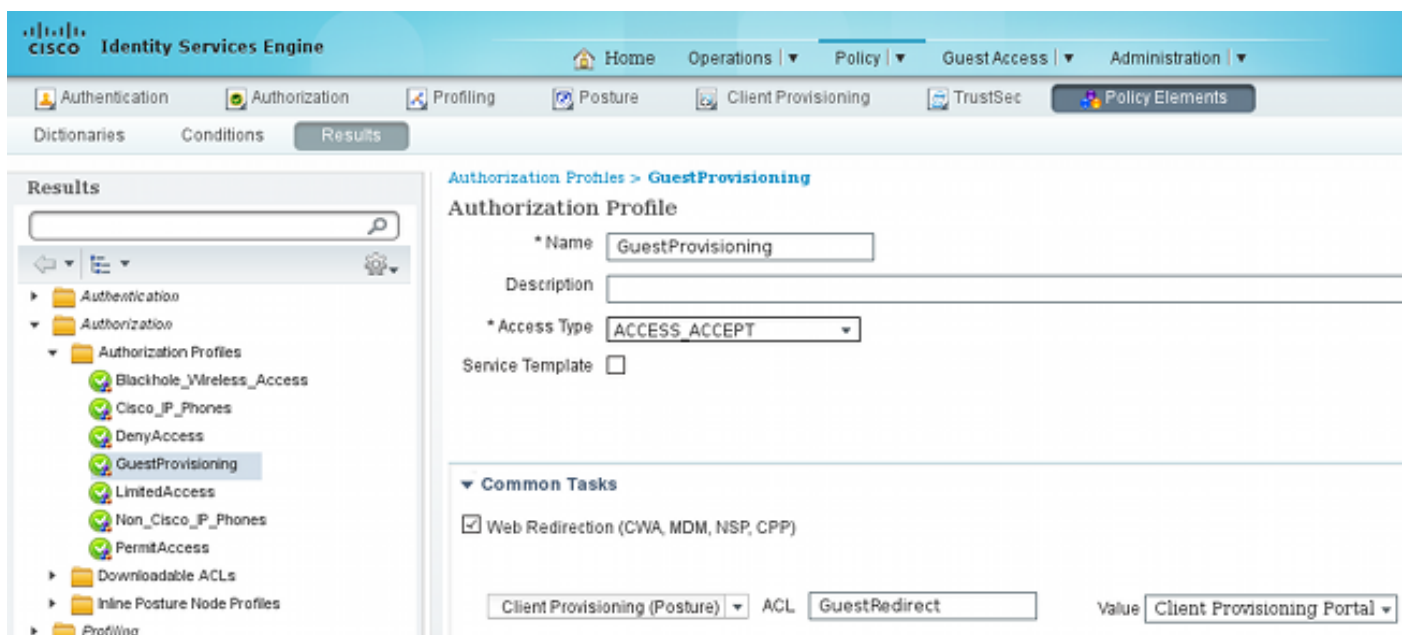
De AnyConnect-configuratie die in Stap 7 is gemaakt, moet in de regels voor clientprovisioning worden vermeld:



Regels voor clientprovisioning bepalen welke toepassing naar de client wordt geduwd. Hier is slechts één regel nodig met het resultaat dat verwijst naar de configuratie die in Stap 7 is gemaakt. Op deze manier zullen alle Microsoft Windows-endpoints die voor clientprovisioning zijn omgeleid, de AnyConnect-configuratie gebruiken met alle modules en profielen.

## Stap 9. Verificatieprofielen

Er moet een vergunningsprofiel voor de levering van klanten worden opgesteld. Het standaard clientprovisioningportal wordt gebruikt:



