Integración de AnyConnect 4.0 con el ejemplo de configuración de la versión 1.3 ISE

Contenido

Introducción

Este documento describe las nuevas funciones en la versión 1.3 del Cisco Identity Services Engine (ISE) que permite que usted configure varios módulos cliente seguros de la movilidad de AnyConnect y que provision los automáticamente al punto final. Este documento presenta cómo configurar los módulos VPN, del administrador del acceso a la red (NAM), y de la postura en el ISE y avanzarlos al usuario corporativo.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Implementaciones, autenticación, y autorización ISE
- Configuración de los reguladores del Wireless LAN (WLCs)
- Conocimiento básico VPN y del 802.1x

- Configuración de los perfiles VPN y NAM con los editores del perfil de AnyConnect

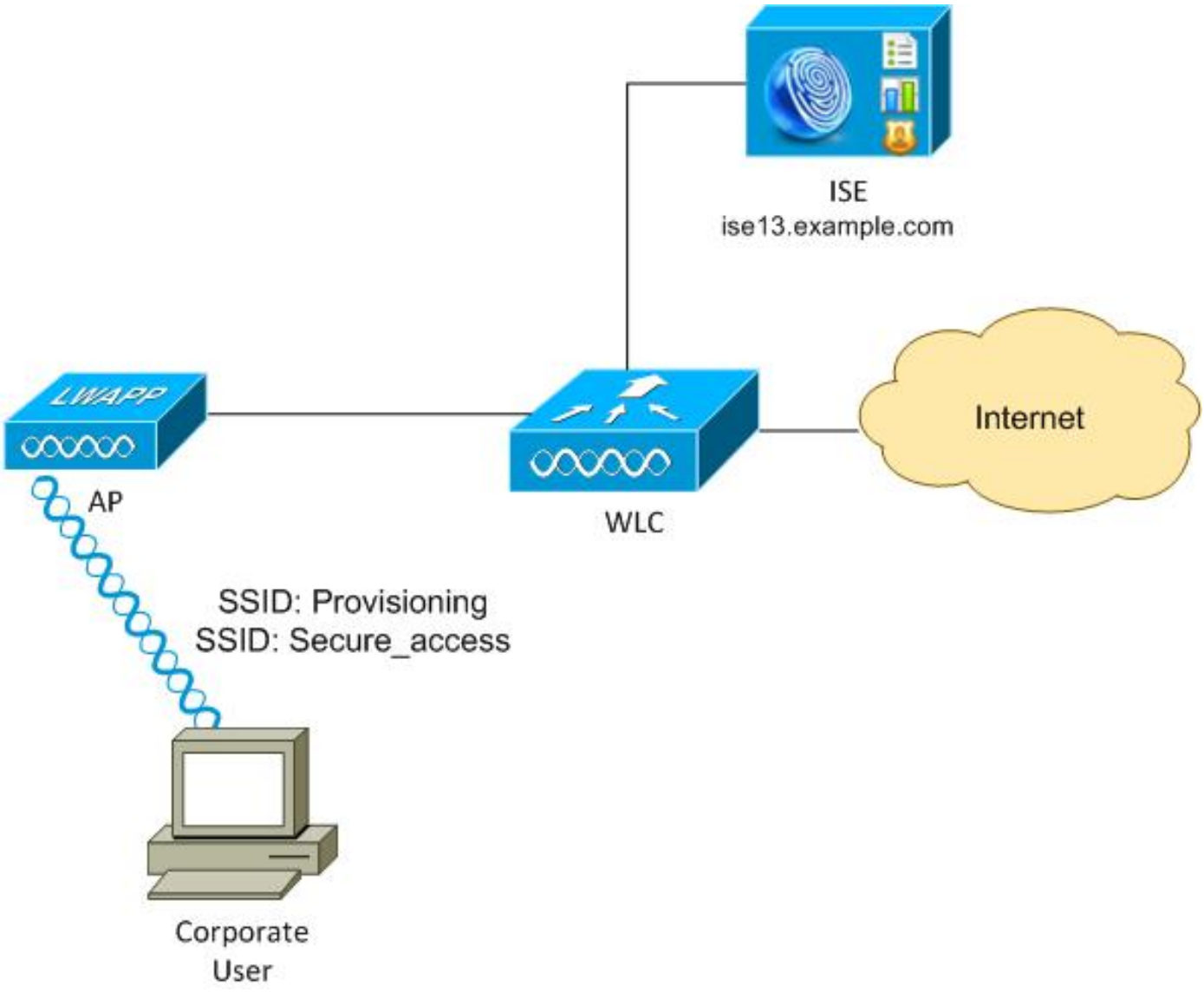
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Versión 7.6 y posterior del WLC de Cisco
- Software de Cisco ISE, versiones 1.3 y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Topología y flujo



Aquí está el flujo:

Paso 1. Service Set Identifier (SSID) de los acceses del usuario corporativo: Disposición. Realiza

la autenticación del 802.1x con EAP Protocolo-protegido autenticación ampliable (EAP-PEAP). La regla de la autorización del **aprovisionamiento** se encuentra en el ISE y reorientan al usuario para el aprovisionamiento de AnyConnect (vía la disposición del cliente protal). Si AnyConnect no se detecta en la máquina, todos los módulos configurados están instalados (VPN, NAM, postura). Junto con ese perfil, la configuración para cada módulo se avanza.

Paso 2. Una vez que AnyConnect está instalado, el usuario debe reiniciar el PC. Después de que la reinicialización, AnyConnect se ejecute y el SSID correcto se utiliza automáticamente según el perfil configurado NAM (Secure_access). Se utiliza EAP-PEAP (como un ejemplo, la Seguridad de la capa del Protocolo-transporte de la autenticación ampliable (EAP-TLS) se podría también utilizar). Al mismo tiempo, el módulo de la postura marca si la estación es obediente (las comprobaciones para la existencia del **archivo de c:\test.txt**).

Paso 3. Si el estatus de la postura de la estación es desconocido (ningún informe del módulo de la postura), todavía se reorienta para disposición, porque la regla de Authz el **desconocido** se encuentra en el ISE. Una vez que la estación es obediente, el ISE envía un cambio de la autorización (CoA) al regulador del Wireless LAN, que acciona la reautentificación. Una segunda autenticación ocurre, y la regla **obediente** se golpea en el ISE, que proporcionará al usuario con el acceso total a la red.

Como consecuencia, el usuario ha sido aprovisionado con AnyConnect VPN, NAM, y los módulos de la postura que permiten el acceso unificado a la red. Las funciones similares se pueden utilizar en el dispositivo de seguridad adaptante (ASA) para el acceso VPN. Actualmente, el ISE puede hacer lo mismo para cualquier tipo de acceso con un acercamiento muy granular.

Estas funciones no se limitan a los usuarios corporativos, sino que son posiblemente las mas comunes desplegarlas para ese grupo de usuarios.

Configurar

WLC

El WLC se configura con dos SSID:

- Disposición - [WPA + WPA2][Auth(802.1X)]. Este SSID se utiliza para el aprovisionamiento de AnyConnect.
- Secure_access - [WPA + WPA2][Auth(802.1X)]. Este SSID se utiliza para el acceso seguro después de que el punto final haya sido aprovisionado con el módulo NAM que se configura para ese SSID.

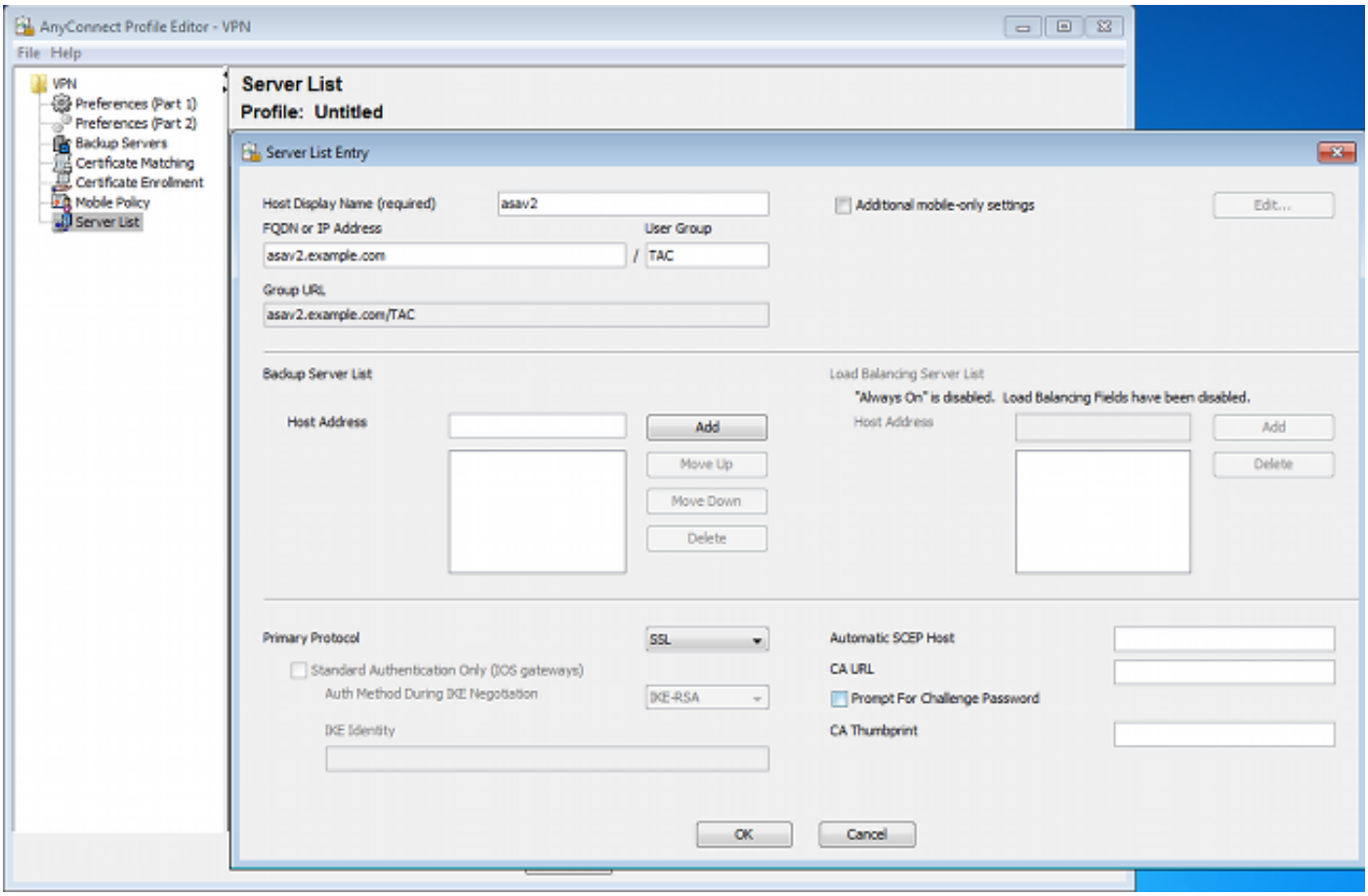
ISE

Paso 1. Agregue el WLC

Agregue el WLC a los dispositivos de red en el ISE.

