

Esempio di configurazione dell'integrazione di AnyConnect 4.0 con ISE versione 1.3

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia e flusso](#)

[Configurazione](#)

[WLC](#)

[ISE](#)

[Passaggio 1. Aggiungere il WLC](#)

[Passaggio 2. Configurare il profilo VPN](#)

[Passaggio 3. Configurare il profilo NAM](#)

[Passaggio 4. Installare l'applicazione](#)

[Passaggio 5. Installare il profilo VPN/NAM](#)

[Passaggio 6. Configurazione della postura](#)

[Passaggio 7. Configurazione di AnyConnect](#)

[Passaggio 8. Regole di provisioning client](#)

[Passaggio 9. Profili di autorizzazione](#)

[Passaggio 10. Regole di autorizzazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive le nuove funzionalità di Cisco Identity Services Engine (ISE) versione 1.3 che consentono di configurare diversi moduli AnyConnect Secure Mobility Client e di eseguirne il provisioning automatico sull'endpoint. Questo documento illustra come configurare i moduli VPN, Network Access Manager (NAM) e Posture su ISE e spostarli sull'utente aziendale.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Implementazioni, autenticazione e autorizzazione ISE
- Configurazione dei Wireless LAN Controller (WLC)
- VPN di base e conoscenza 802.1x
- Configurazione dei profili VPN e NAM con gli editor di profili AnyConnect

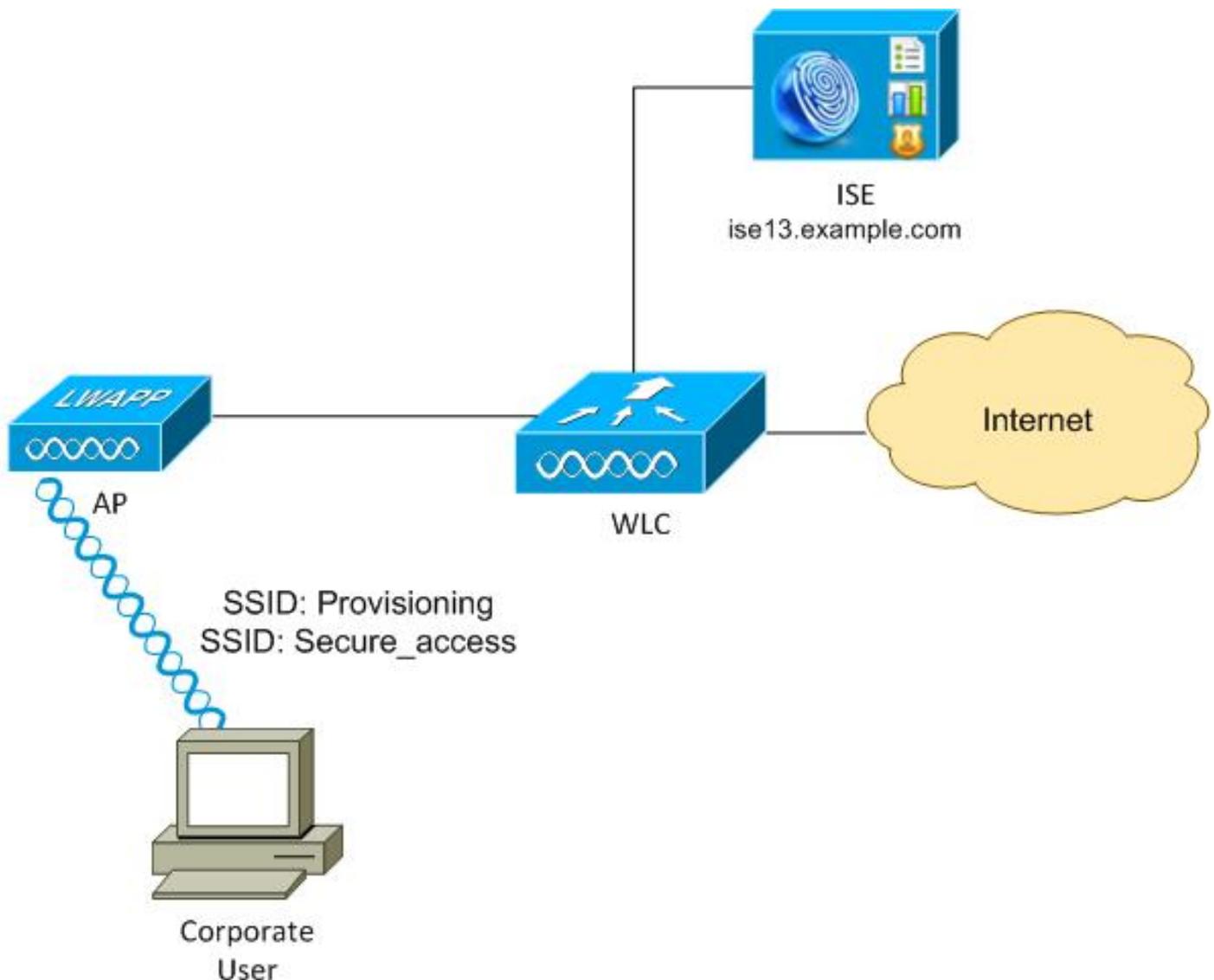
Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- Cisco WLC versione 7.6 e successive
- Software Cisco ISE, versione 1.3 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia e flusso