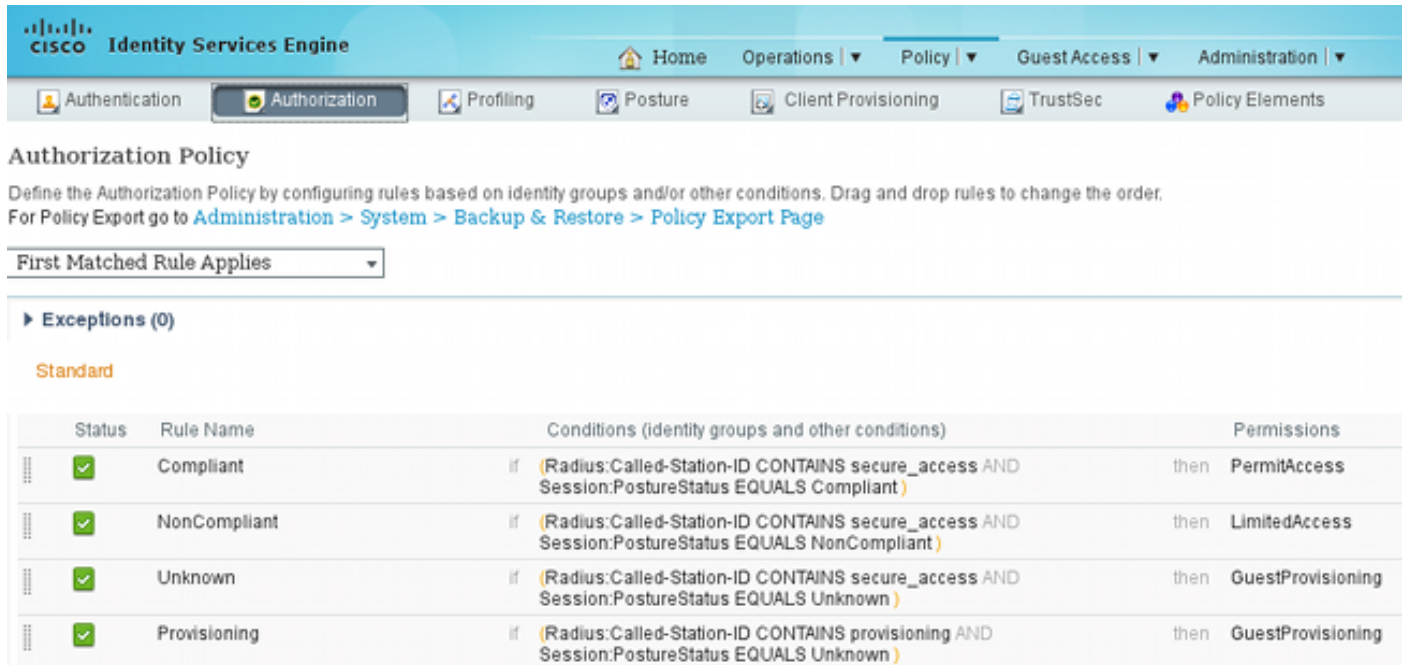
Dit profiel dwingt de gebruikers om voor provisioning naar het standaard clientprovisioningportal te worden omgeleid. Dit portal evalueert het clientprovisioningbeleid (regels die in Stap 8 zijn gemaakt). De machtigingsprofielen zijn de resultaten van de machtigingsregels die in Stap 10 zijn ingesteld.

GuestRedirect Access Control List (ACL) is de naam van de ACL die in de WLC is gedefinieerd. Dit ACL beslist welke verkeer moet worden omgeleid naar ISE. Raadpleeg voor meer informatie de [Central Web Verificatie met een Configuratievoorbeeld van Switch- en Identity Services Engine](#).

Er is ook een ander machtigingsprofiel dat de beperkte netwerktoegang (DACL) biedt voor niet-conforme gebruikers (Limited Access).

## Stap 10. Vergunningsregels

Al deze regels zijn samengevoegd in vier vergunningsregels:



**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

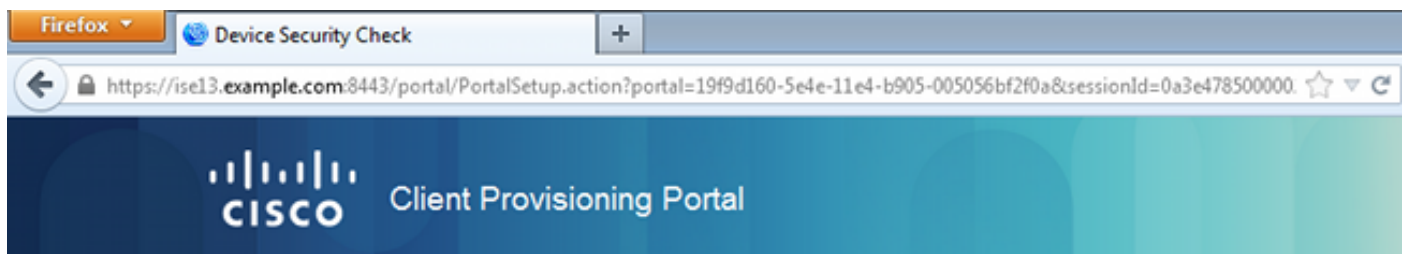
Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Compliant	if (Radius:Called-Station-ID CONTAINS secure_access AND Session:PostureStatus EQUALS Compliant )	then PermitAccess
✓	NonCompliant	if (Radius:Called-Station-ID CONTAINS secure_access AND Session:PostureStatus EQUALS NonCompliant )	then LimitedAccess
✓	Unknown	if (Radius:Called-Station-ID CONTAINS secure_access AND Session:PostureStatus EQUALS Unknown )	then GuestProvisioning
✓	Provisioning	if (Radius:Called-Station-ID CONTAINS provisioning AND Session:PostureStatus EQUALS Unknown )	then GuestProvisioning