Paso 2. Configure el perfil VPN

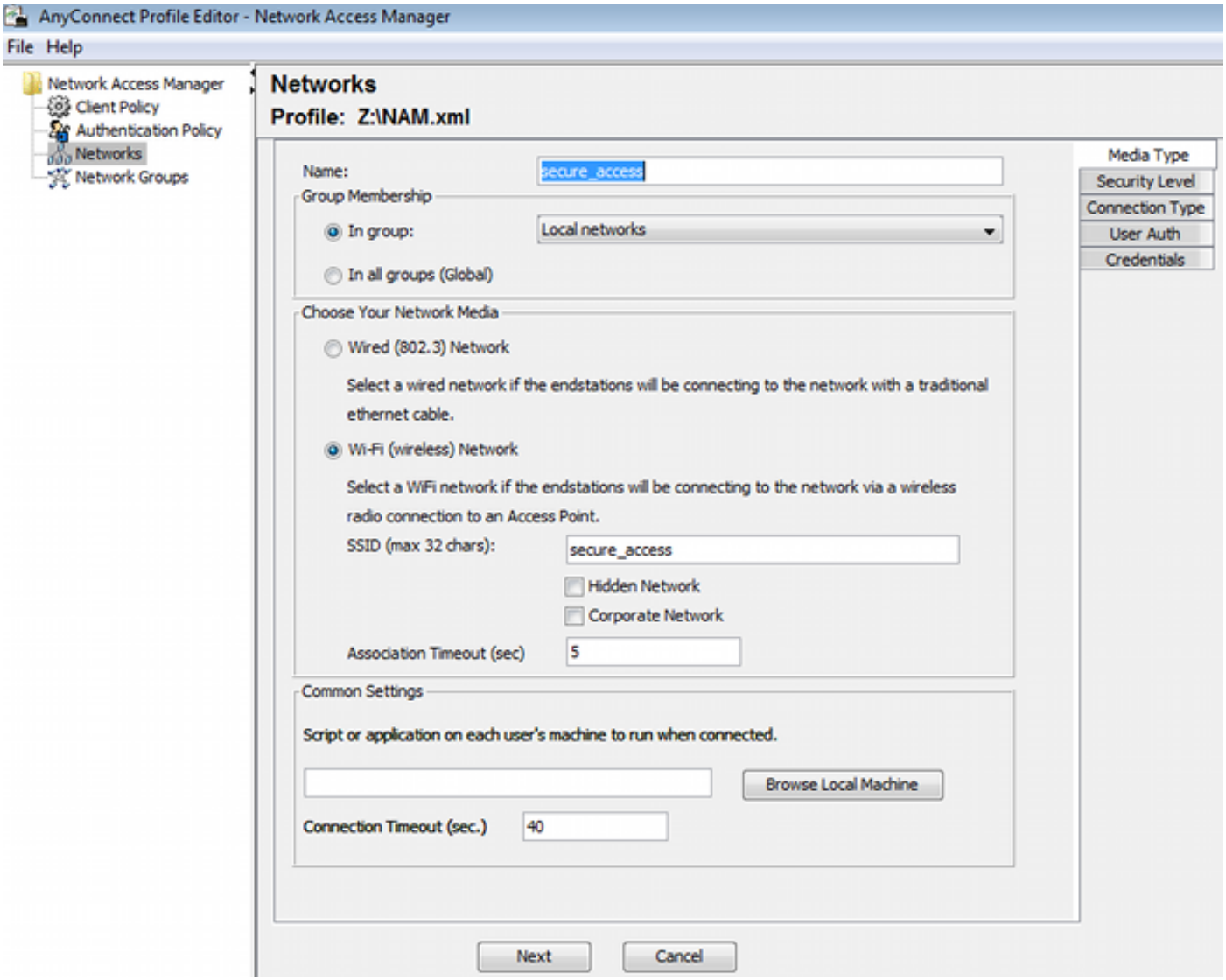
Configure el perfil VPN con el editor del perfil de AnyConnect para el VPN.



Solamente una entrada se ha agregado para el acceso VPN. Excepto que archivo XML a **VPN.xml.**

Paso 3. Configure el perfil NAM

Configure el perfil NAM con el editor del perfil de AnyConnect para el NAM.



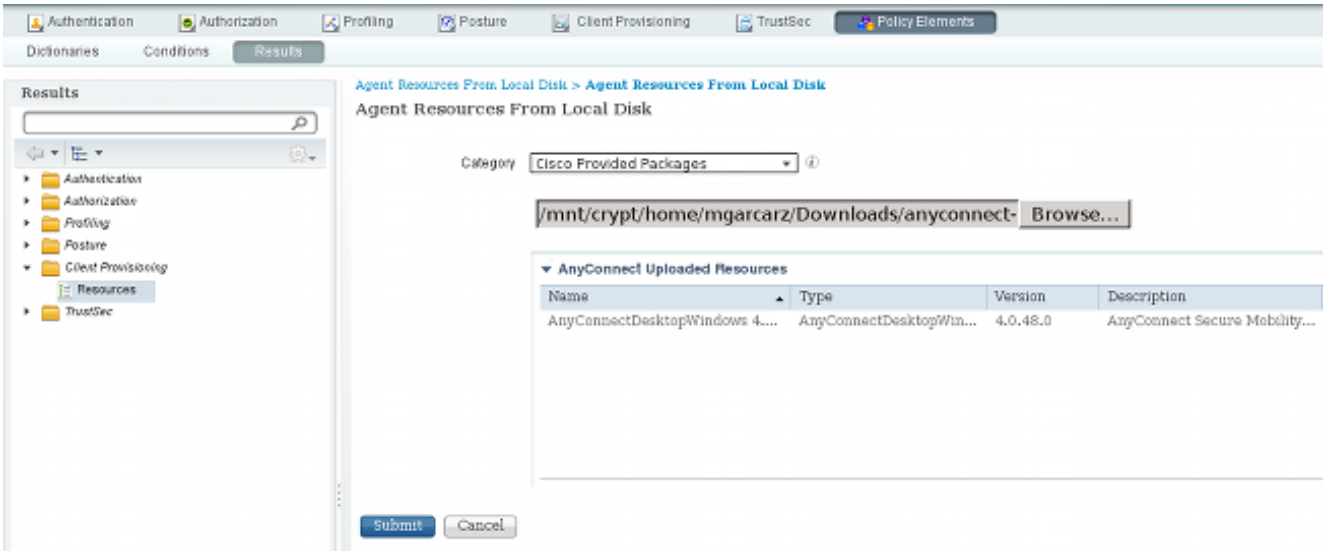
Se ha configurado solamente un SSID: **secure_access**. Excepto que archivo XML a **NAM.xml.**

Paso 4. Instale la aplicación

1. Descargue la aplicación manualmente del cisco.com.

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

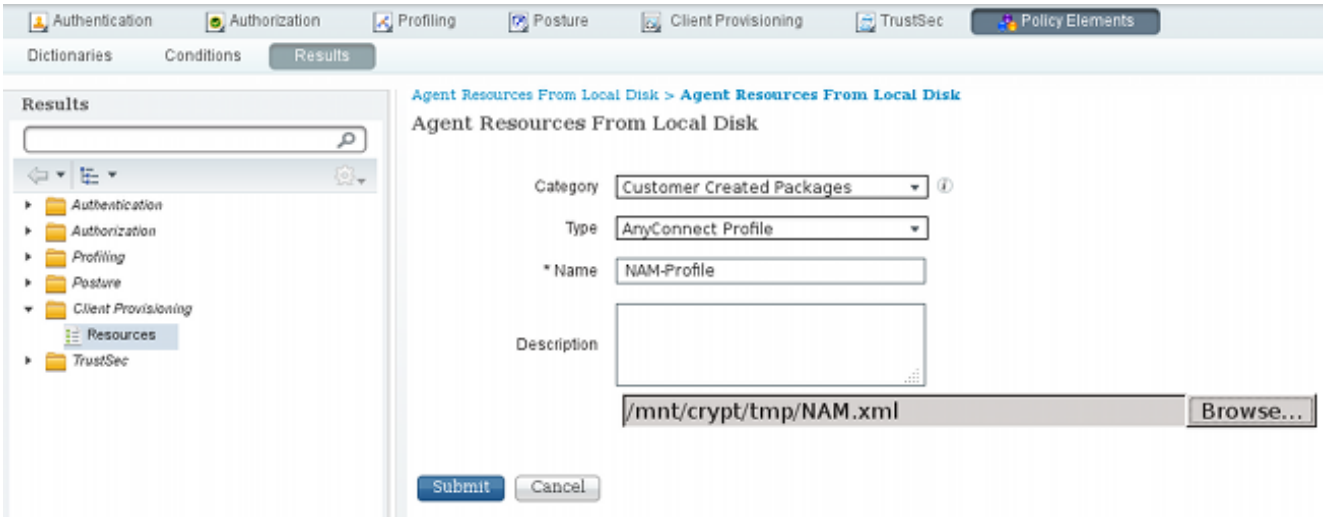
2. En el ISE, navegue a la **directiva > a los resultados > al aprovisionamiento > a los recursos del cliente**, y agregue a los recursos del agente del disco local.
3. Elija Cisco proporcionó a los paquetes y seleccionan el **anyconnect-win-4.0.00048-k9.pkg**:



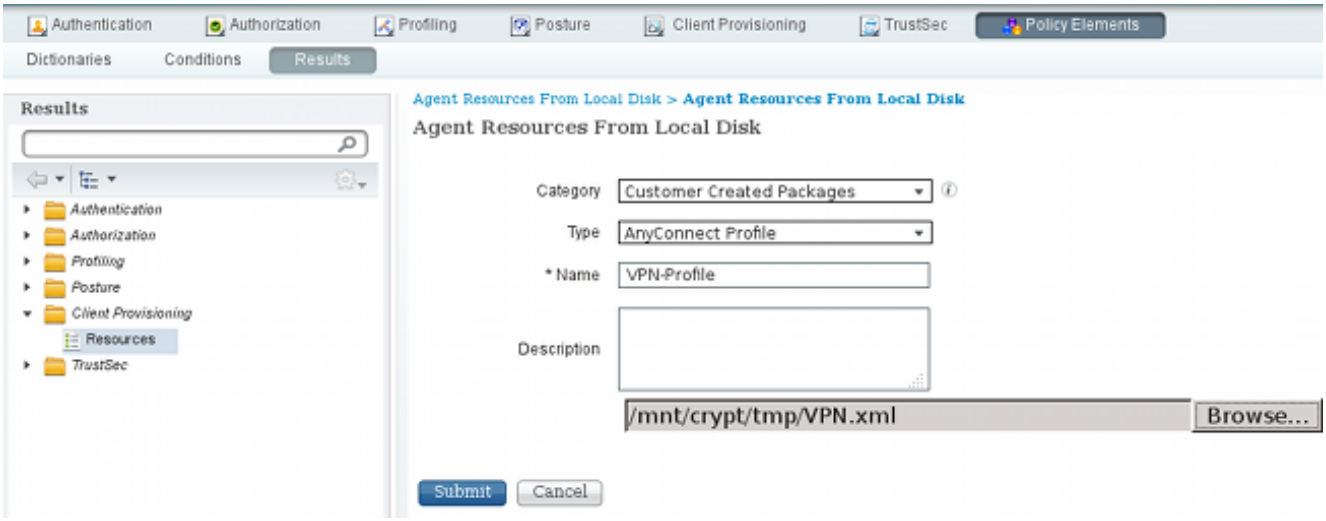
4. Relance el paso 4 para el módulo de la conformidad.

Paso 5. Instale el perfil VPN/NAM

1. Navegue a la **directiva > a los resultados > al aprovisionamiento > a los recursos del cliente**, y agregue a los recursos del agente del disco local.
2. Elija los paquetes y el **perfil** creados cliente de **AnyConnect del** tipo. Seleccione el perfil previamente creado NAM (archivo XML):



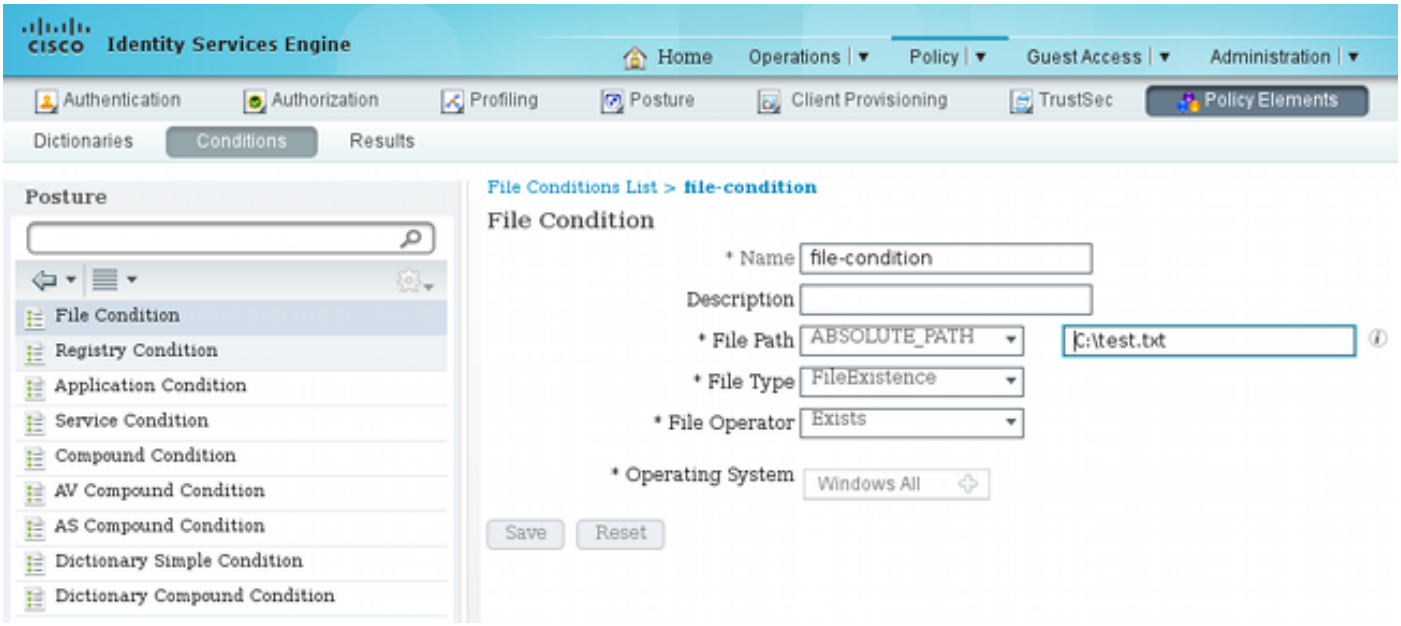
3. Relance los pasos similares para el perfil VPN:



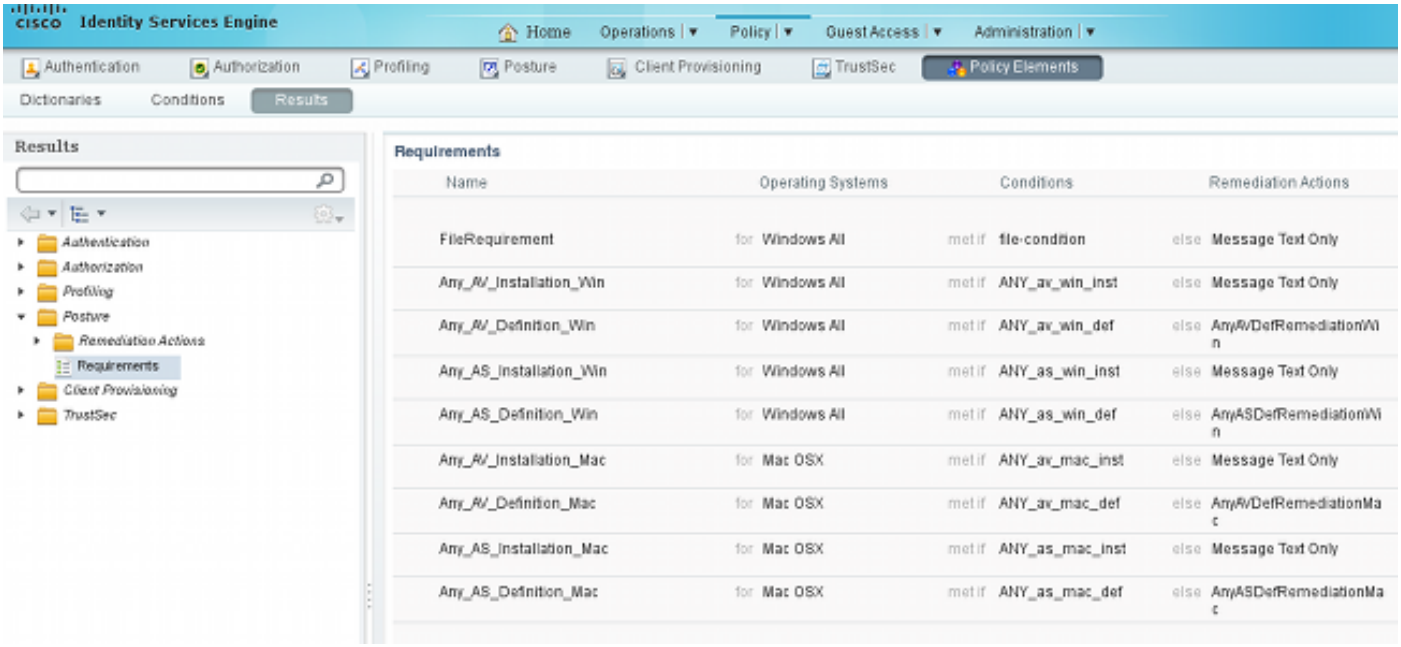
Paso 6. Configure la postura

Los perfiles NAM y VPN tienen que ser configurados externamente con el editor del perfil de AnyConnect y ser importados en el ISE. Pero la postura es de configuración completa en el ISE.

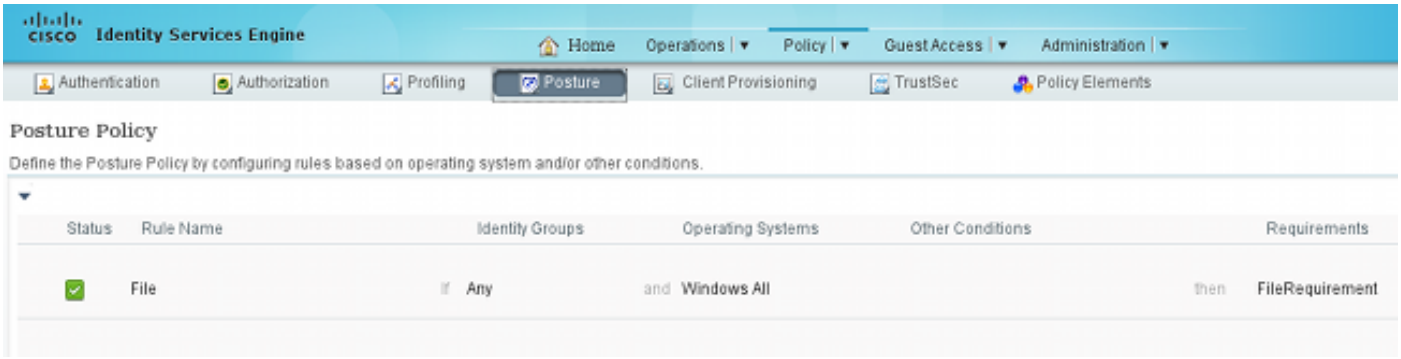
Navegue a la **directiva > a las condiciones > a la postura > al archivo Condition.You** puede ver que una condición simple para la existencia del archivo se ha creado. Usted debe tener ese archivo para ser obediente con la directiva verificada por el módulo de la postura:



Esta condición se utiliza para un requisito:



Y el requisito se utiliza en la directiva de la postura para los sistemas de Microsoft Windows:

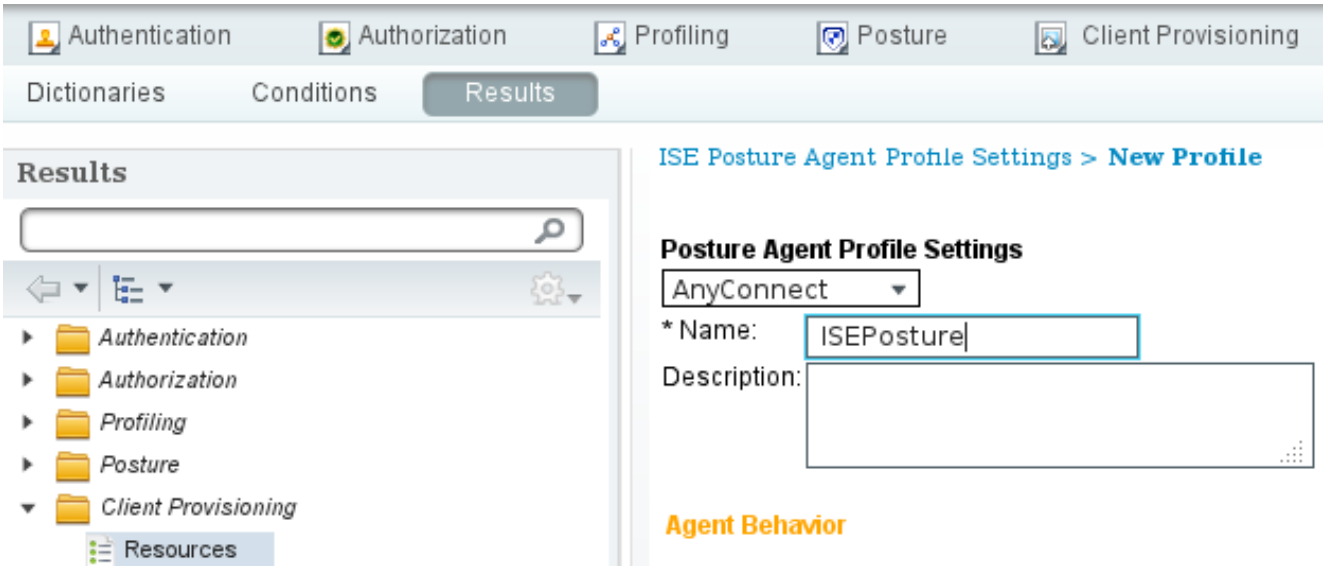


Para más información sobre la configuración de la postura, refiera a los [servicios de la postura en la guía de configuración de Cisco ISE].

Una vez que la directiva de la postura está lista, es hora de agregar la Configuración del agente de la postura.

1. Navegue a la **directiva > a los resultados > al aprovisionamiento > a los recursos del cliente** y agregue el perfil de la postura del agente del Network Admission Control (NAC) o del agente de AnyConnect.

2. AnyConnect selecto (un nuevo módulo de la postura de la versión 1.3 ISE se ha utilizado en vez del agente viejo del NAC):



3. De la sección de protocolo de la postura, no olvide agregar ***** para permitir que el agente conecte con todos los servidores.

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 Nombre del servidor gobierna el campo se deja vacío, el ISE no salva las configuraciones y señala este error:

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

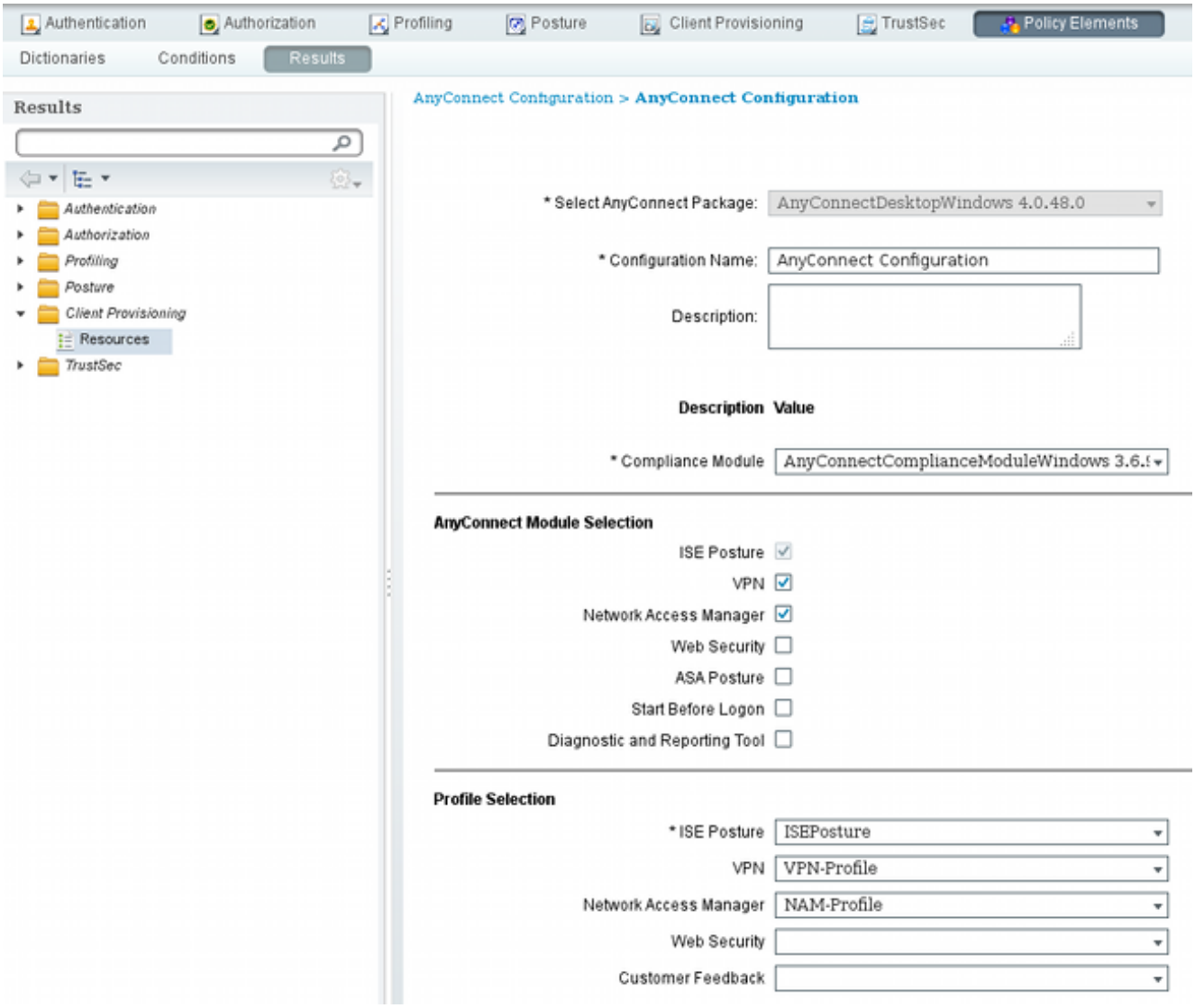
Paso 7. Configuración AnyConnect

En esta etapa, se han configurado todas las aplicaciones (AnyConnect) y la configuración del perfil para todos los módulos (VPN, NAM, y postura). Es hora de vincularlo.

1. Navegue a la **directiva > a los resultados > al aprovisionamiento > a los recursos del cliente**, y agregue la configuración de AnyConnect.

2. Configure el nombre y seleccione el módulo y todos los módulos requeridos de AnyConnect (VPN, NAM, y postura) de la conformidad.

3. En la selección del perfil, elija el perfil configurado anterior para cada módulo.



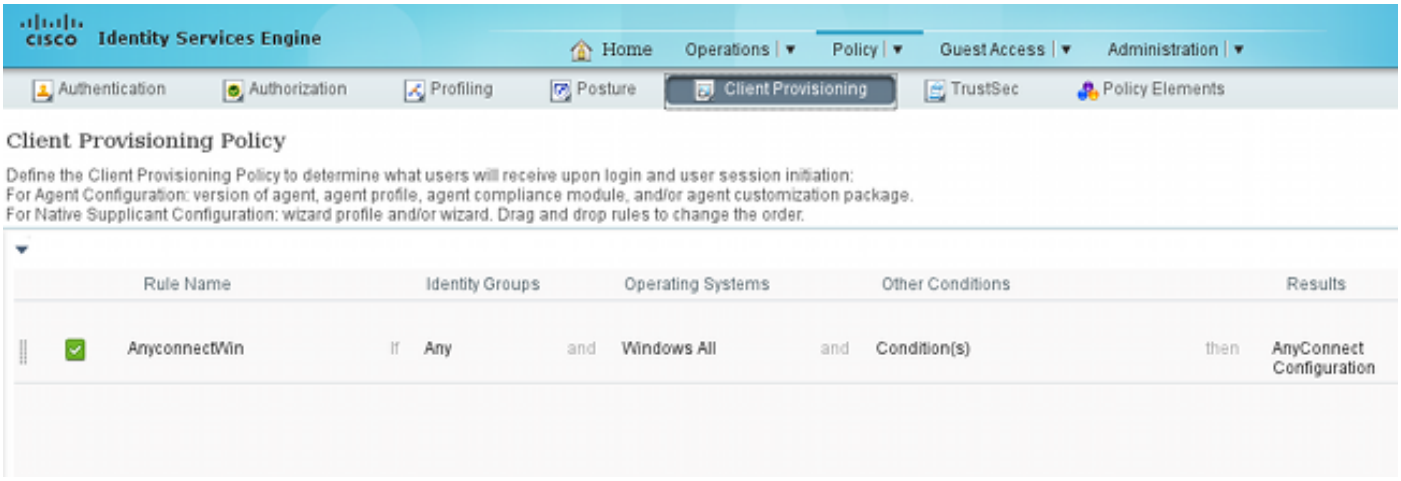
4. El módulo VPN es obligatorio para que el resto de los módulos funcionen corrrectly. Incluso si el módulo VPN no se selecciona para la instalación, será avanzado y instalado en el cliente. Si usted no quiere utilizar el VPN, hay una posibilidad para configurar un perfil especial para el VPN que oculta la interfaz de usuario para el módulo VPN. Estas líneas se deben agregar al **archivo VPN.xml:**

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

5. Esta clase de perfil también está instalada cuando usted utiliza el **setup.exe del** paquete ISO (anyconnect-win-3.1.06073-pre-deploy-k9.iso**).** Entonces, el **perfil** VPNDisable_ServiceProfile.xml para el VPN está instalado junto con la configuración, que inhabilita la interfaz de usuario para el módulo VPN.