Ecco il flusso:

Passaggio 1. L'utente aziendale accede a SSID (Service Set Identifier): Provisioning. Esegue l'autenticazione 802.1x con EAP-PEAP (Extensible Authentication Protocol-Protected EAP). La regola di autorizzazione **Provisioning** viene rilevata su ISE e l'utente viene reindirizzato per il provisioning AnyConnect (tramite il portale di provisioning client). Se AnyConnect non viene

rilevato sul computer, vengono installati tutti i moduli configurati (VPN, NAM, Posture). Insieme al profilo, viene eseguito il push della configurazione per ogni modulo.

Passaggio 2. Dopo aver installato AnyConnect, l'utente deve riavviare il PC. Dopo il riavvio, AnyConnect viene eseguito e viene utilizzato automaticamente il SSID corretto, in base al profilo NAM configurato (Secure_access). Viene utilizzato EAP-PEAP (ad esempio, potrebbe essere utilizzato anche EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)). Allo stesso tempo, il modulo Postura verifica se la stazione è conforme (verifica l'esistenza del file c:\test.txt).

Passaggio 3. Se lo stato della postura della stazione è sconosciuto (nessun report dal modulo Postura), viene comunque reindirizzato per il provisioning, in quanto su ISE viene rilevata la regola **Unknown** Authz. Una volta che la stazione è conforme, ISE invia un Change of Authorization (CoA) al Wireless LAN Controller, che attiva la riautenticazione. Si verifica una seconda autenticazione e la regola **Compliant** viene attivata su ISE, che fornisce all'utente l'accesso completo alla rete.

Di conseguenza, all'utente sono stati forniti moduli AnyConnect VPN, NAM e Posture che consentono l'accesso unificato alla rete. Una funzionalità simile può essere utilizzata sull'appliance ASA (Adaptive Security Appliance) per l'accesso VPN. Attualmente, ISE può offrire lo stesso servizio per qualsiasi tipo di accesso, con un approccio molto granulare.

Questa funzionalità non è limitata agli utenti aziendali, ma è probabilmente la più comune da implementare per quel gruppo di utenti.

Configurazione

WLC

Il WLC è configurato con due SSID:

- Provisioning - [WPA + WPA2][Auth(802.1X)]. Questo SSID viene usato per il provisioning di AnyConnect.
- Secure_access - [WPA + WPA2][Auth(802.1X)]. Questo SSID viene utilizzato per l'accesso sicuro dopo il provisioning dell'endpoint con il modulo NAM configurato per tale SSID.