Eerst sluit u aan op de Provisioning SSID en wordt voor provisioning opnieuw gericht aan een standaard Client Provisioning Portal (regel genaamd Provisioning). Zodra u verbinding maakt met **Secure\_access** SSID, wijst dit nog steeds op voor provisioning als geen rapport van de Postmodule door ISE (regel genaamd Onbekend) wordt ontvangen. Zodra het eindpunt volledig in overeenstemming is, wordt de volledige toegang verleend (regelnaam conform). Als het eindpunt als niet-conform wordt gerapporteerd, heeft het de beperkte toegang tot het netwerk (regel genaamd Nonconform).

## Verifiëren

U associeert met de Provisioning SSID, probeert toegang te krijgen tot een webpagina en wordt opnieuw gericht naar Client Provisioning Portal:



Firefox Device Security Check

https://ise13.example.com:8443/portal/PortalSetup.action?portal=19f9d160-5e4e-11e4-b905-005056bf2f0a&sessionId=0a3e47850000.

**CISCO** Client Provisioning Portal

### Device Security Check

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

Start

Aangezien AnyConnect niet wordt gedetecteerd, wordt u gevraagd het te installeren:

### Device Security Check


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

#### Unable to detect AnyConnect Posture Agent

**- + This is my first time here**

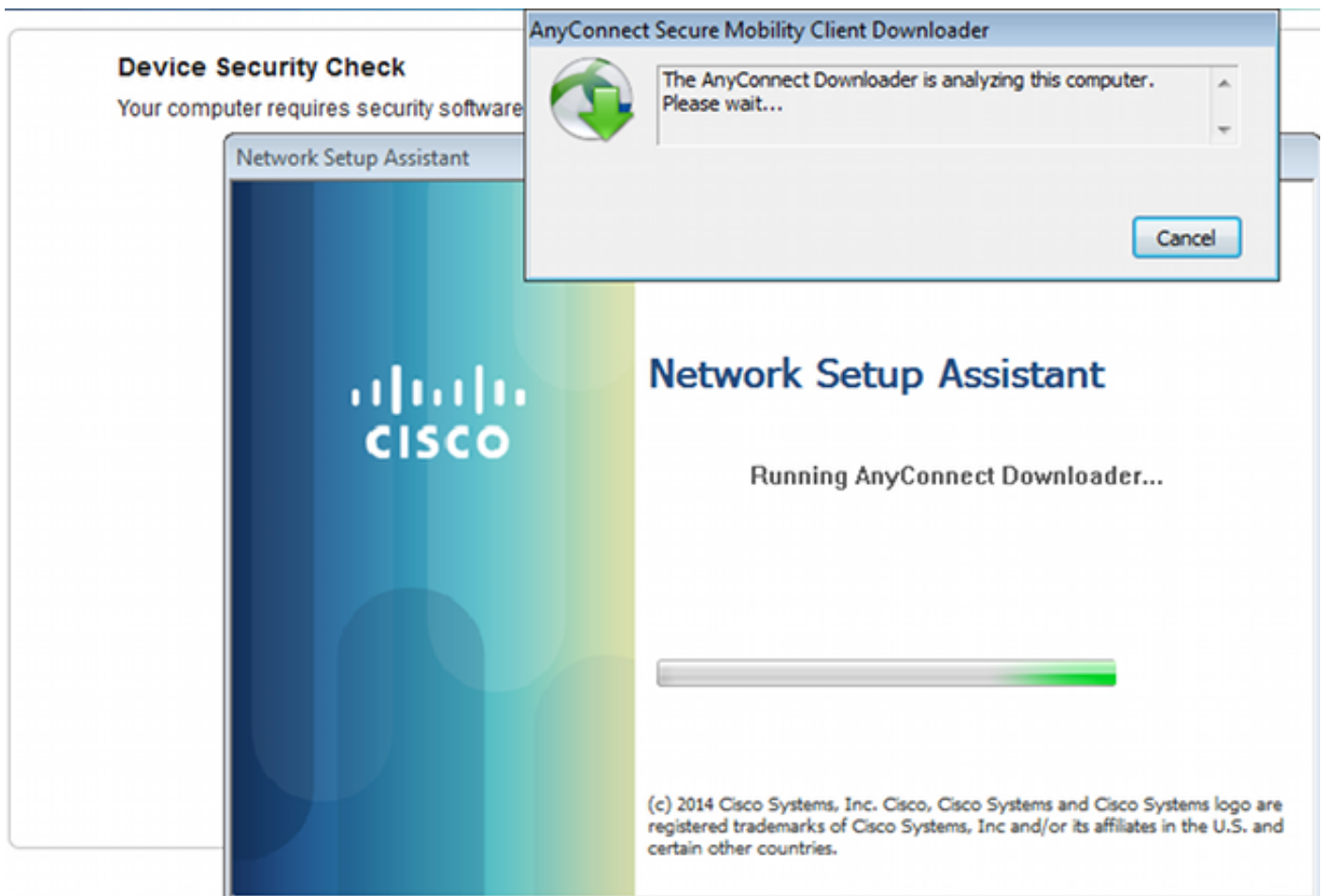
1. You must install AnyConnect to check your device before accessing the network. [Click here to download and install AnyConnect](#)
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave AnyConnect running so it will automatically scan your device and connect you faster next time you access this network.

