Integração de AnyConnect 4.0 com exemplo de configuração da versão 1.3 ISE

Índice

Introdução

Este original descreve a funcionalidade nova na versão 1.3 do Cisco Identity Services Engine (ISE) que permite que você configure diversos módulos seguros do cliente da mobilidade de AnyConnect e os provision automaticamente ao valor-limite. Este original apresenta como configurar os módulos VPN, de gerente do acesso de rede (NAM), e de postura no ISE e empurrá-los para o usuário corporativo.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Disposições, autenticação, e autorização ISE
- Configuração de controladores do Wireless LAN (WLCs)
- Conhecimento básico VPN e de 802.1x

- Configuração de perfis VPN e NAM com os editores do perfil de AnyConnect

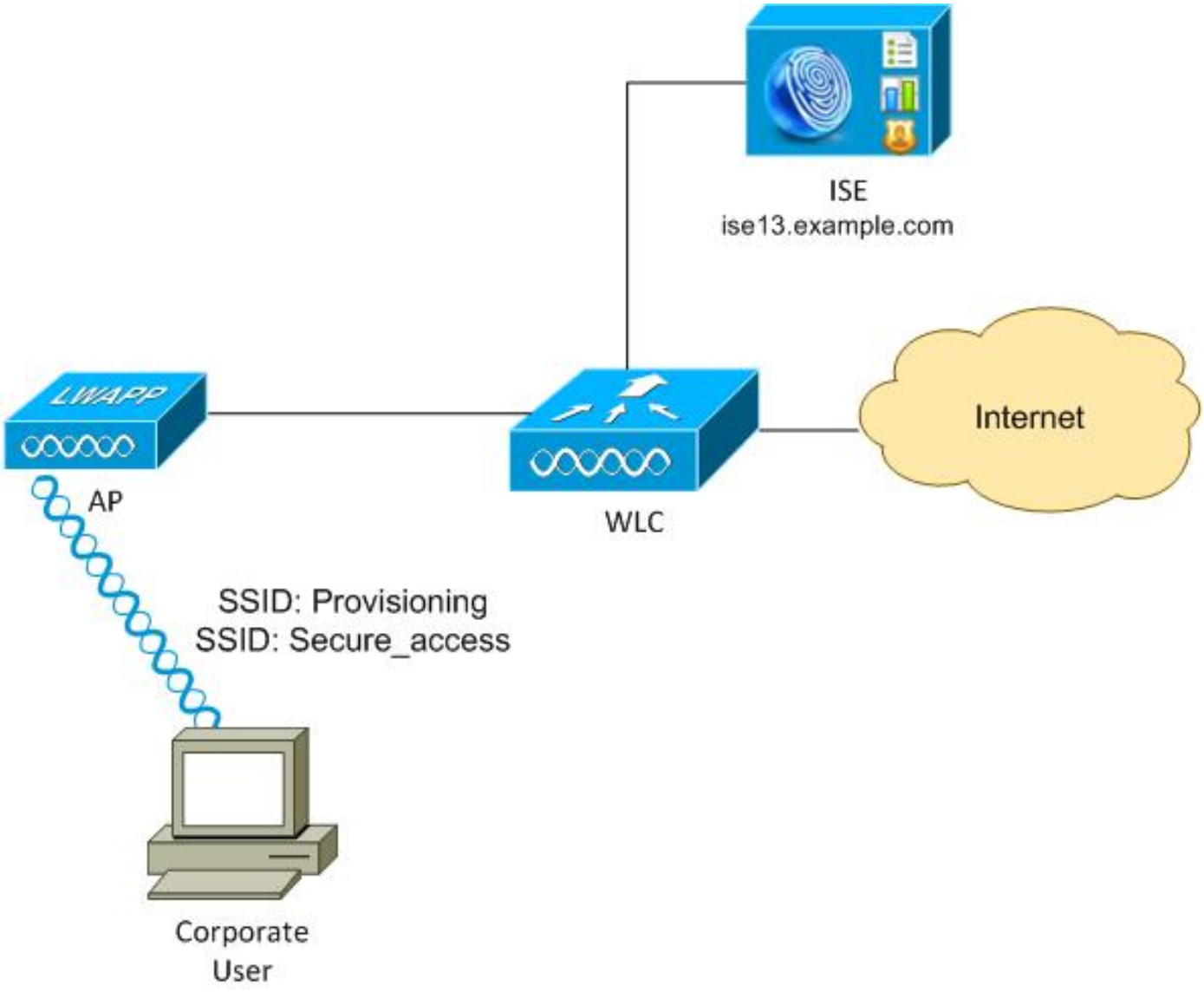
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Versão 7.6 e mais recente de Cisco WLC
- Software de Cisco ISE, versões 1.3 e mais recente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Topologia e fluxo



Está aqui o fluxo:

Etapa 1. Service Set Identifier (SSID) dos acceses do usuário corporativo: Abastecimento. Executa a autenticação do 802.1x com o EAP Protocolo-protegido autenticação extensível (EAP-

PEAP). A regra da autorização do **abastecimento** é encontrada no ISE e o usuário é reorientado para o abastecimento de AnyConnect (através do abastecimento do cliente Protal). Se AnyConnect não é detectado na máquina, todos os módulos configurados estão instalados (VPN, NAM, postura). Junto com esse perfil, a configuração para cada módulo é empurrada.

Etapa 2. Uma vez que AnyConnect é instalado, o usuário deve recarregar o PC. Depois que a repartição, AnyConnect é executado e o SSID correto está usado automaticamente conforme o perfil configurado NAM (Secure_access). EAP-PEAP é usado (como um exemplo, a Segurança da camada do Protocolo-transporte da autenticação extensível (EAP-TLS) poderia igualmente ser usada). Ao mesmo tempo, o módulo da postura verifica se a estação é complacente (verificações para a existência do **arquivo de c:\test.txt**).

Etapa 3. Se o estado da postura da estação é desconhecido (nenhum relatório do módulo da postura), está reorientado ainda para o abastecimento, porque a regra de Authz do **desconhecido** é encontrada no ISE. Uma vez que a estação é complacente, o ISE envia uma mudança da autorização (CoA) ao controlador do Wireless LAN, que provoca a reautenticação. Uma segunda autenticação ocorre, e a regra **complacente** é batida no ISE, que fornecerá o usuário o acesso direto à rede.

Em consequência, o usuário provisioned com AnyConnect VPN, NAM, e módulos da postura que permitem o acesso unificado à rede. A funcionalidade similar pode ser usada na ferramenta de segurança adaptável (ASA) para o acesso VPN. Atualmente, o ISE pode fazer o mesmos para qualquer tipo de acesso com uma aproximação muito granulada.

Esta funcionalidade não é limitada aos usuários corporativos, mas é possivelmente a mais comum distribui-la para esse grupo de usuários.

Configurar

WLC

O WLC é configurado com dois SSID:

- Abastecimento - [WPA + WPA2][Auth(802.1X)]. Este SSID é usado para o abastecimento de AnyConnect.
- Secure_access - [WPA + WPA2][Auth(802.1X)]. Este SSID está usado para o acesso seguro depois que o valor-limite provisioned com o módulo de NAM que está configurado para esse SSID.

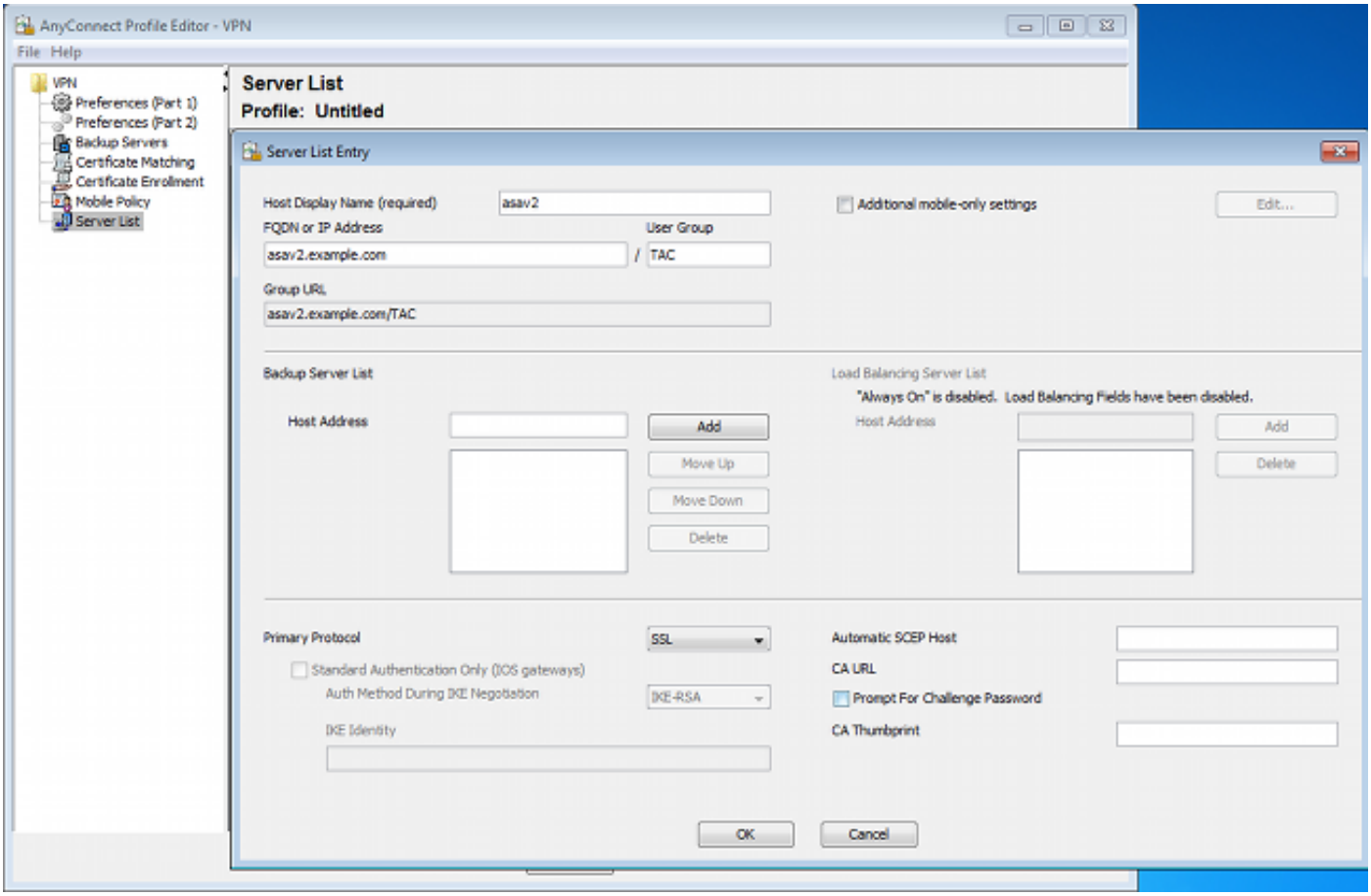
ISE

Etapa 1. Adicionar o WLC

Adicionar o WLC aos dispositivos de rede no ISE.