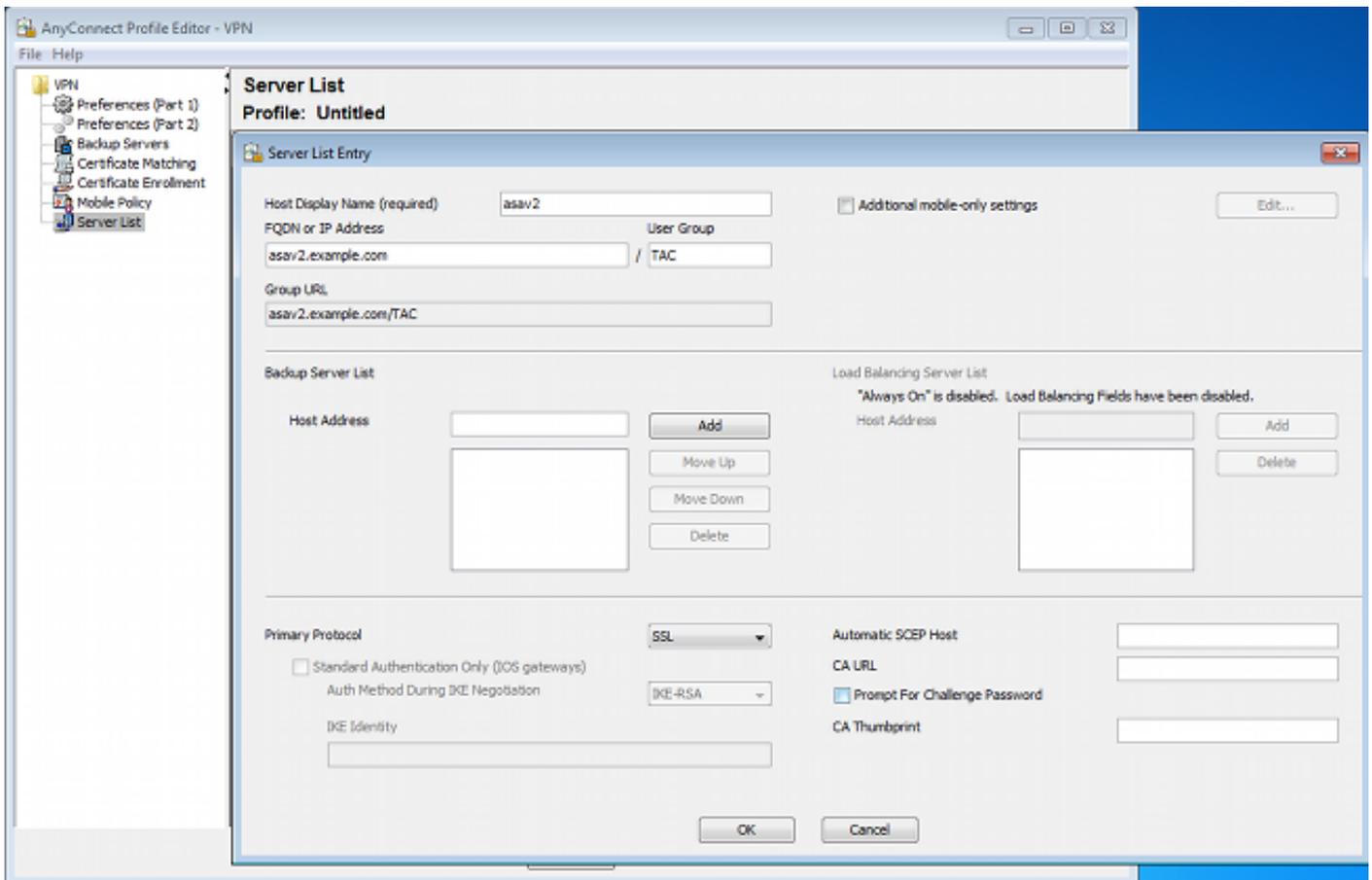
ISE

Passaggio 1. Aggiungere il WLC

Aggiungere il WLC ai dispositivi di rete su ISE.