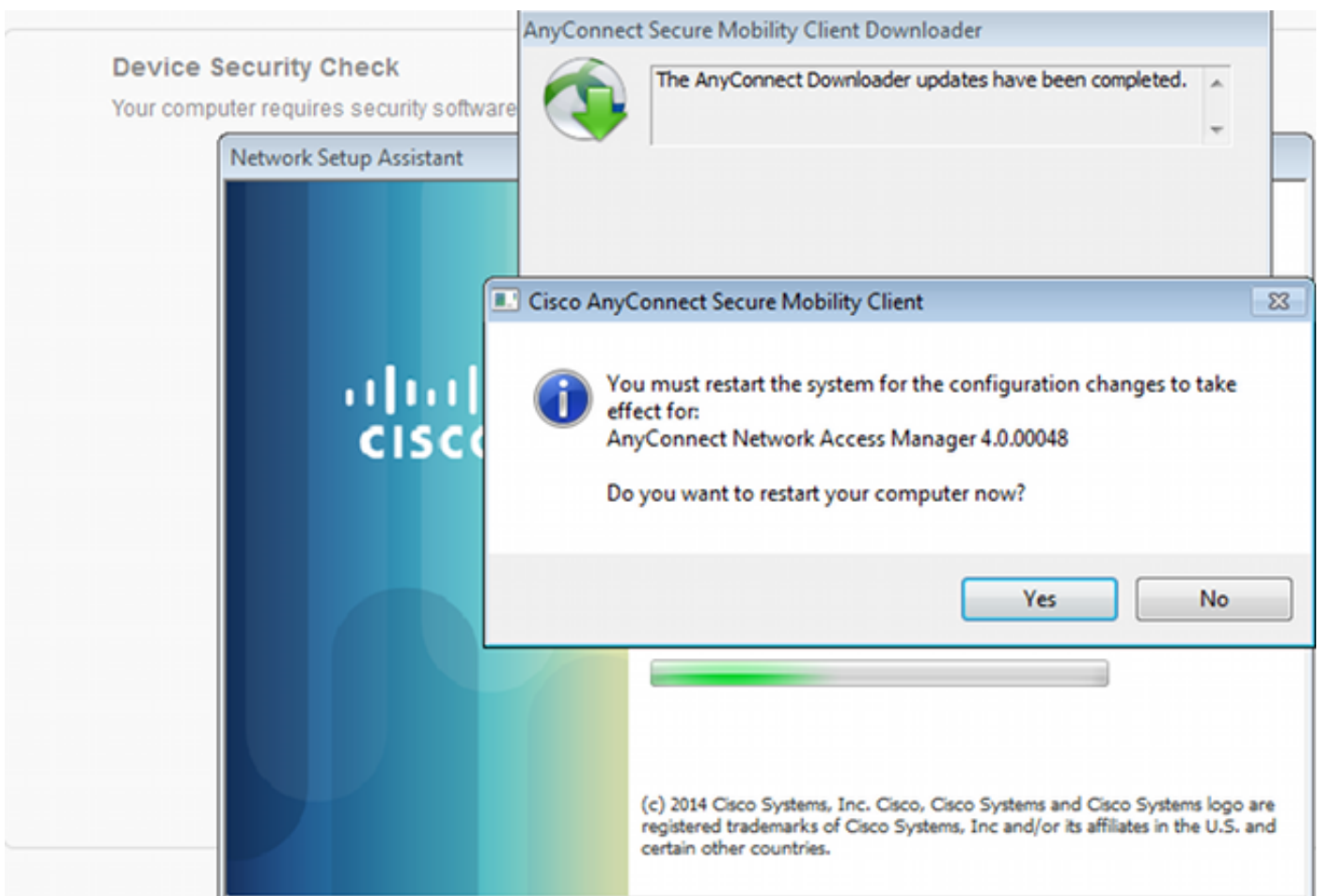
 You have 4 minutes to install and for the compliance check to complete