Etapa 2. Configurar o perfil VPN

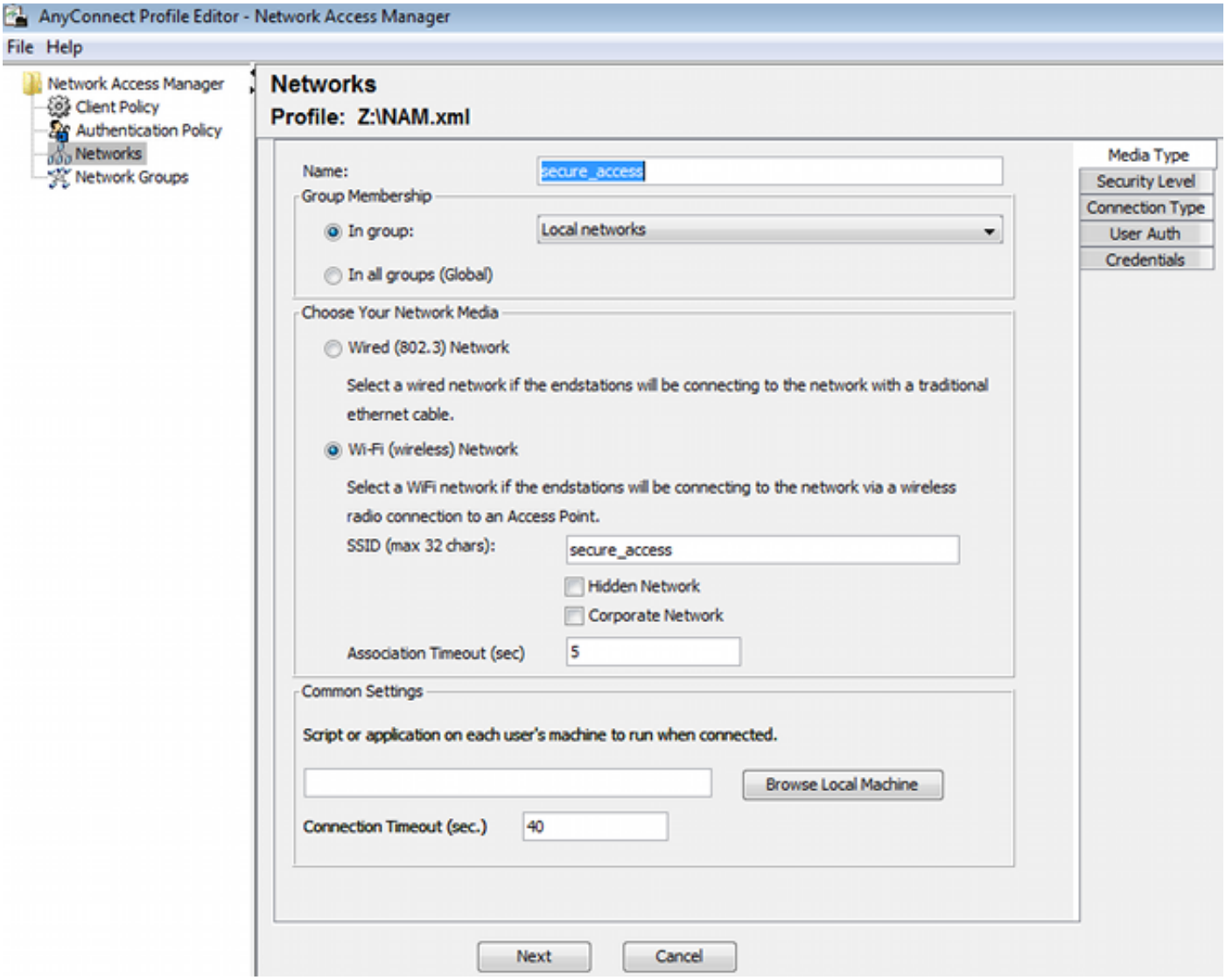
Configurar o perfil VPN com o editor do perfil de AnyConnect para o VPN.



Somente uma entrada foi adicionada para o acesso VPN. Salvar que arquivo XML a **VPN.xml.**

Etapa 3. Configurar o perfil NAM

Configurar o perfil NAM com o editor do perfil de AnyConnect para o NAM.



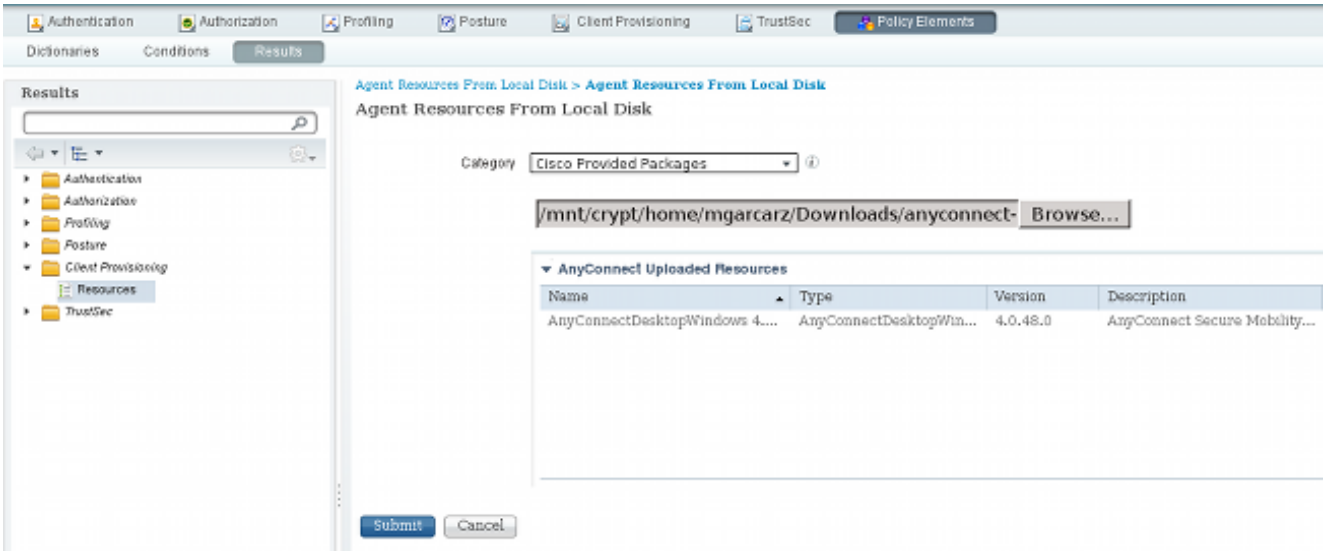
Somente um SSID foi configurado: **secure_access**. Salvar que arquivo XML a **NAM.xml.**

Etapa 4. Instale o aplicativo

1. Transfira o aplicativo manualmente do cisco.com.

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

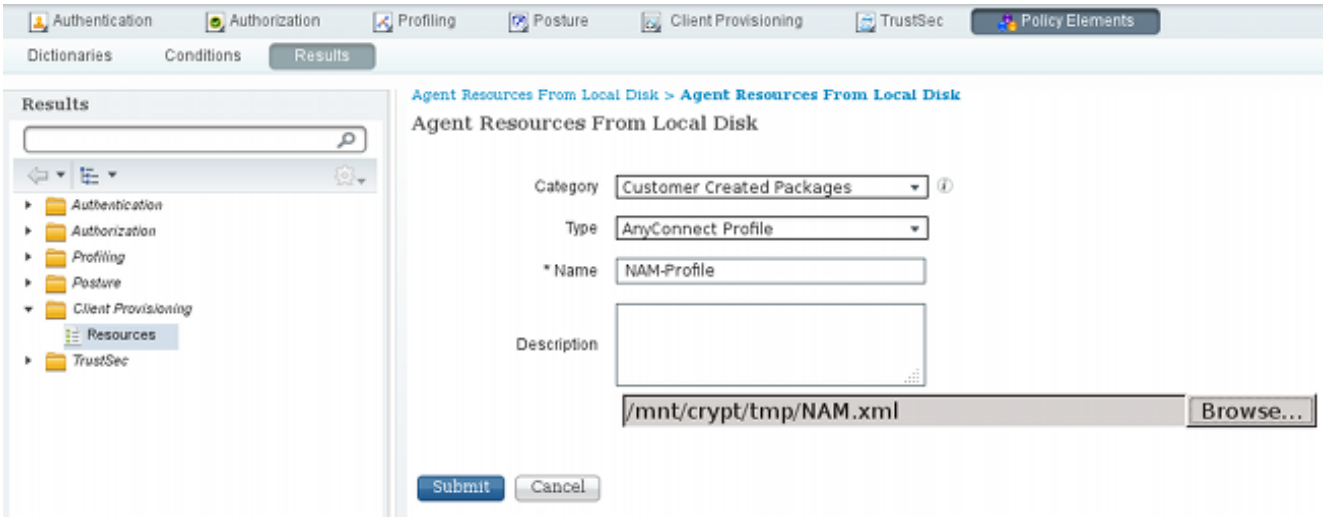
2. No ISE, navegue à **política > aos resultados > ao abastecimento > aos recursos do cliente**, e adicionar recursos de agente do disco local.
3. Escolha Cisco forneceu pacotes e selecionam o **anyconnect-win-4.0.00048-k9.pkg**:



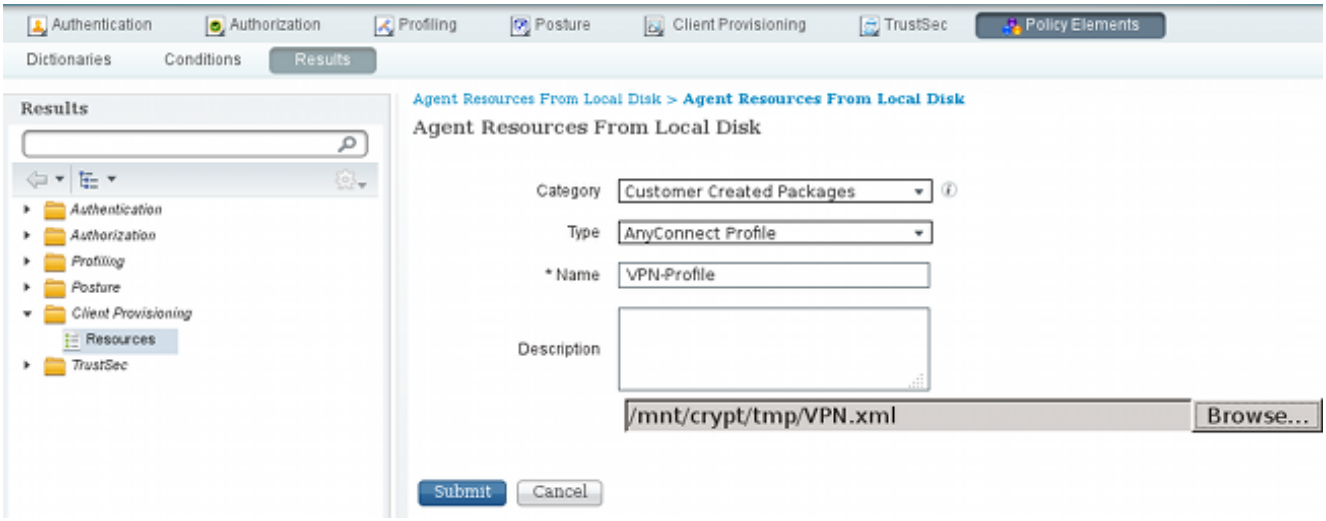
4. Repita etapa 4 para o módulo da conformidade.

Etapa 5. Instale o perfil VPN/NAM

1. Navegue à **política > aos resultados > ao abastecimento > aos recursos do cliente**, e adicionar recursos de agente do disco local.
2. Escolha pacotes e o tipo criados cliente **perfil de AnyConnect**. Selecione o perfil previamente criado NAM (arquivo XML):



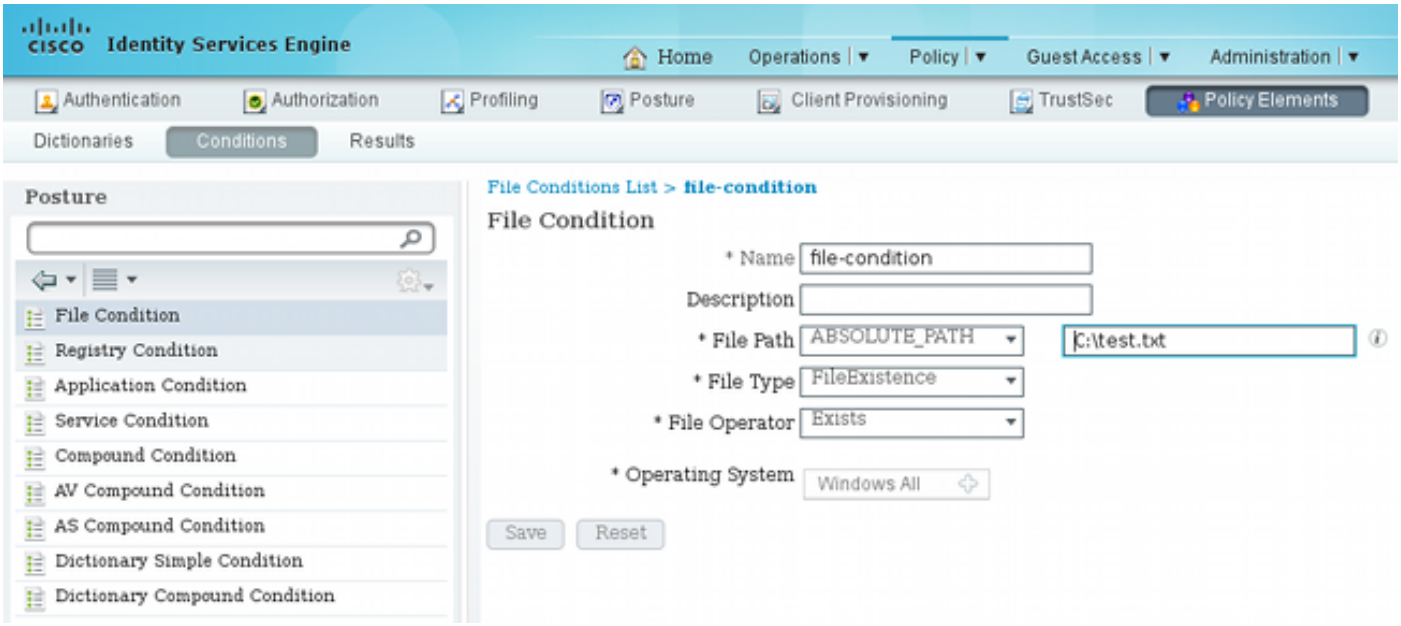
3. Repita etapas similares para o perfil VPN:



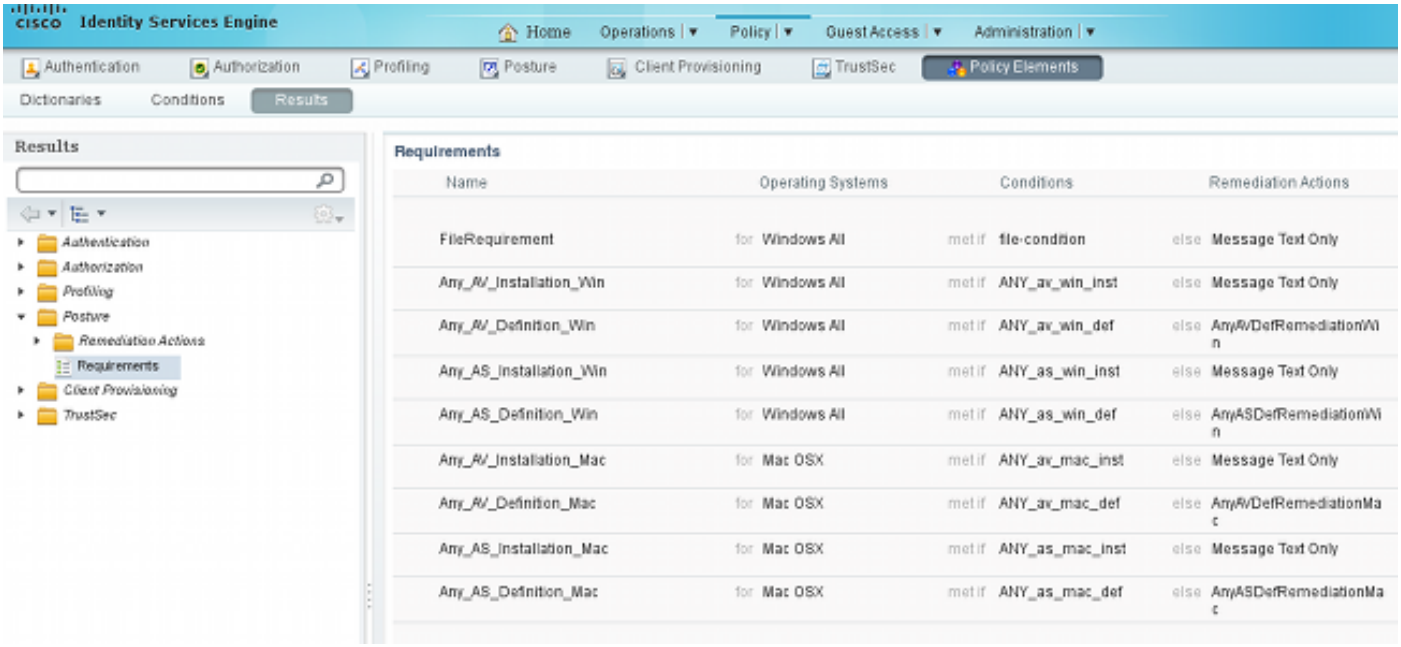
Etapa 6. Configurar a postura

Os perfis NAM e VPN têm que ser configurados externamente com o editor do perfil de AnyConnect e ser importados no ISE. Mas a postura é configurada inteiramente no ISE.

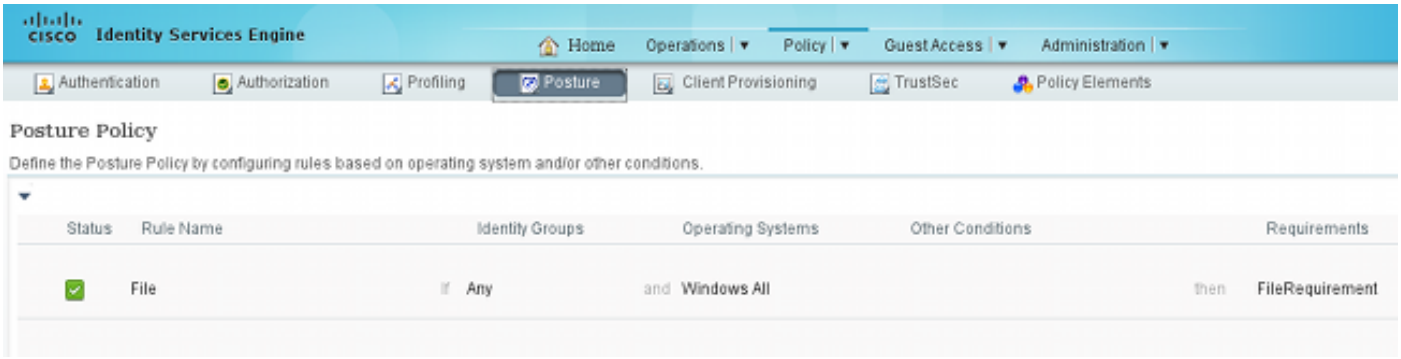
Navegue à **política > às circunstâncias > à postura > ao arquivo Condition.You** pode ver que uma condição simples para a existência do arquivo esteve criada. Você deve ter esse arquivo a fim ser complacente com a política verificada pelo módulo da postura:



Esta circunstância é usada para uma exigência:



E a exigência é usada na política da postura para sistemas de Microsoft Windows:

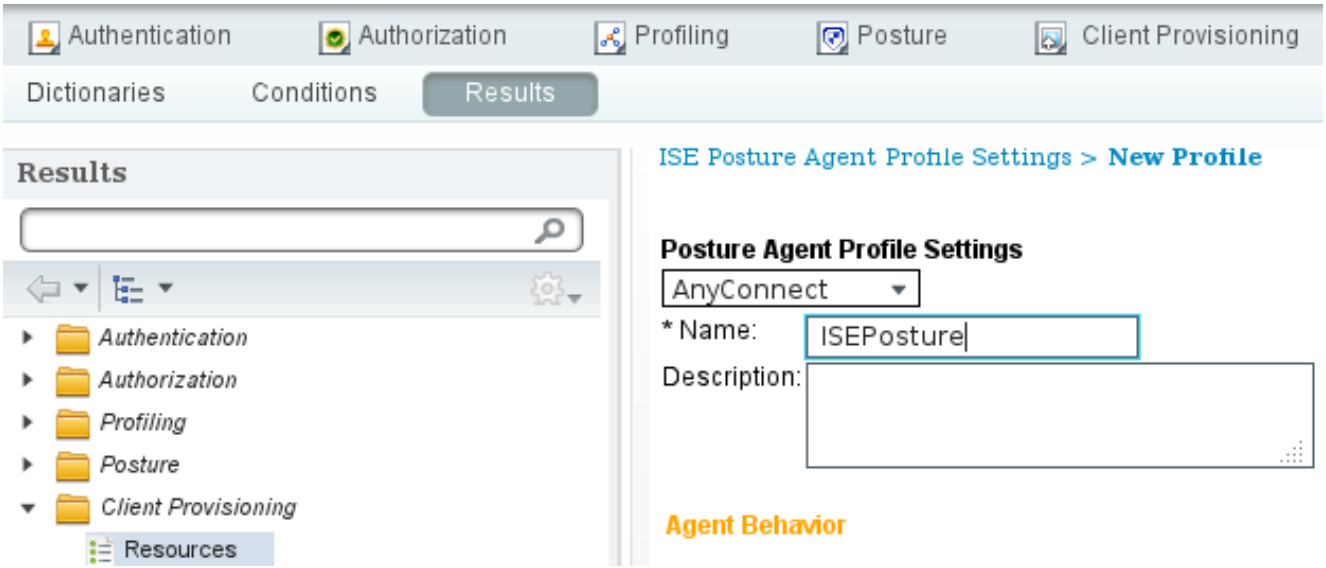


Para obter mais informações sobre da configuração da postura, refira serviços da postura no manual de configuração de Cisco ISE.

Uma vez que a política da postura está pronta, é hora de adicionar a configuração de agente da postura.

1. Navegue à **política > aos resultados > ao abastecimento > aos recursos do cliente** e adicionar o perfil da postura do agente do Network Admission Control (NAC) ou do agente de AnyConnect.

2. AnyConnect seleto (um módulo novo da postura da versão 1.3 ISE foi usado em vez do agente velho NAC):



3. Da seção de protocolo da postura, não esqueça adicionar ***** a fim permitir que o agente conecte a todos os server.

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. Se o campo das regras do nome de server é saido vazio, o ISE não salvar ajustes e relata este erro:

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

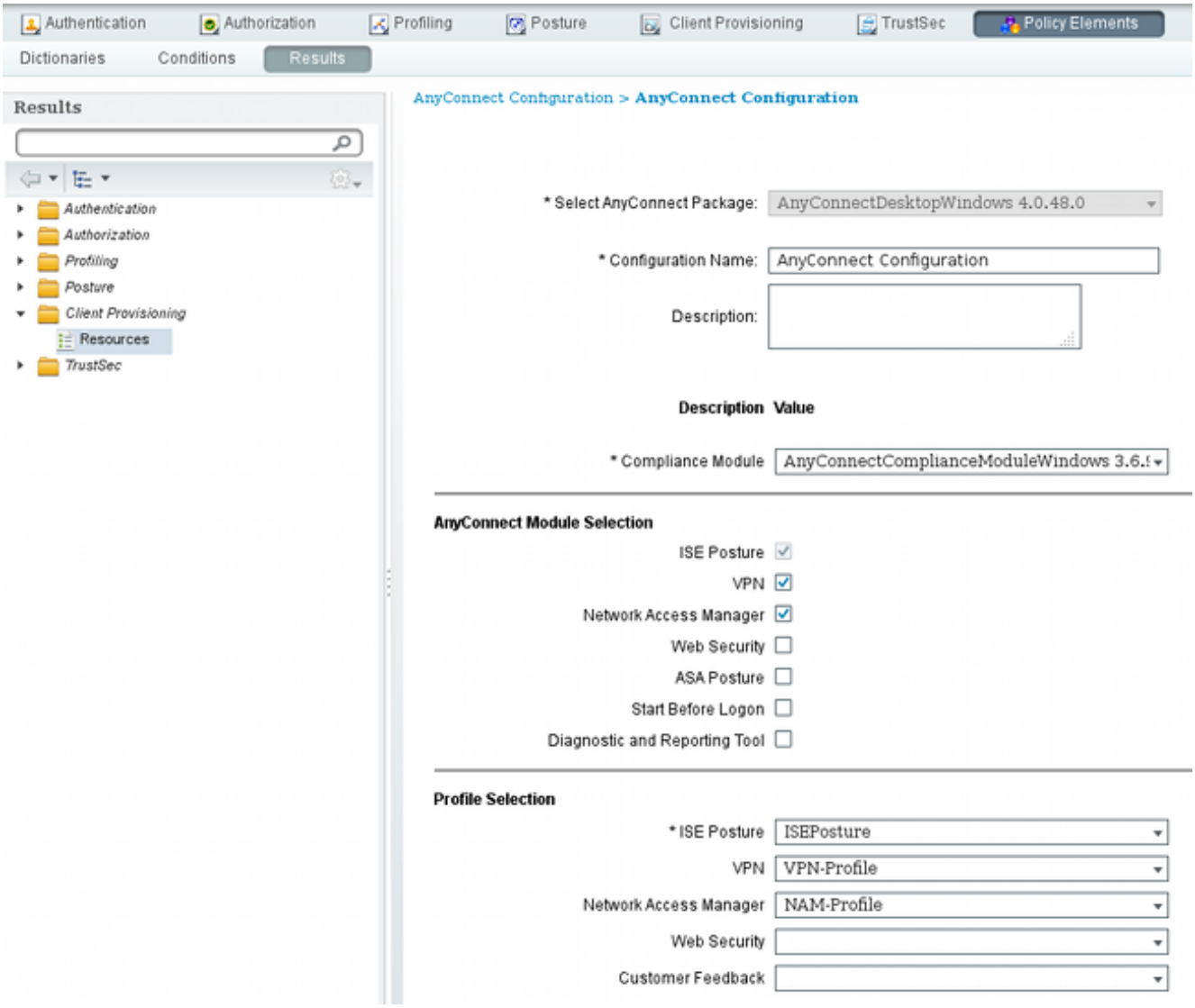
Etapa 7. Configurar AnyConnect

Nesta fase, todos os aplicativos (AnyConnect) e a configuração de perfil para todos os módulos (VPN, NAM, e postura) foram configurados. É hora de ligá-lo junto.

1. Navegue à **política > aos resultados > ao abastecimento > aos recursos do cliente**, e adicionar a configuração de AnyConnect.

2. Configurar o nome e selecione módulo da conformidade e todos os módulos exigidos de AnyConnect (VPN, NAM, e postura).

3. Na seleção do perfil, escolha o perfil configurado mais cedo para cada módulo.



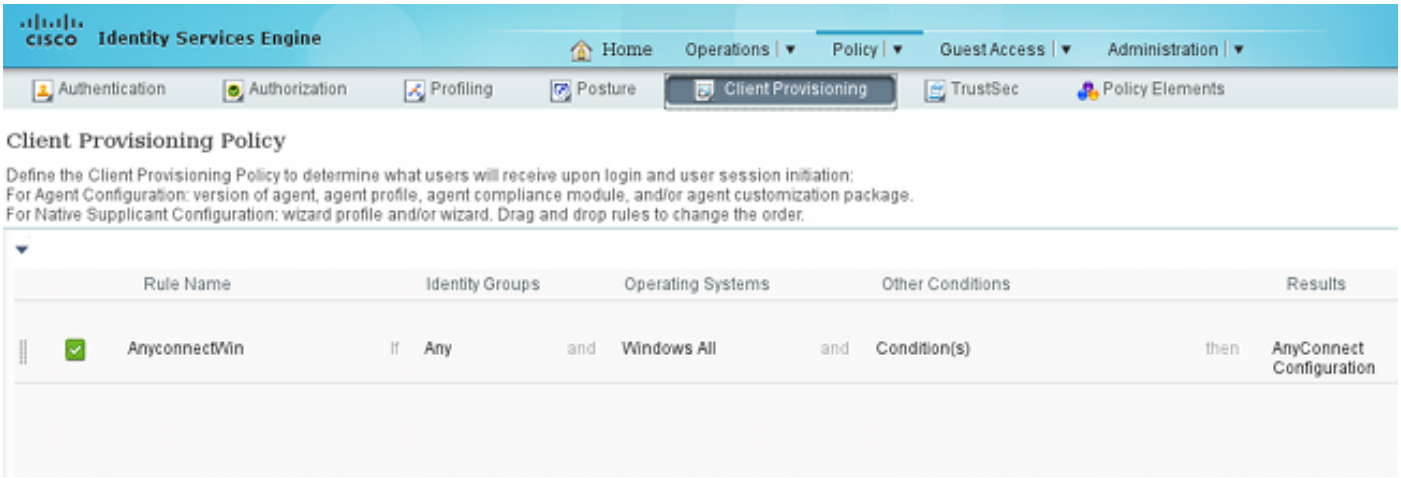
4. O módulo de VPN é imperativo para que todos módulos restantes funcionem corrrectly. Mesmo se o módulo de VPN não é selecionado para a instalação, será empurrado e instalado no cliente. Se você não quer usar o VPN, há uma possibilidade para configurar um perfil especial para o VPN que esconde a interface do utilizador para o módulo de VPN. Estas linhas devem ser adicionadas ao **arquivo VPN.xml:**

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

5. Este tipo do perfil é instalado igualmente quando você usa **Setup.exe do** pacote iso (anyconnect-win-3.1.06073-pre-deploy-k9.iso**).** Então, o **perfil** VPNDisable_ServiceProfile.xml para o VPN é instalado junto com a configuração, que desabilita a interface do utilizador para o módulo de VPN.