Paso 8. Reglas del aprovisionamiento del cliente

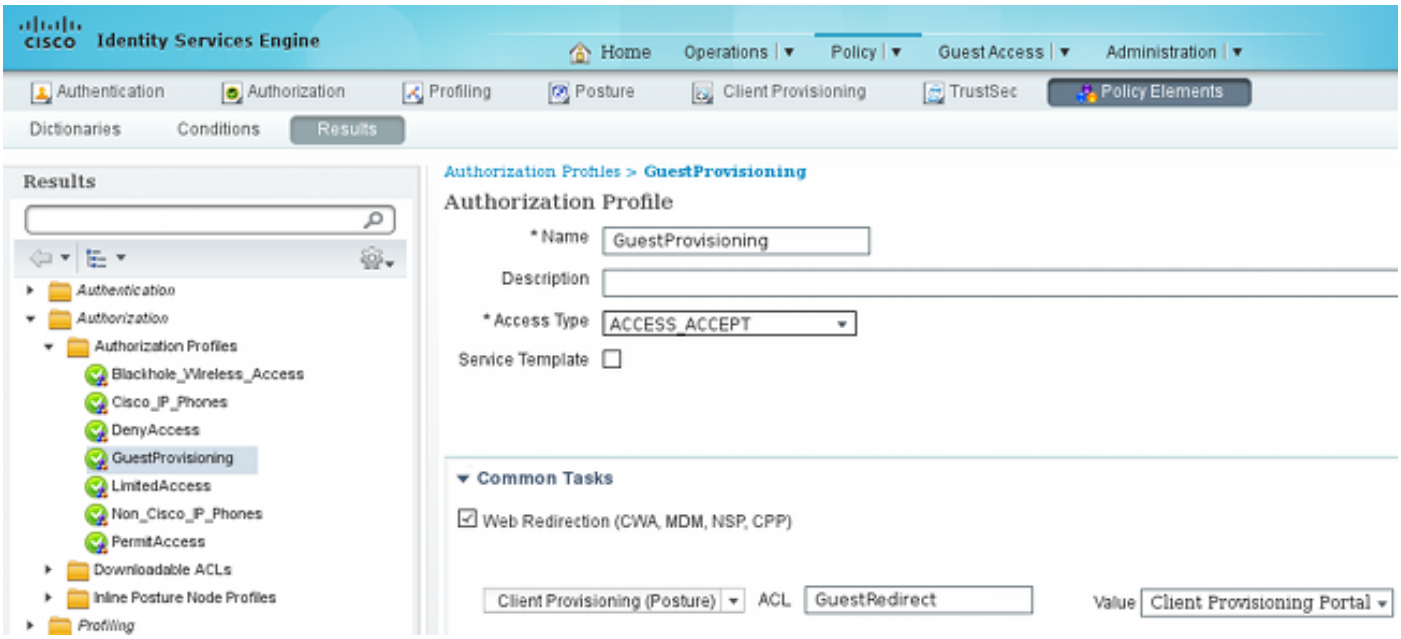
La configuración de AnyConnect creada en el paso 7 se debe referir a las reglas del aprovisionamiento del cliente:



Las reglas del aprovisionamiento del cliente deciden a qué aplicación será avanzada al cliente. Solamente una regla se necesita aquí con el resultado que señala a la configuración creada en el paso 7. Esta manera, todos los puntos finales de Microsoft Windows que se reorienten para el aprovisionamiento del cliente utilizará la configuración de AnyConnect con todos los módulos y perfiles.

Paso 9. Perfiles de la autorización

El perfil de la autorización para el aprovisionamiento del cliente necesita ser creado. Se utiliza el portal de disposición del cliente predeterminado:



Este perfil fuerza a los usuarios a ser reorientado para disposición al portal de disposición del cliente predeterminado. Este portal evalúa la directiva de Provisiong del cliente (reglas creadas en el paso 8). Los perfiles de la autorización son los resultados de las reglas de la autorización configuradas en el paso 10.

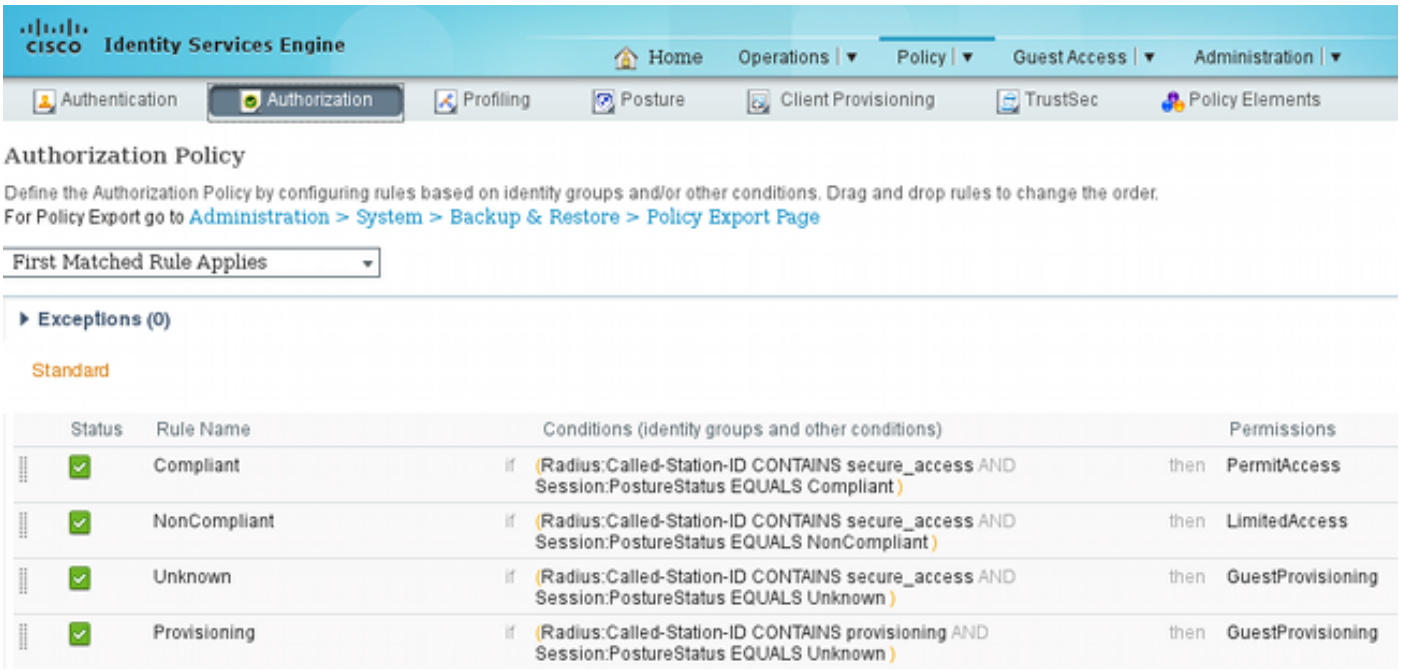
La lista de control de acceso (ACL) de GuestRedirect es el nombre del ACL definido en el WLC. Este ACL decide a qué tráfico se debe reorientar al ISE. Para más información, refiera a la autenticación Web central con un ejemplo de configuración del Switch y del Identity Services Engine.

Hay también otro perfil de la autorización que proporciona el acceso a la red limitado (DACL) para

los usuarios no obedientes (llamados LimitedAccess).

Paso 10. Reglas de la autorización

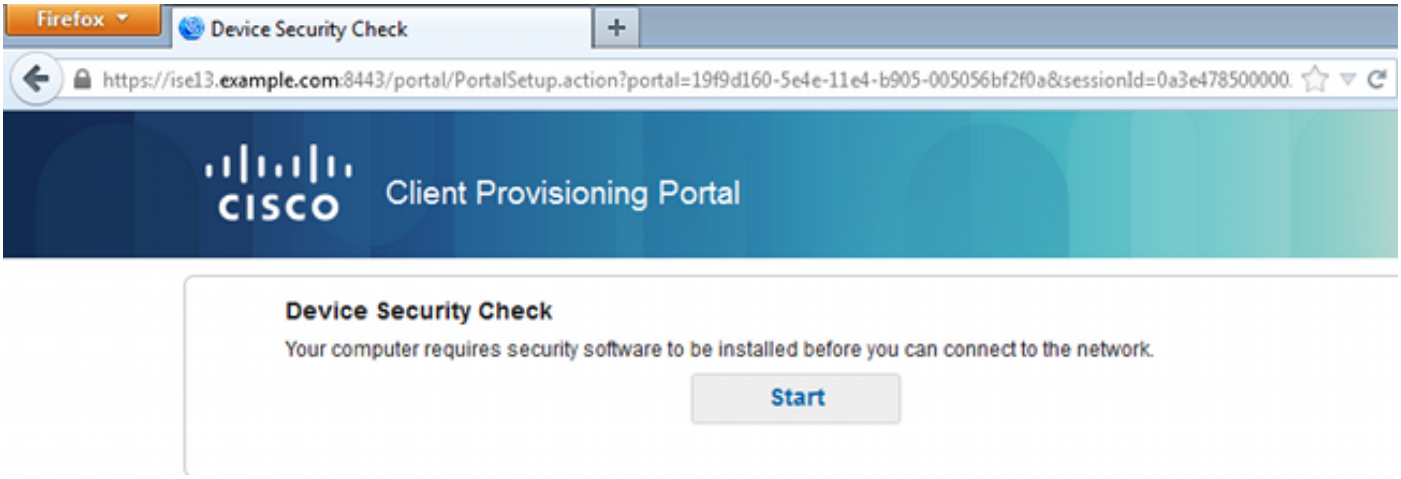
Todo el ésos se combinan en cuatro reglas de la autorización:



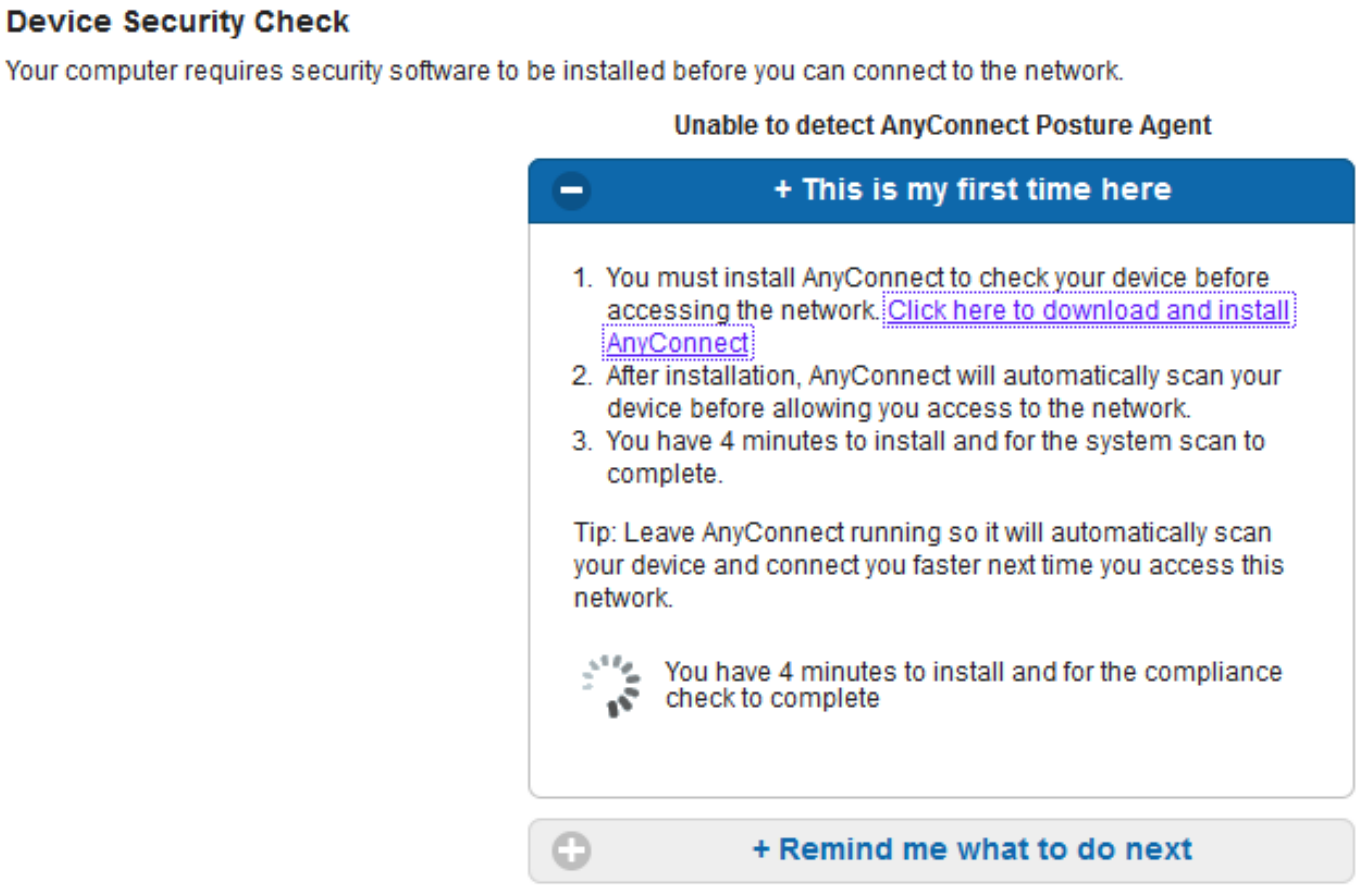
Primero usted conecta con el SSID de disposición y se reorienta para disposición a un portal de disposición del cliente predeterminado (regla Provisioning Nombrado). Una vez que usted conecta con el **Secure_access** SSID, todavía reorienta para disposición si no se recibe ningún informe del módulo de la postura por ISE (regla Unknown Nombrado). Una vez que el punto final es completamente obediente, se concede el acceso total (nombre de la regla obediente). Si el punto final está señalado como no obediente, ha limitado el acceso a la red (regla NonCompliant Nombrado).

Verificación

Usted se asocia al SSID de disposición, intenta acceder cualquier página web, y se reorienta al portal de disposición del cliente:

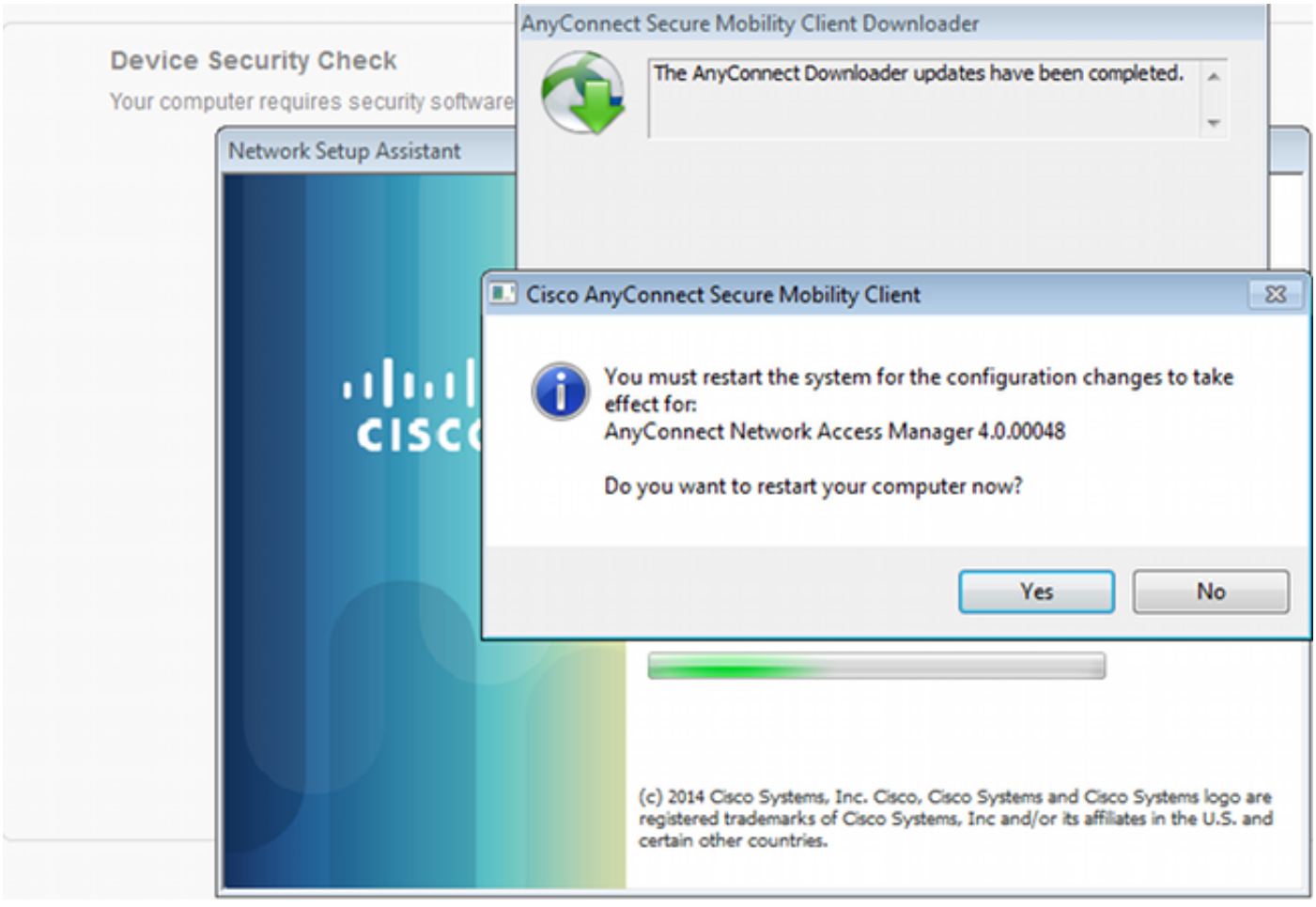


Puesto que AnyConnect no se detecta, le piden instalarlo:

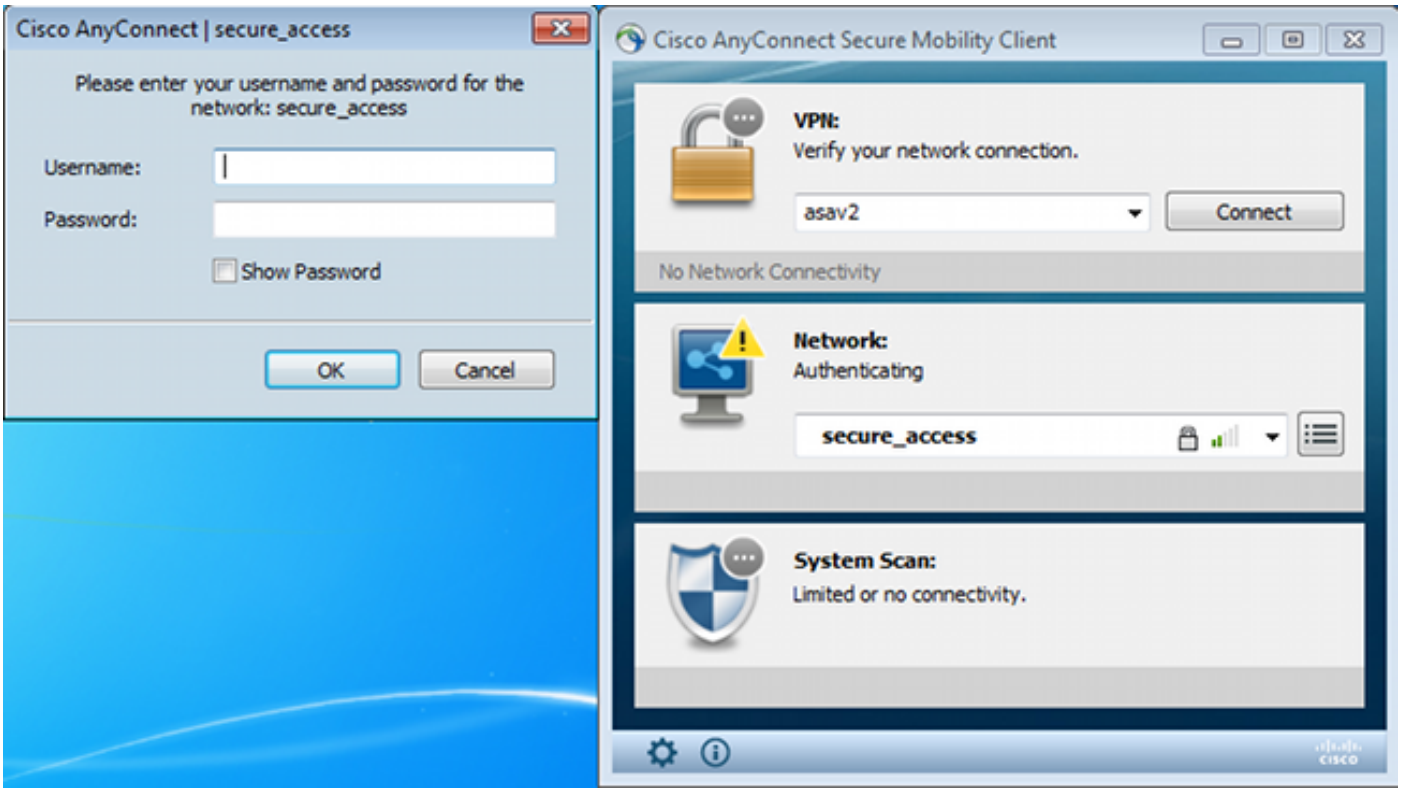


Se descarga una pequeña aplicación llamó al ayudante de la configuración de la red, que es responsable del proceso de instalación entero. Note que es diferente que el ayudante de la configuración de la red en la versión 1.2.