**+ Remind me what to do next**

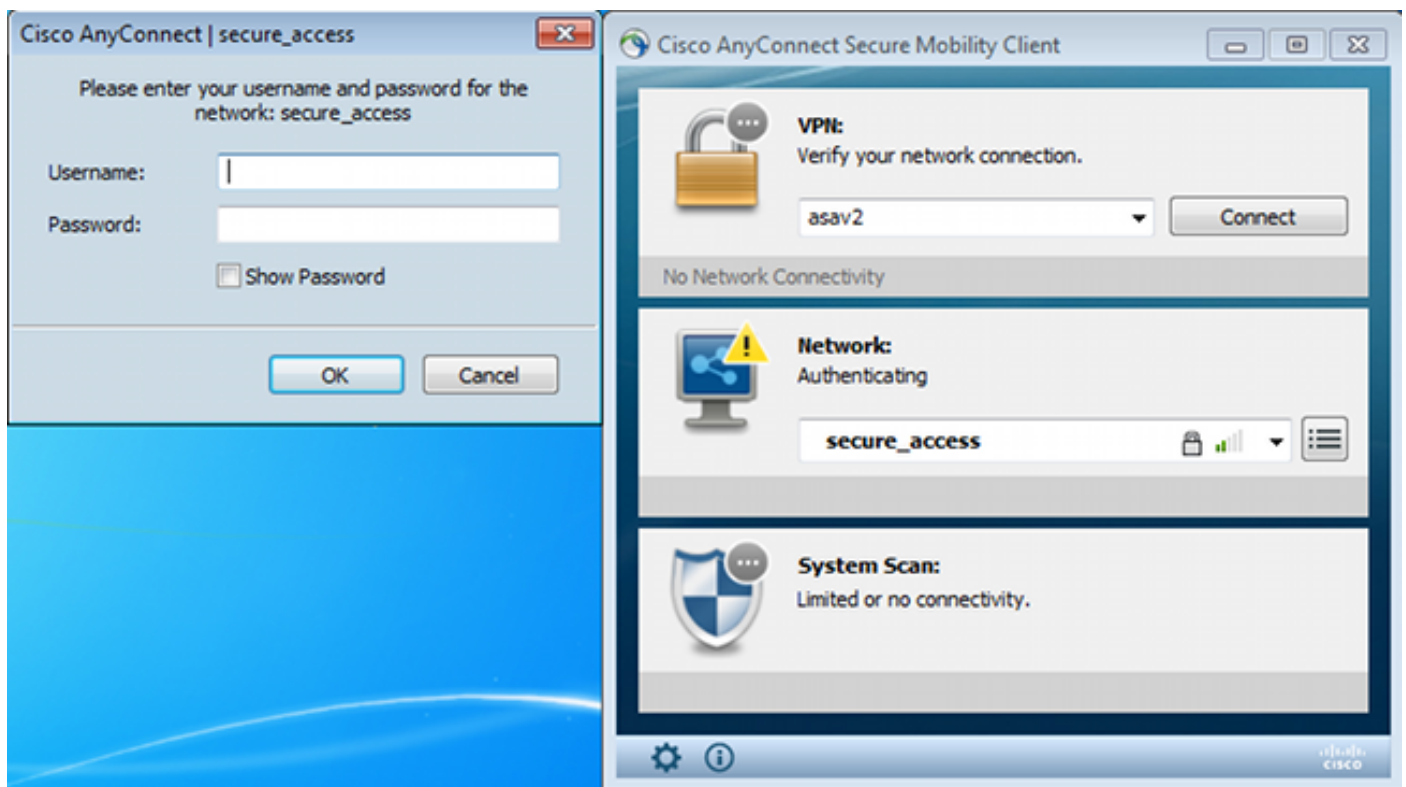
Een kleine toepassing genaamd Network Setup Assistant, die verantwoordelijk is voor het gehele installatieproces, wordt gedownload. Merk op dat het verschilt van de Network Setup Assistant in versie 1.2.