Etapa 8. Regras do abastecimento do cliente

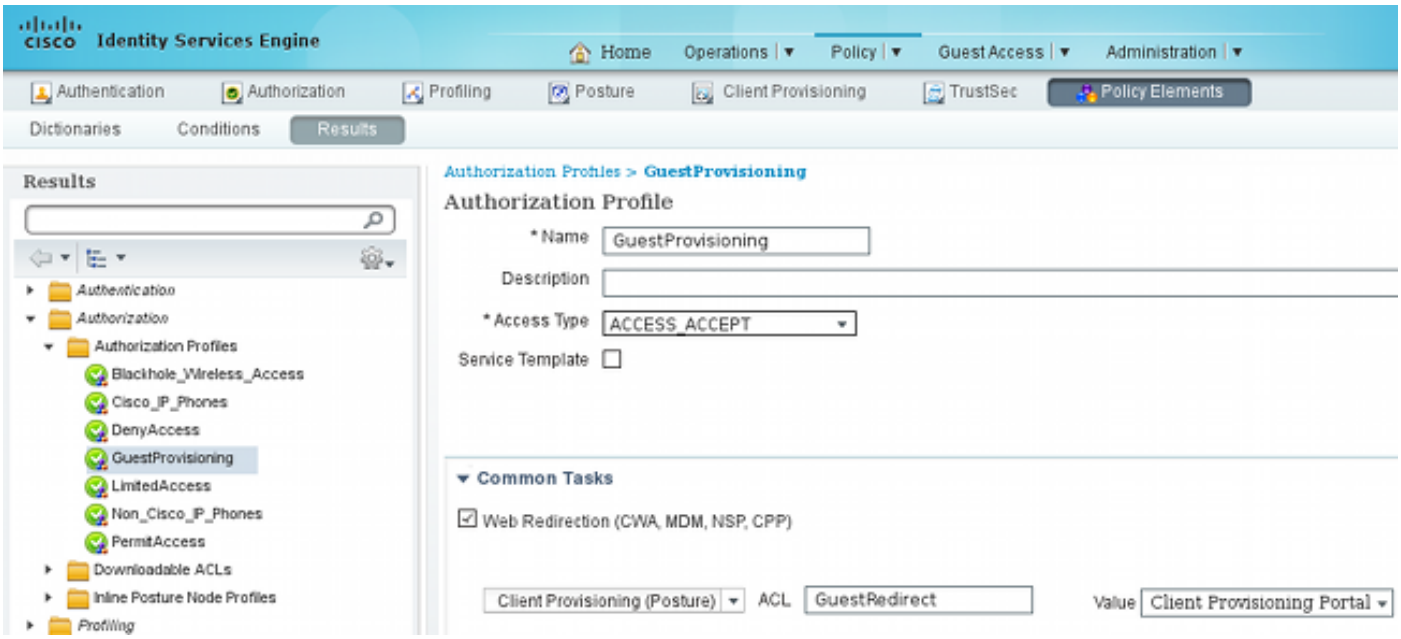
A configuração de AnyConnect criada na etapa 7 deve ser provida nas regras do abastecimento do cliente:



As regras do abastecimento do cliente decidem que aplicativo será empurrado para o cliente. Somente uma regra é precisada aqui com o resultado que aponta à configuração criada na etapa 7. Esta maneira, todos os valores-limite de Microsoft Windows que são reorientados para o abastecimento do cliente usará a configuração de AnyConnect com todos os módulos e perfis.

Etapa 9. Perfis da autorização

O perfil da autorização para o abastecimento do cliente precisa de ser criado. O portal do abastecimento do cliente do padrão é usado:



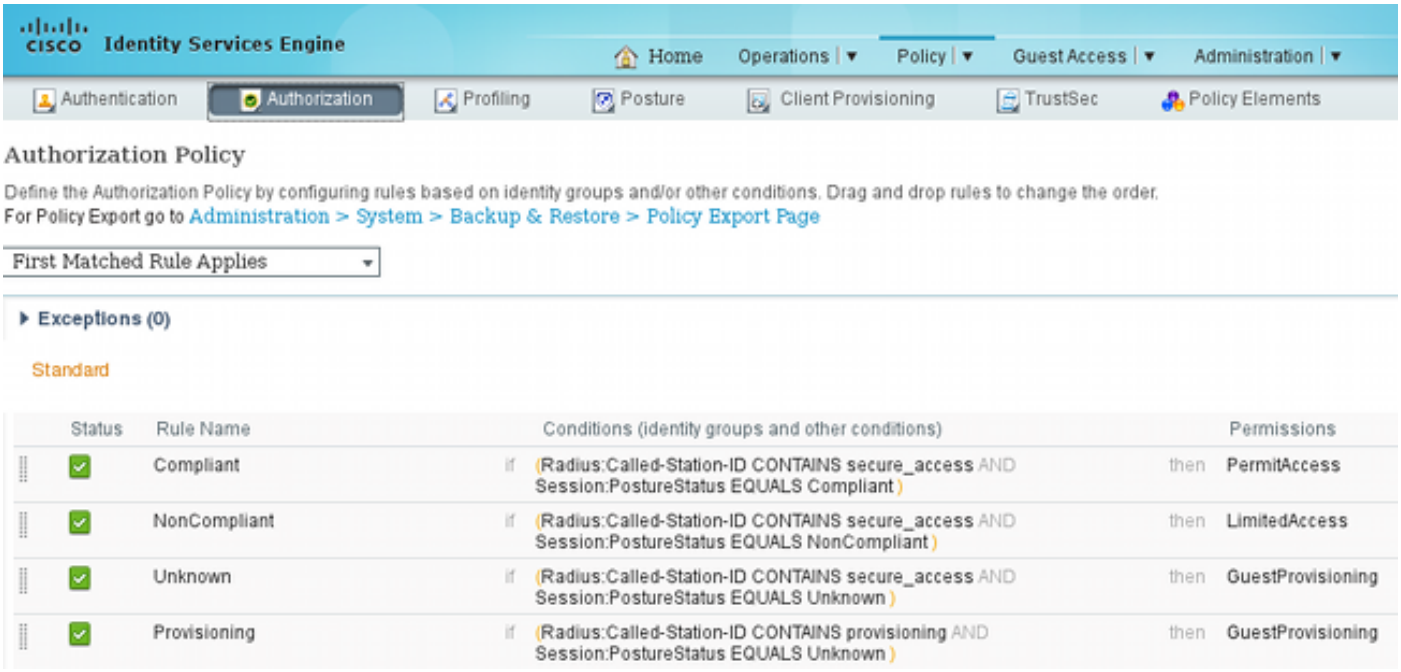
Este perfil força os usuários a ser reorientado para o abastecimento ao portal do abastecimento do cliente do padrão. Este portal avalia a política de Provisiong do cliente (regras criadas em etapa 8). Os perfis da autorização são os resultados das regras da autorização configuradas na etapa 10.

O Access Control List de GuestRedirect (ACL) é o nome do ACL definido no WLC. Este ACL decide que tráfego deve ser reorientado ao ISE. Para mais informação, refira a autenticação da Web central com um exemplo de configuração do interruptor e do Identity Services Engine.

Há igualmente um outro perfil da autorização que forneça o acesso de rede limitado (DACL) para os usuários NON-complacentes (chamados LimitedAccess).

Etapa 10. Regras da autorização

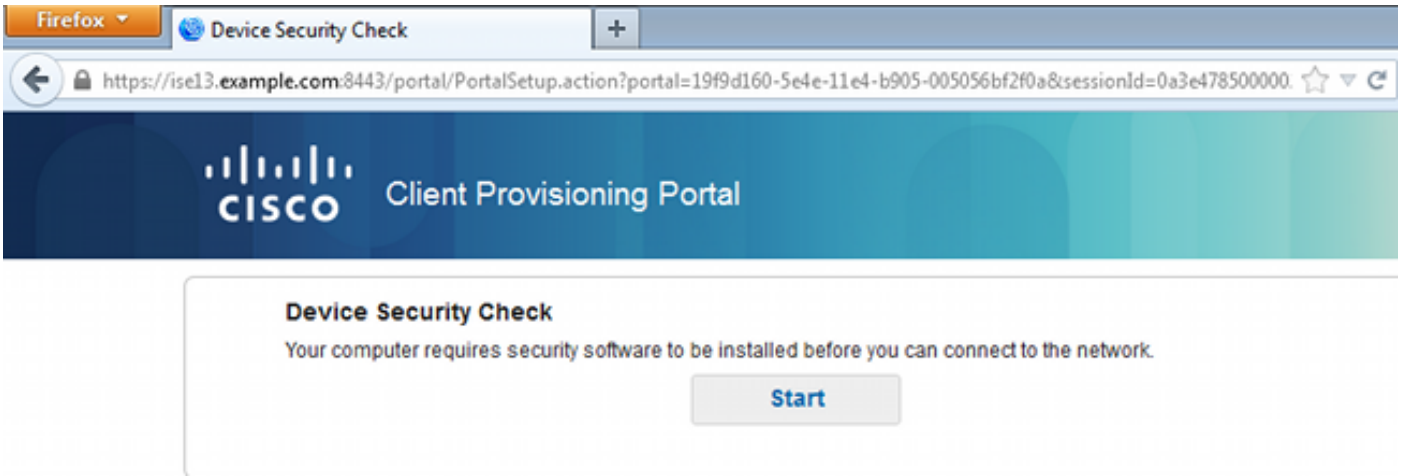
Todo o aqueles são combinados em quatro regras da autorização:



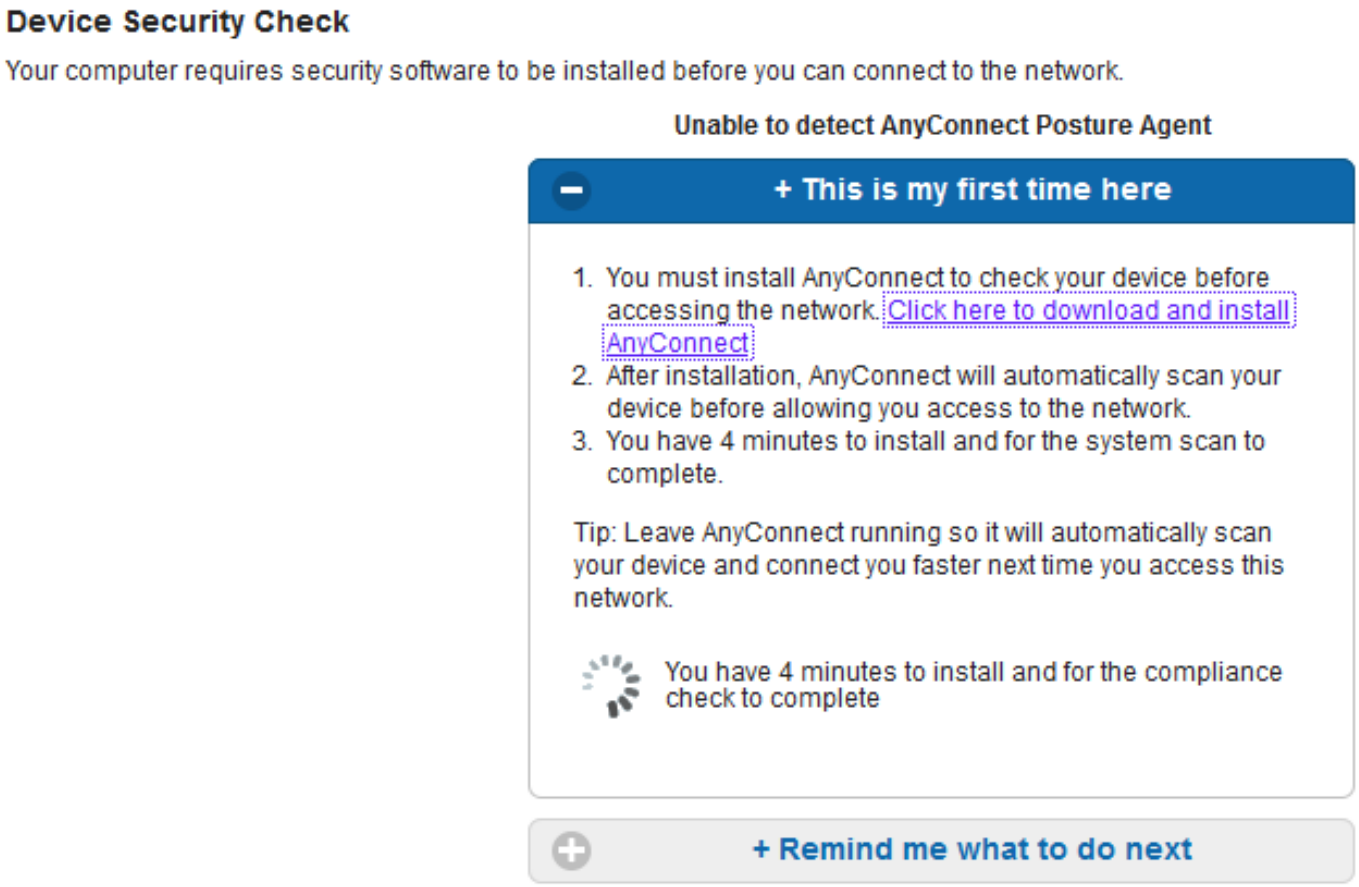
Você conecta ao abastecimento SSID e é reorientado primeiramente para o abastecimento a um portal do abastecimento do cliente do padrão (regra Abastecimento Nomeado). Uma vez que você conecta ao **Secure_access** SSID, ainda reorienta para o abastecimento se nenhum relatório do módulo da postura é recebido por ISE (regra Desconhecido Nomeado). Uma vez que o valor-limite é inteiramente complacente, o acesso direto está concedido (nome da regra complacente). Se o valor-limite é relatado como NON-complacente, limitou o acesso de rede (regra NonCompliant Nomeado).

Verificar

Você associa com o abastecimento SSID, tenta alcançar todo o página da web, e é reorientado ao portal do abastecimento do cliente:

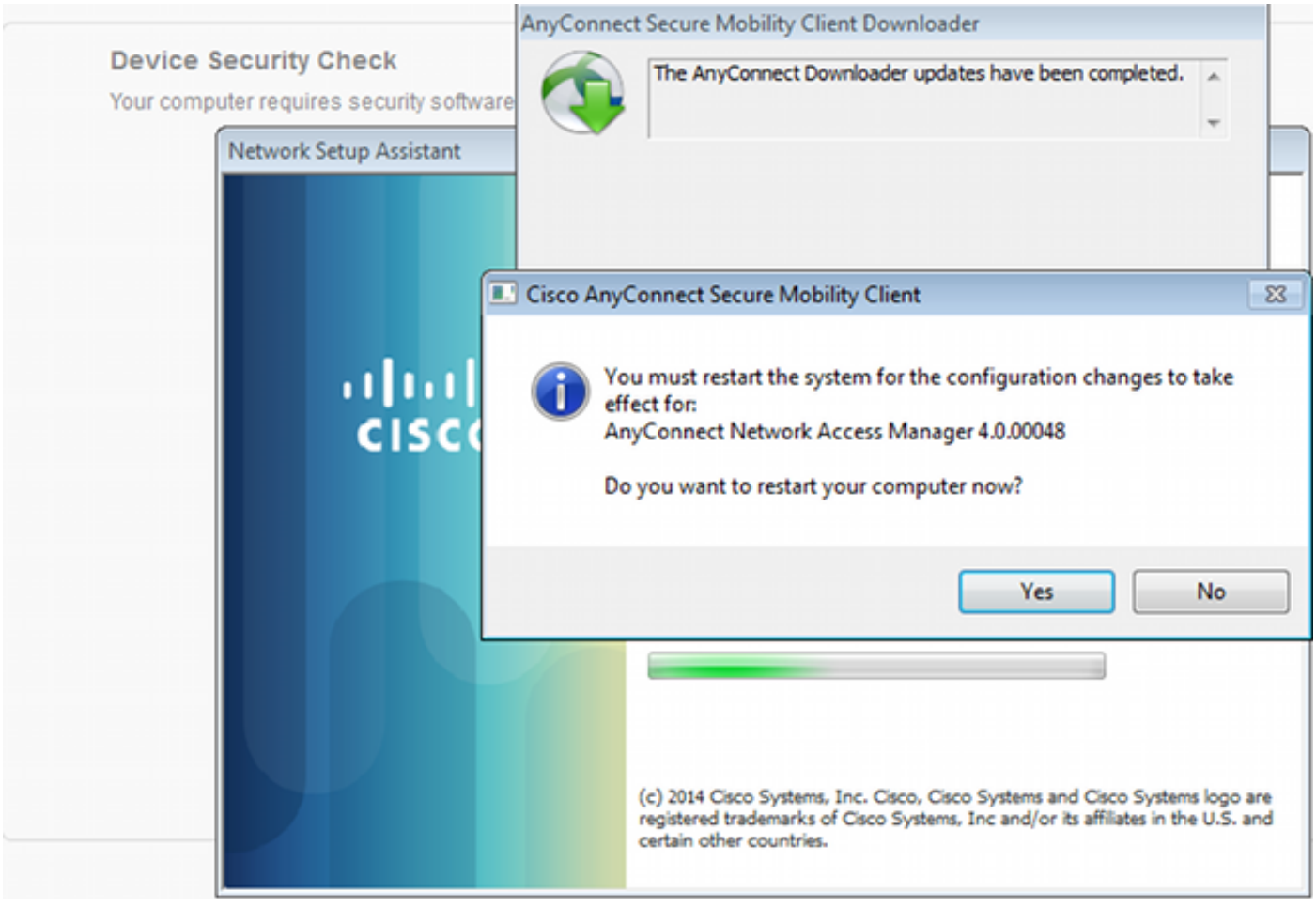


Desde que AnyConnect não é detectado, você é pedido para instalá-lo:

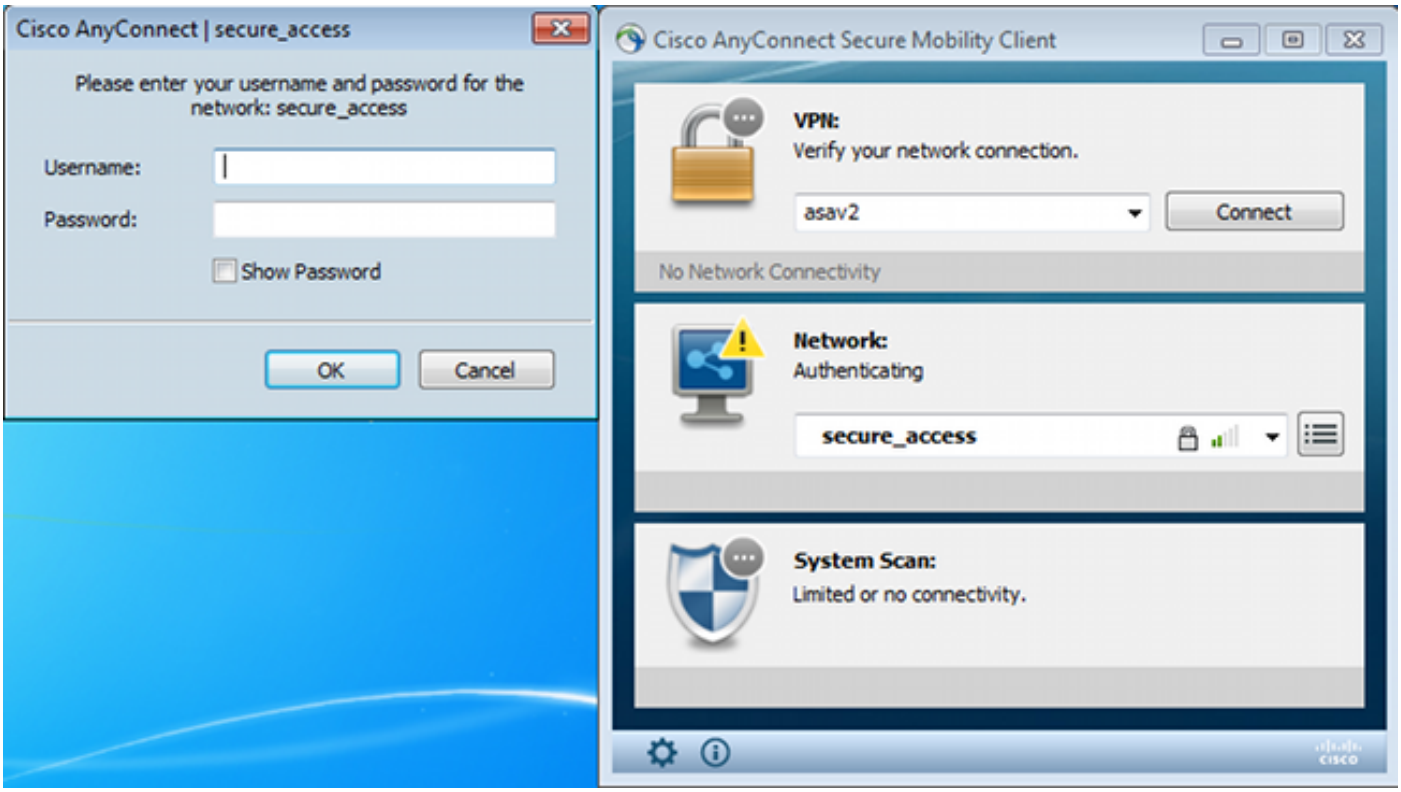


Um aplicativo pequeno chamou o assistente da instalação de rede, que é responsável para o processo de instalação inteiro, é transferido. Observe que é diferente do que o assistente da instalação de rede na versão 1.2.