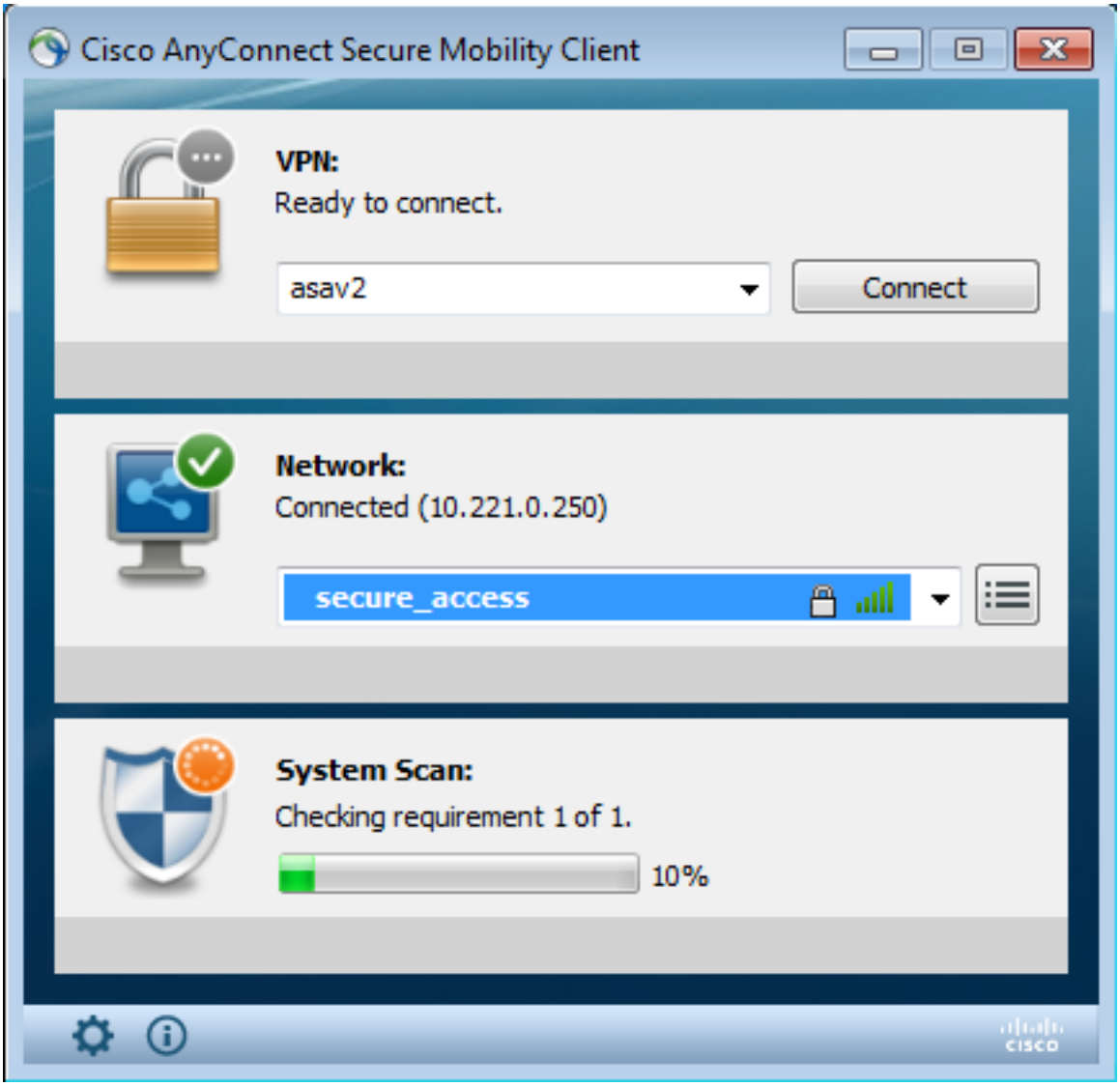
Todos los módulos (VPN, NAM, y postura) están instalados y configurados. Usted debe reiniciar su PC:



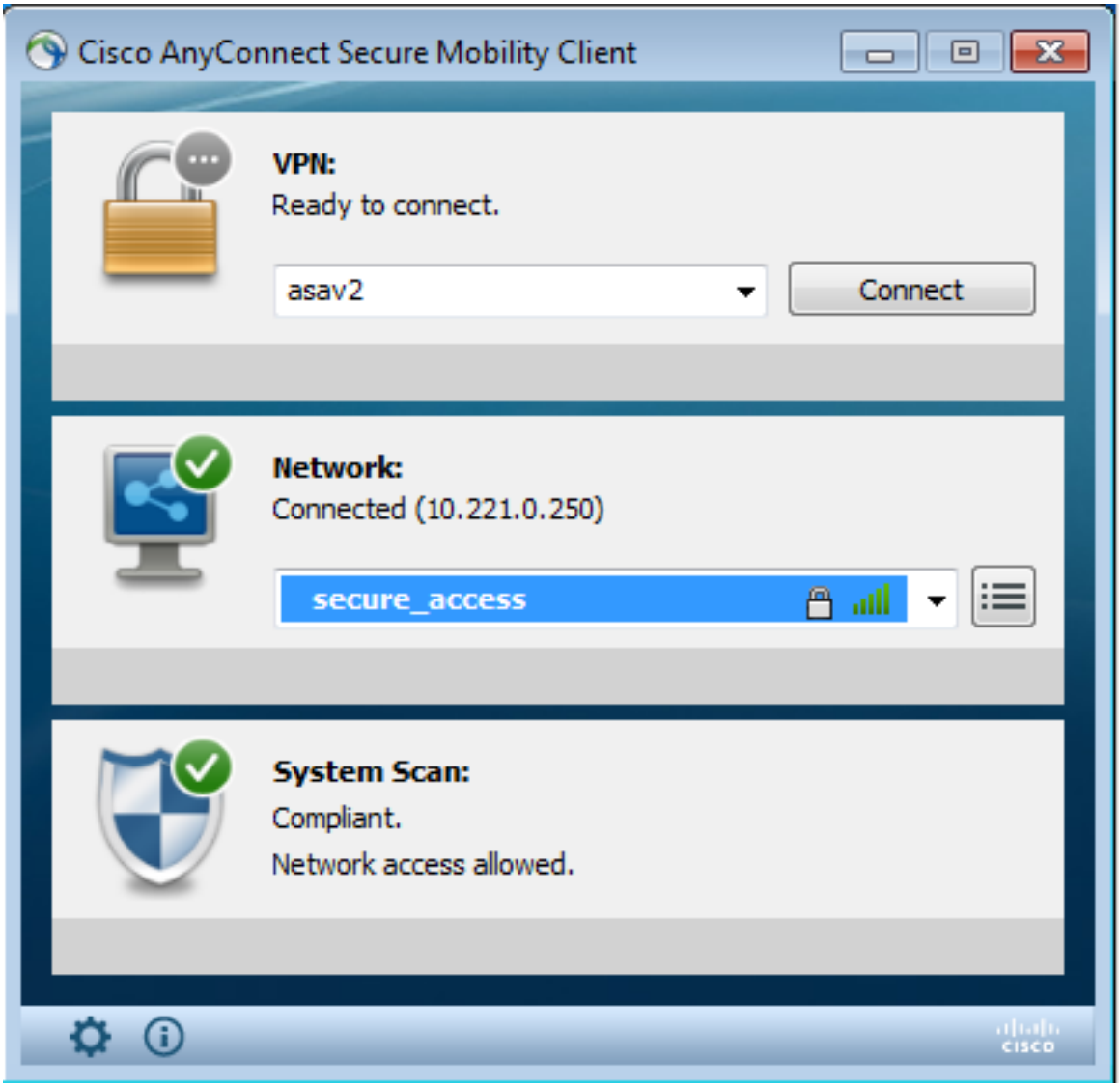
Después de que la reinicialización, AnyConnect se ejecute automáticamente y los intentos NAM para asociarse a los secure_access SSID (según el perfil configurado). Note que el perfil VPN está instalado correctamente (la entrada asav2 para el VPN):