Passaggio 2. Configurare il profilo VPN

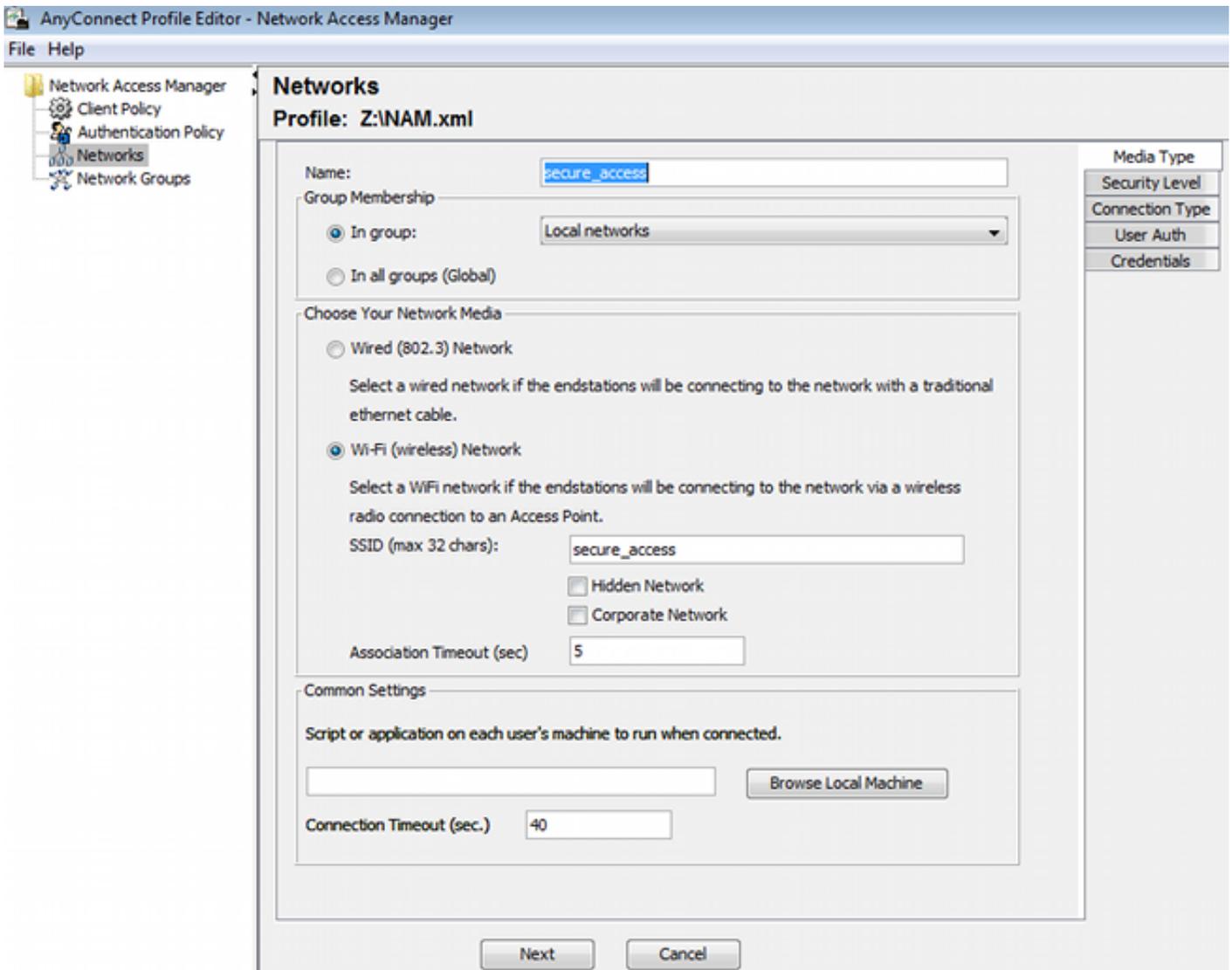
Configurare il profilo VPN con AnyConnect Profile Editor per VPN.



È stata aggiunta una sola voce per l'accesso VPN. Salvare il file XML in **VPN.xml**.

Passaggio 3. Configurare il profilo NAM

Configurare il profilo NAM con AnyConnect Profile Editor per NAM.