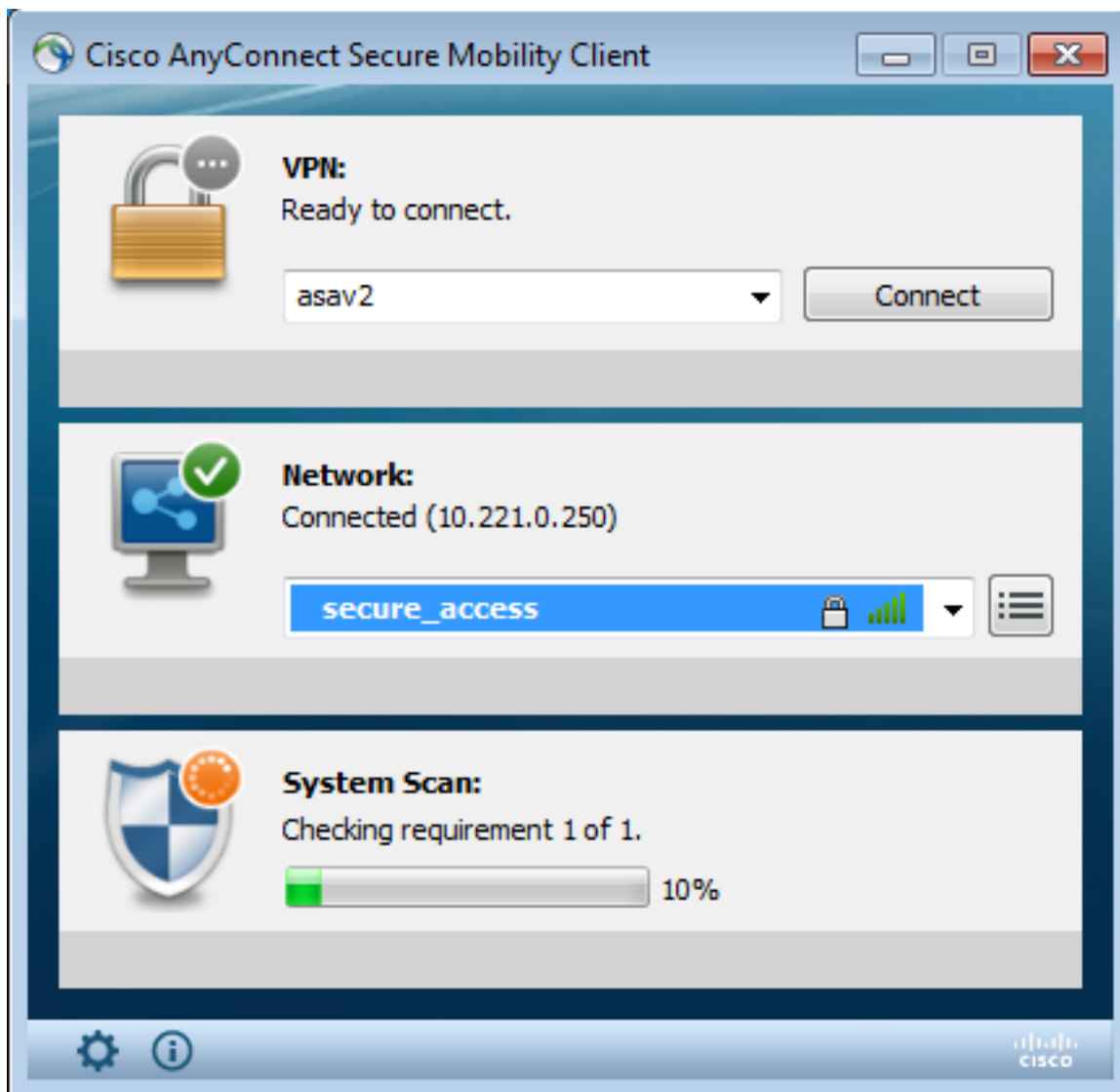
Alle modules (VPN, NAM en Posture) worden geïnstalleerd en geconfigureerd. U moet de computer opnieuw opstarten:



Na de herstart wordt AnyConnect automatisch uitgevoerd en NAM probeert te associëren met Secure\_access SSID (volgens het geconfigureerde profiel). Merk op dat het VPN-profiel correct geïnstalleerd is (ASA2-ingang voor VPN):