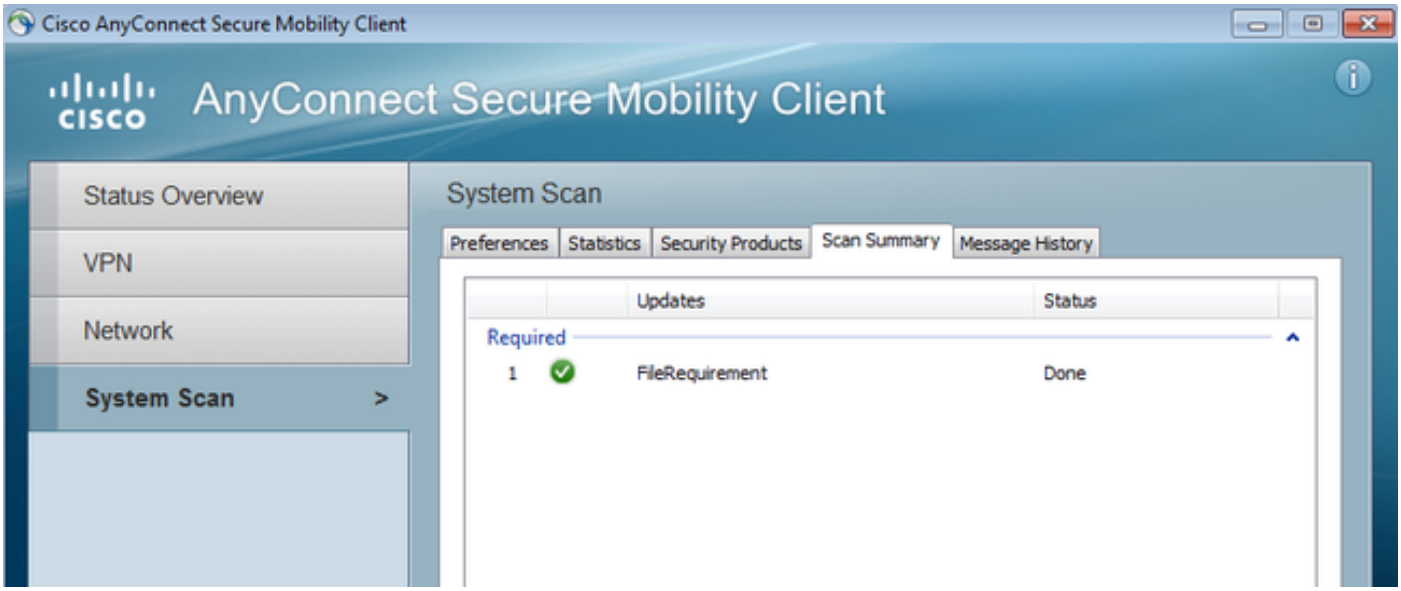
Después de la autenticación, AnyConnect descarga las actualizaciones y también Posture las reglas para las cuales se realiza la verificación:



En esta etapa, pudo todavía haber acceso limitado (usted encuentra la regla desconocida de la autorización en el ISE). Una vez que la estación es obediente, eso es señalada por el módulo de la postura:



Los detalles pueden también ser verificados (se satisface el FileRequirement):

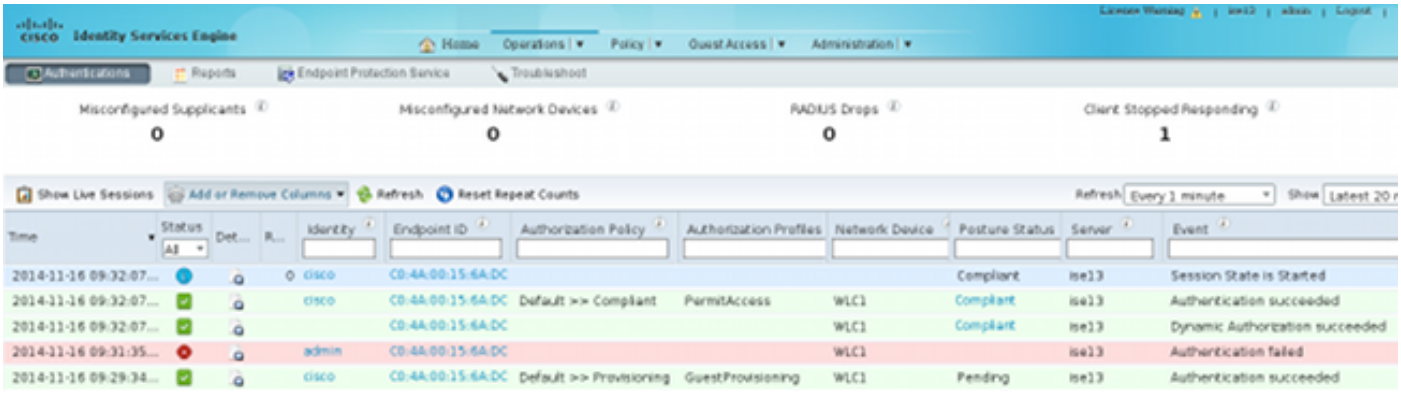


El historial del mensaje muestra los pasos detallados:

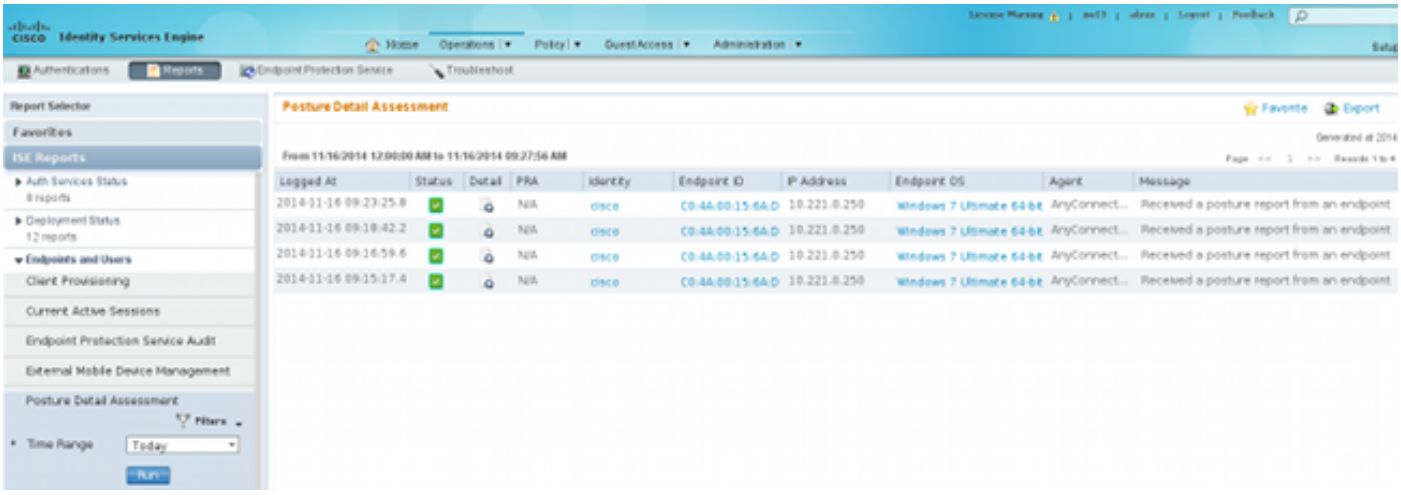
```
9:18:38 AM The AnyConnect Downloader is performing update checks...
9:18:38 AM Checking for profile updates...
9:18:38 AM Checking for product updates...
```

```
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.
```

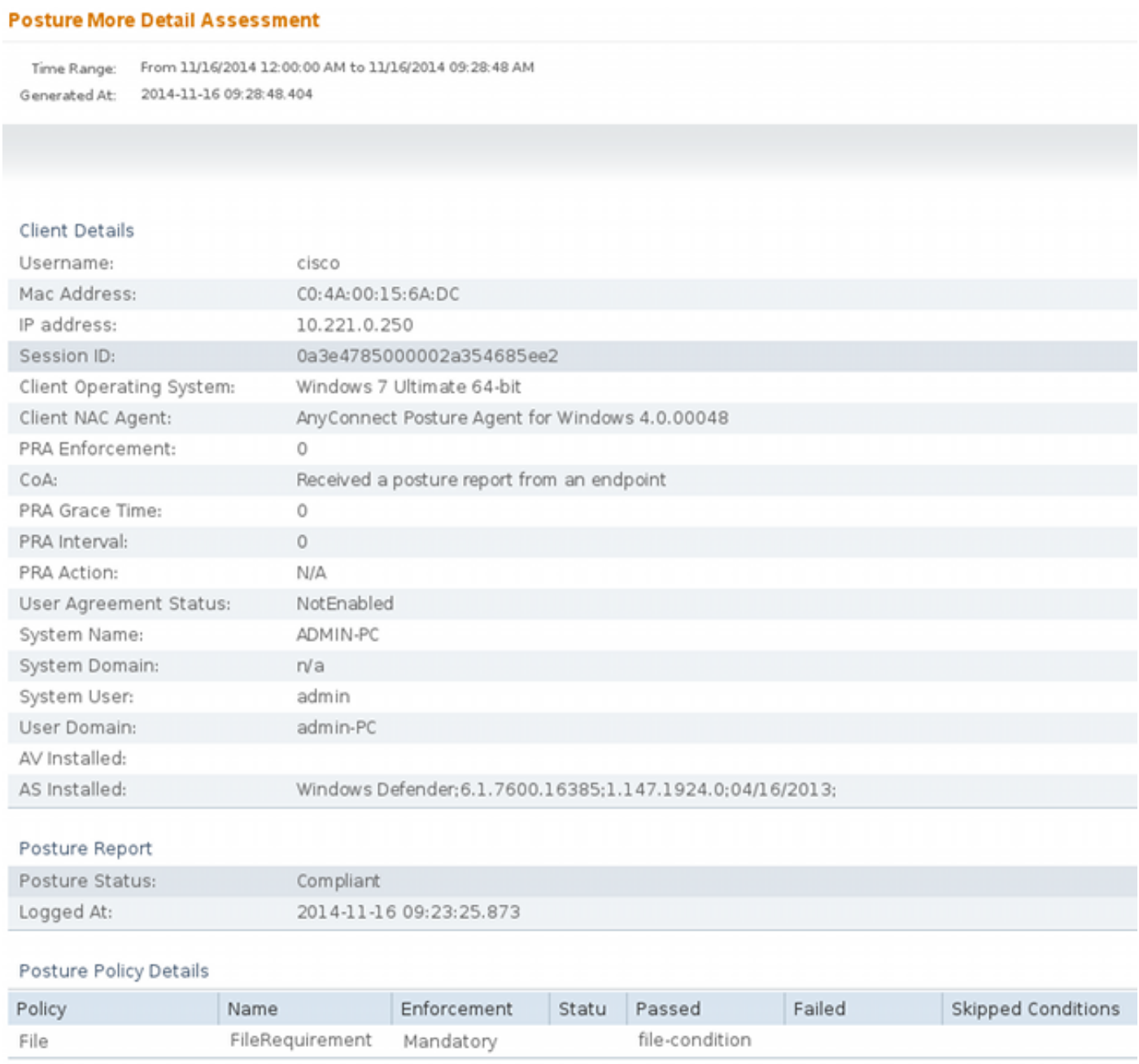
El informe acertado se envía al ISE, que acciona el cambio de la autorización. La segunda autenticación encuentra la regla obediente y se concede el acceso a la red completo. Si el informe de la postura se envía mientras que todavía está asociado al SSID de disposición, estos registros se considera en el ISE:



El informe de la postura indica:



Los informes detallados muestran el FileRequirement se satisface que:



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		

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Servicios de la postura en la guía de configuración de Cisco ISE
- Guía de administradores de Cisco ISE 1.3
- Soporte Técnico y Documentación - Cisco Systems