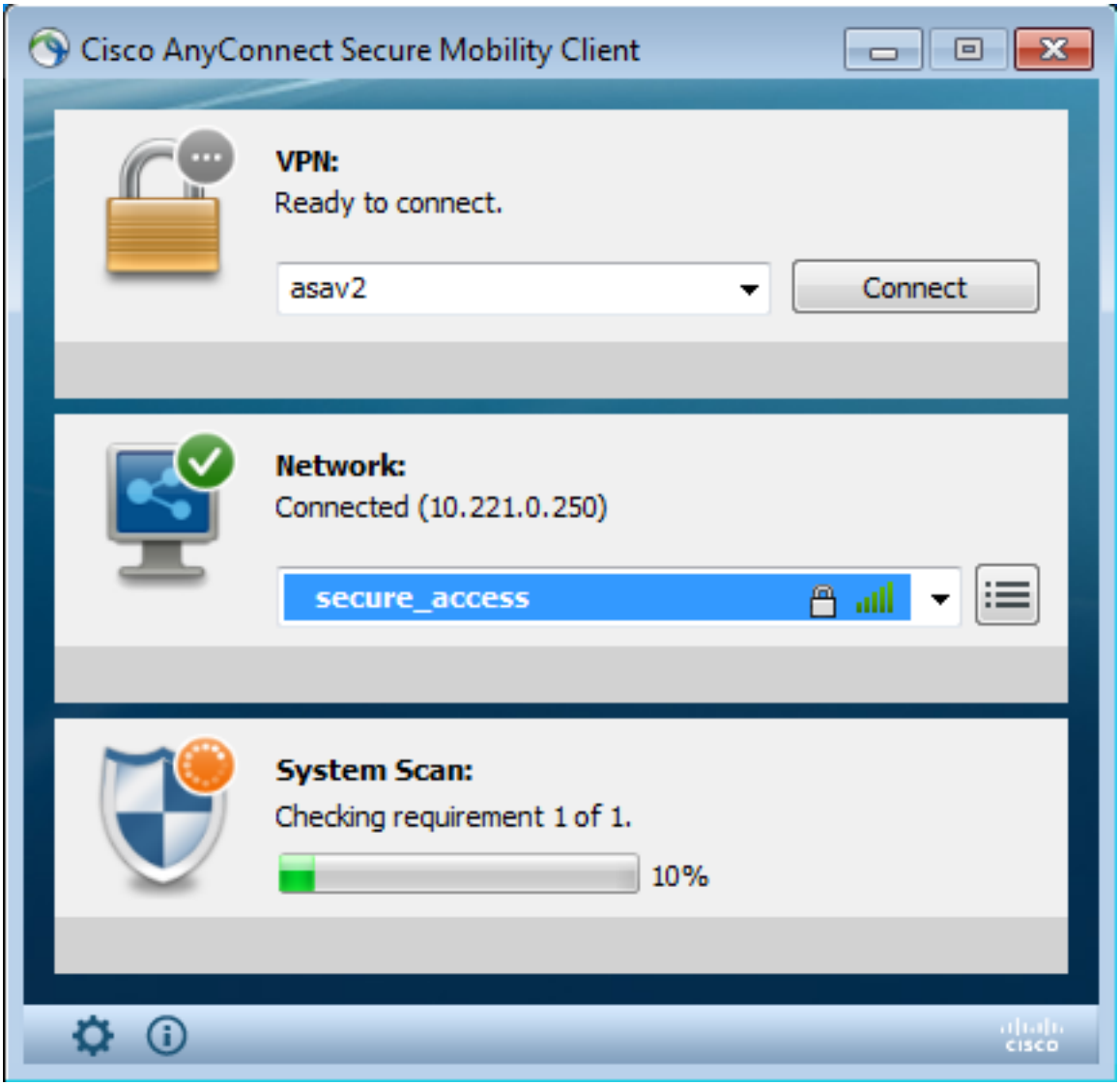
Todos os módulos (VPN, NAM, e postura) são instalados e configurados. Você deve recarregar seu PC:



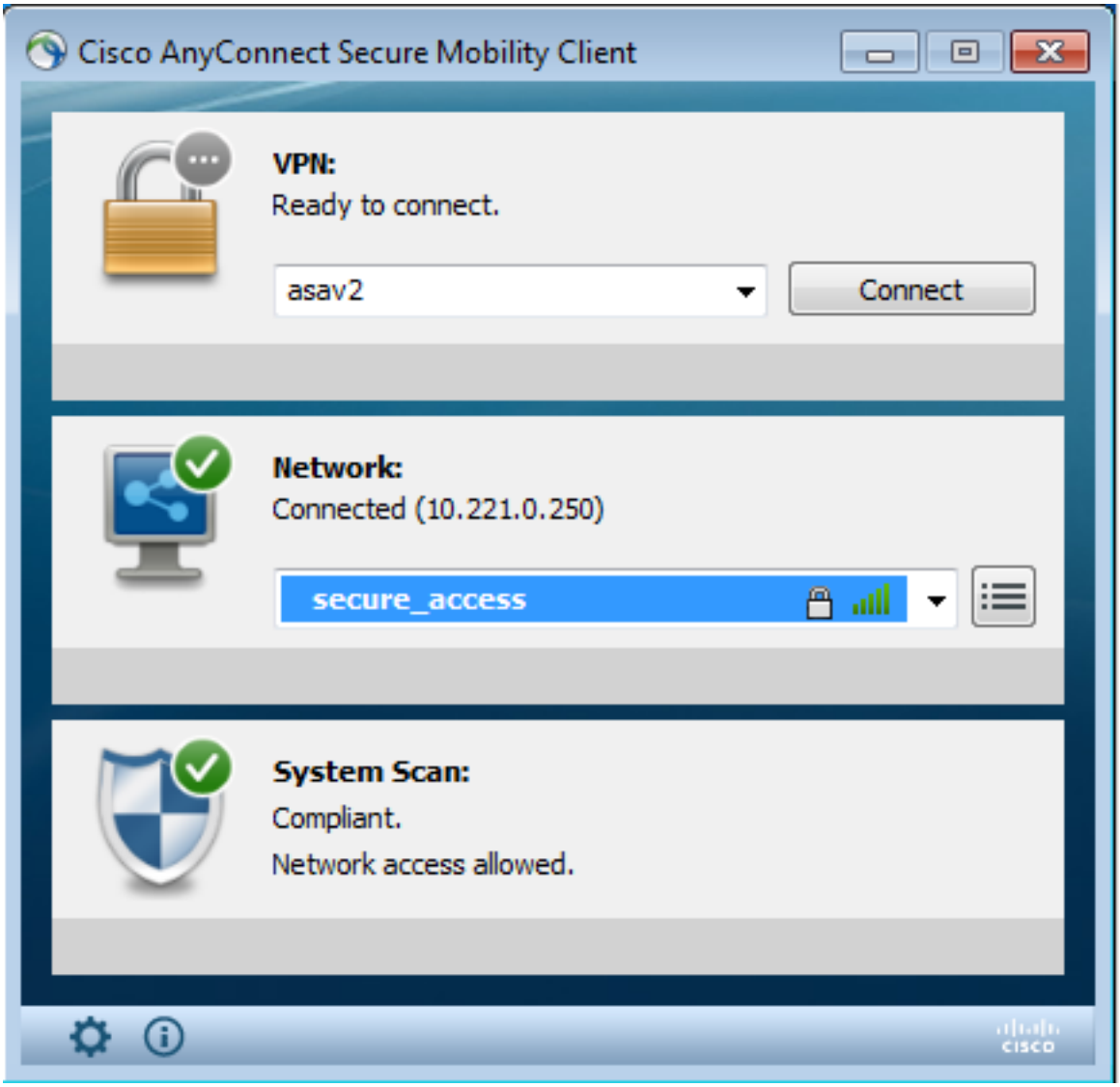
Depois que a repartição, AnyConnect é executada automaticamente e tentativa NAM para associar com os secure_access SSID (conforme o perfil configurado). Observe que o perfil VPN está instalado corretamente (entrada asav2 para o VPN):



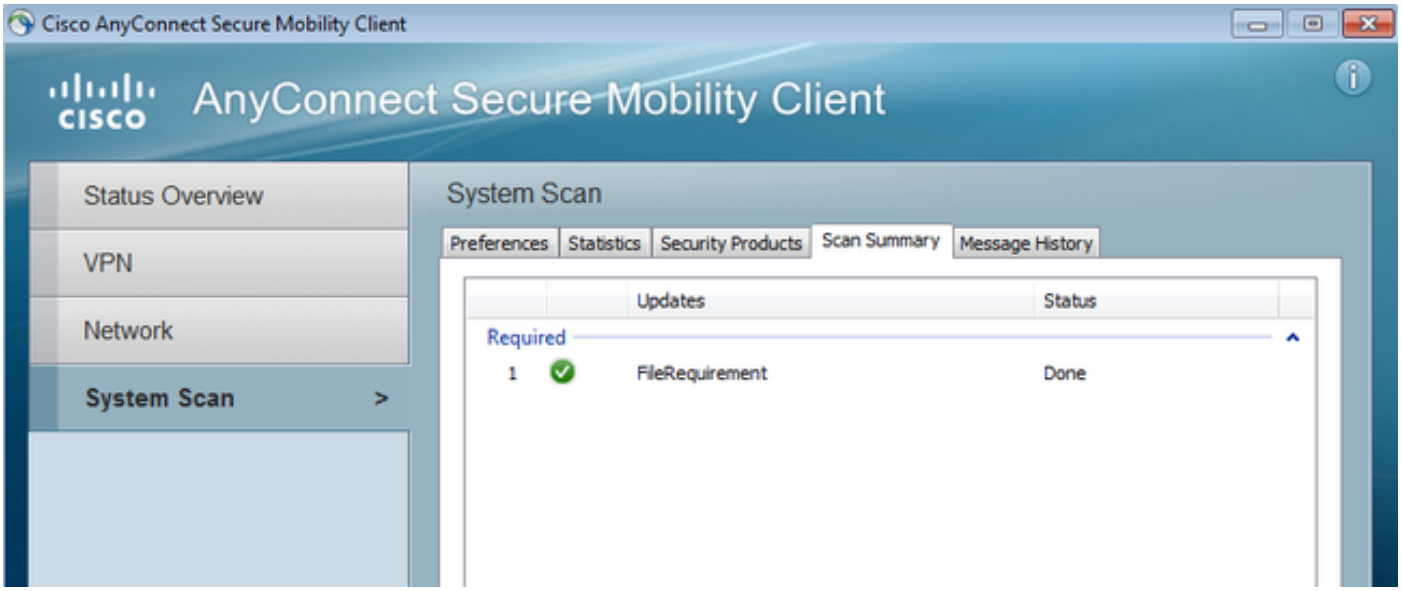
Após a autenticação, AnyConnect transfere atualizações e igualmente Posture as regras para que a verificação é executada:



Nesta fase, pôde ainda haver um acesso limitado (você encontra a regra desconhecida da autorização no ISE). Uma vez que a estação é complacente, aquela está relatada pelo módulo da postura:



Os detalhes podem igualmente ser verificados (o FileRequirement é satisfeito):

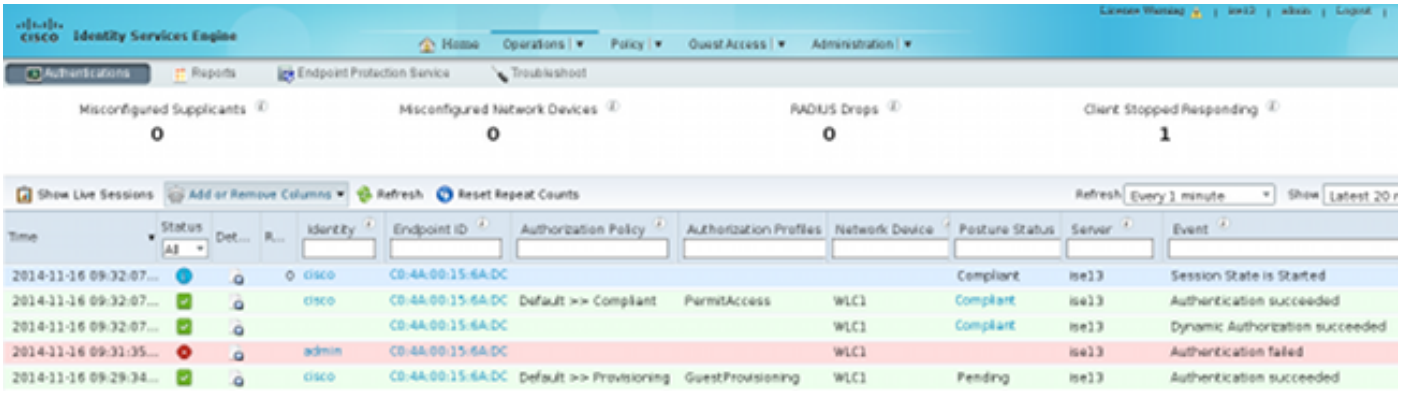


A história da mensagem mostra etapas detalhadas:

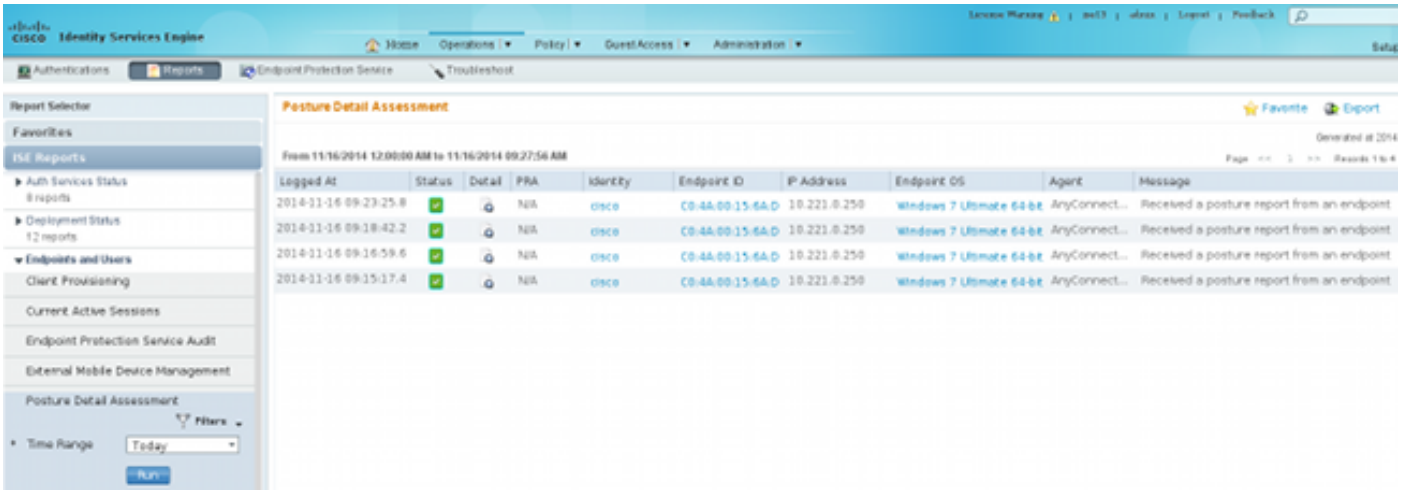
```
9:18:38 AM The AnyConnect Downloader is performing update checks...
9:18:38 AM Checking for profile updates...
9:18:38 AM Checking for product updates...
```

```
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.
```

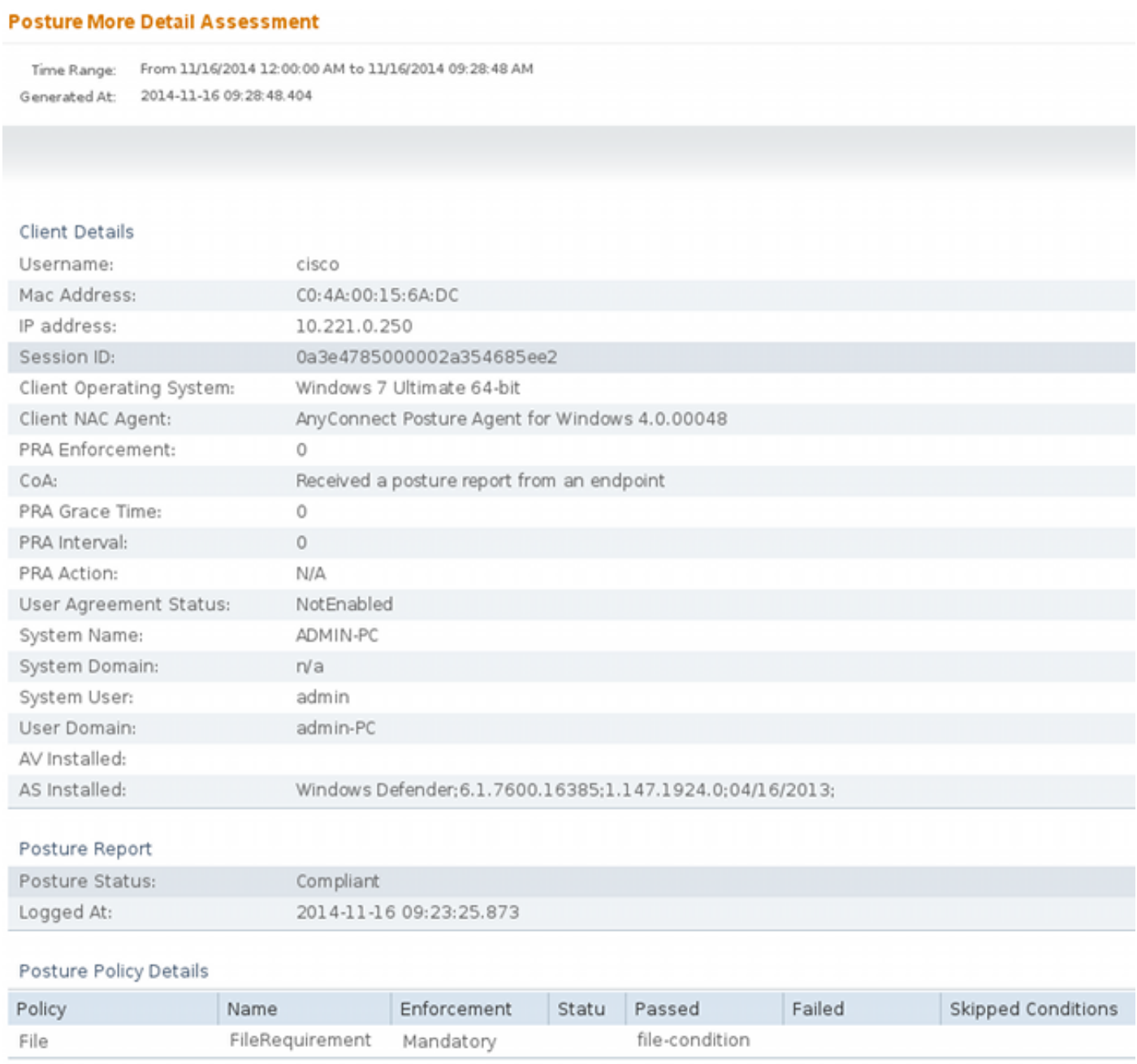
O relatório bem sucedido é enviado ao ISE, que provoca a mudança da autorização. A segunda autenticação encontra a regra complacente e o acesso de rede completo é concedido. Se o relatório da postura está enviado quando ainda associado ao abastecimento SSID, estes logs é considerado no ISE:



O relatório da postura indica:



Os relatórios detalhados mostram o FileRequirement que é satisfeito:



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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Serviços da postura no manual de configuração de Cisco ISE
- Guia de administradores de Cisco ISE 1.3
- Suporte Técnico e Documentação - Cisco Systems