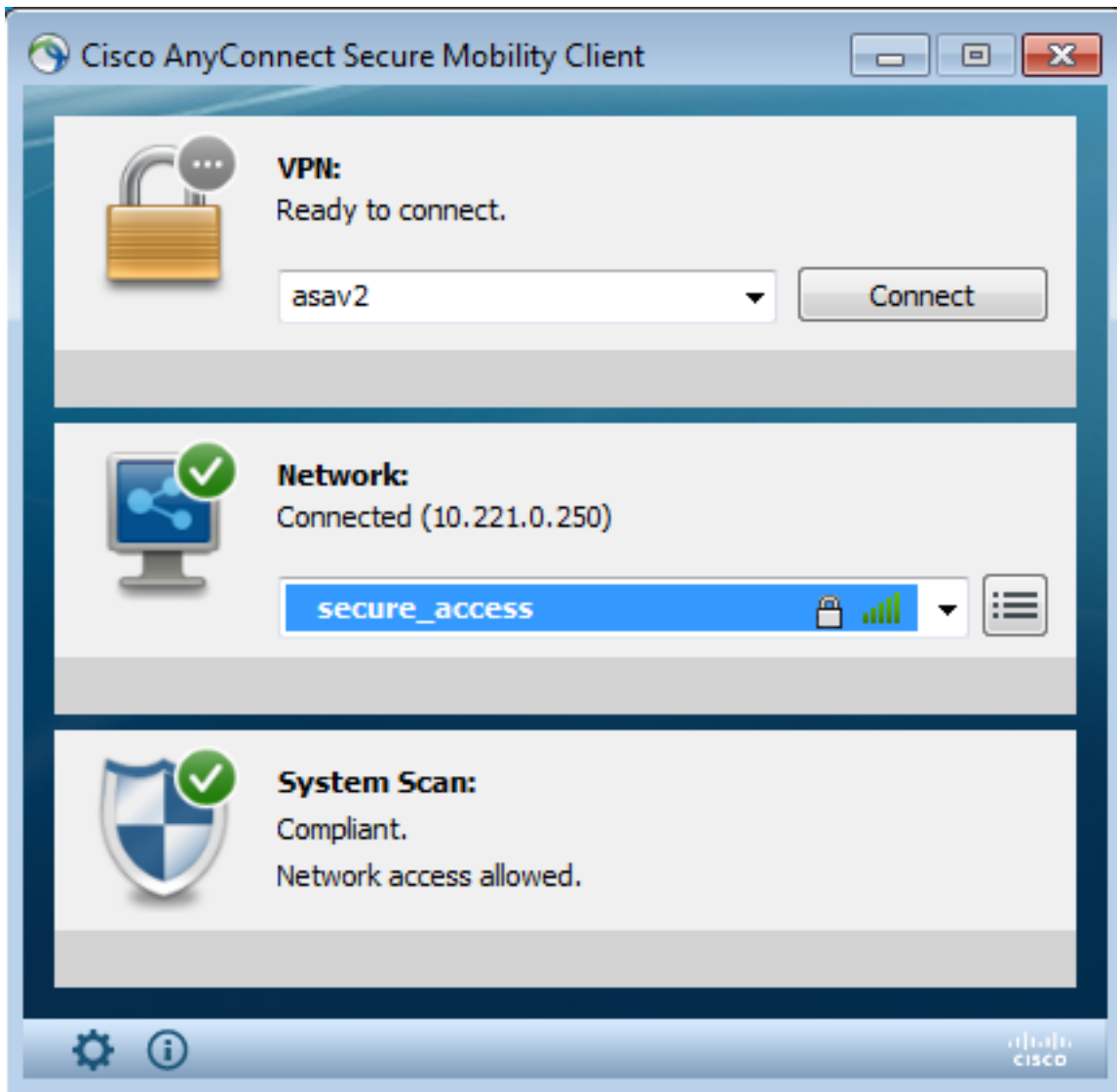


Na verificatie downloads van AnyConnect en ook postregels waarvoor verificatie wordt uitgevoerd:

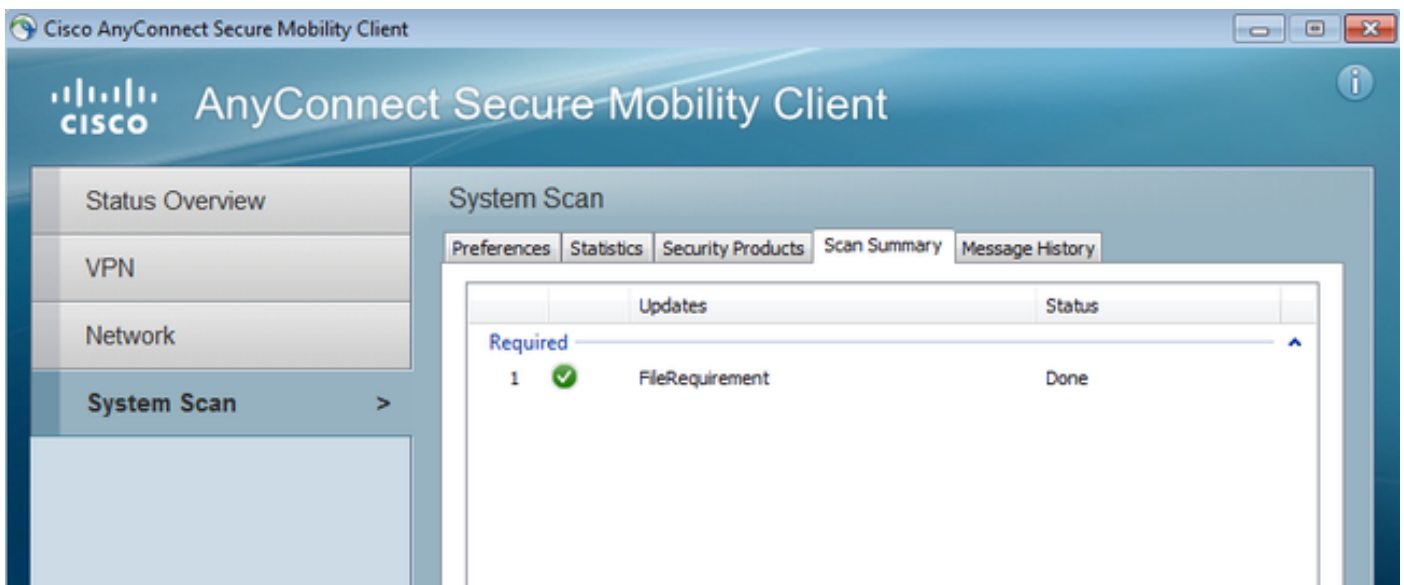


In deze fase is er mogelijk nog steeds beperkte toegang (u krijgt onbekend toestemming via ISE). Zodra het station aan de eisen voldoet, wordt dit gerapporteerd in de Postmodule:





De gegevens kunnen ook worden geverifieerd (aan het vereiste van het bestand is voldaan):



De berichtengeschiedenis toont gedetailleerde stappen:

```
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.**

Het succesvolle rapport wordt naar ISE gestuurd, dat de Wijziging van de Vergunning in gang zet. De tweede authenticatie komt de nalevingsregel tegen en de volledige netwerktoegang wordt verleend. Als het Postrapport wordt verstuurd terwijl het nog steeds gekoppeld is aan de Provisioning SSID, worden deze logs gezien op ISE:

Time	Status	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Posture Status	Server	Event
2014-11-16 09:32:07...	🟢	cisco	CB-4A-00:15-6A-DC				Compliant	ise13	Session State is Started
2014-11-16 09:32:07...	🟢	cisco	CB-4A-00:15-6A-DC	Default => Compliant	PermitAccess	WLC1	Compliant	ise13	Authentication succeeded
2014-11-16 09:32:07...	🟢	cisco	CB-4A-00:15-6A-DC			WLC1	Compliant	ise13	Dynamic Authorization succeeded
2014-11-16 09:31:35...	🔴	admin	CB-4A-00:15-6A-DC			WLC1		ise13	Authentication failed
2014-11-16 09:29:34...	🟢	cisco	CB-4A-00:15-6A-DC	Default => Provisioning	GuestProvisioning	WLC1	Pending	ise13	Authentication succeeded

Het Postrapport vermeldt:

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2014-11-16 09:23:25.8	🟢		N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint
2014-11-16 09:18:42.2	🟢		N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint
2014-11-16 09:16:59.6	🟢		N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint
2014-11-16 09:15:17.4	🟢		N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint

Gedetailleerde verslagen geven de bestandsvereisten weer waaraan wordt voldaan:

## 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		

## Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

## Gerelateerde informatie

- [Postservices op Cisco ISE Configuration Guide](#)
- [Cisco ISE 1.3 beheerdershandleiding](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)