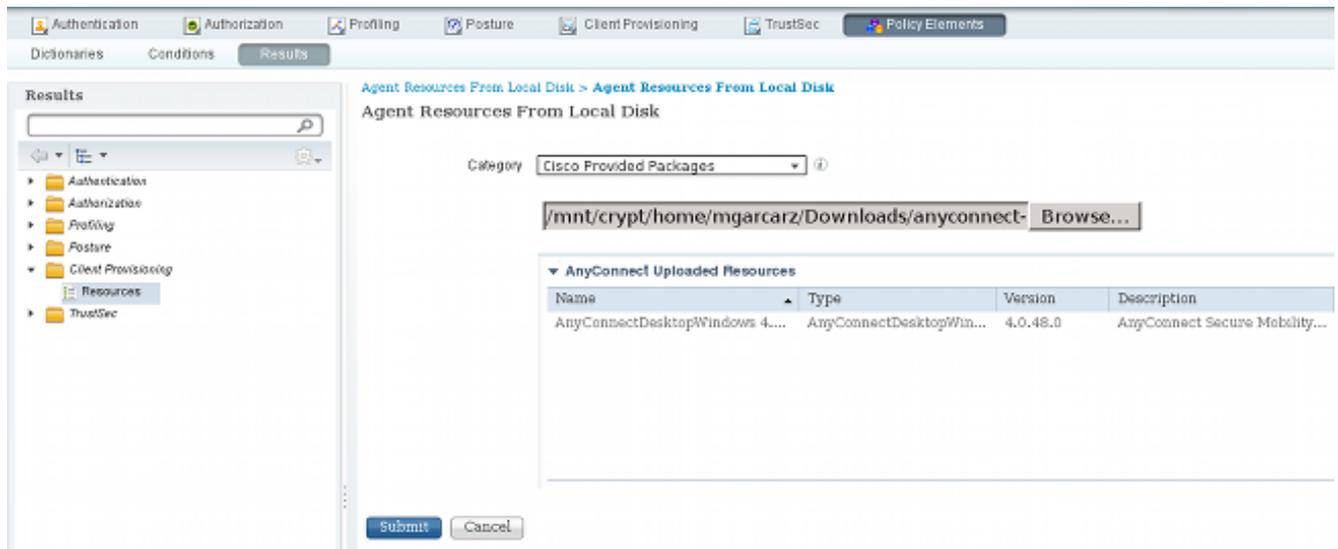
È stato configurato un solo SSID: **secure_access**. Salvare il file XML in **NAM.xml**.

Passaggio 4. Installare l'applicazione

1. Scaricare l'applicazione manualmente da Cisco.com.

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

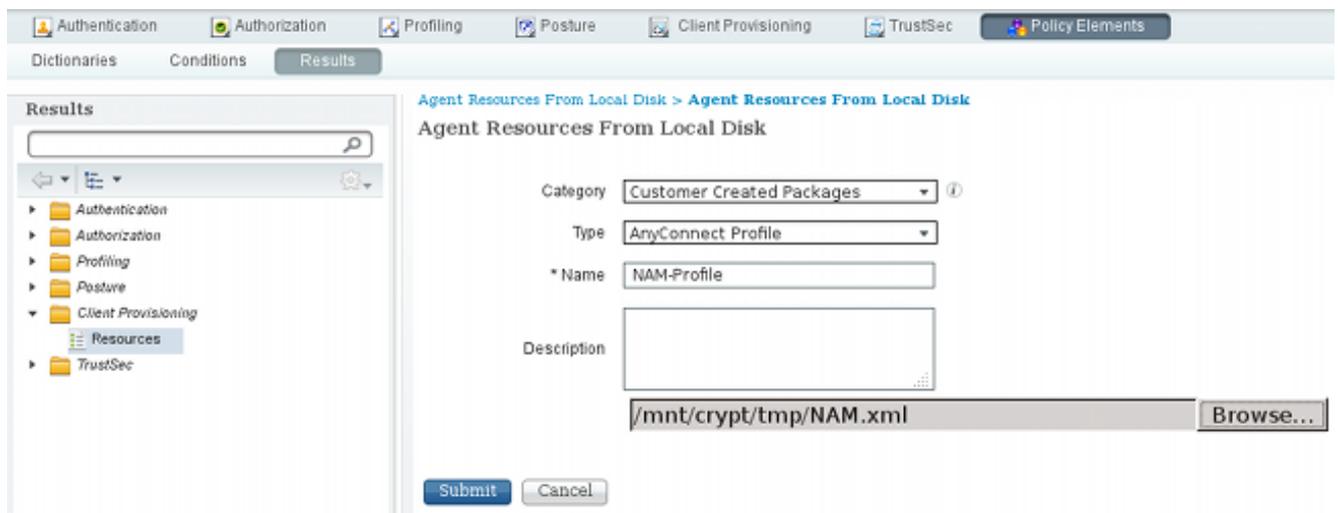
2. Su ISE, selezionare **Policy > Results > Client Provisioning > Resources** (Policy > Risultati > Provisioning client > Risorse), quindi aggiungere le risorse dell'agente dal disco locale.
3. Scegliere i pacchetti Cisco forniti e selezionare il file **anyconnect-win-4.0.00048-k9.pkg**:



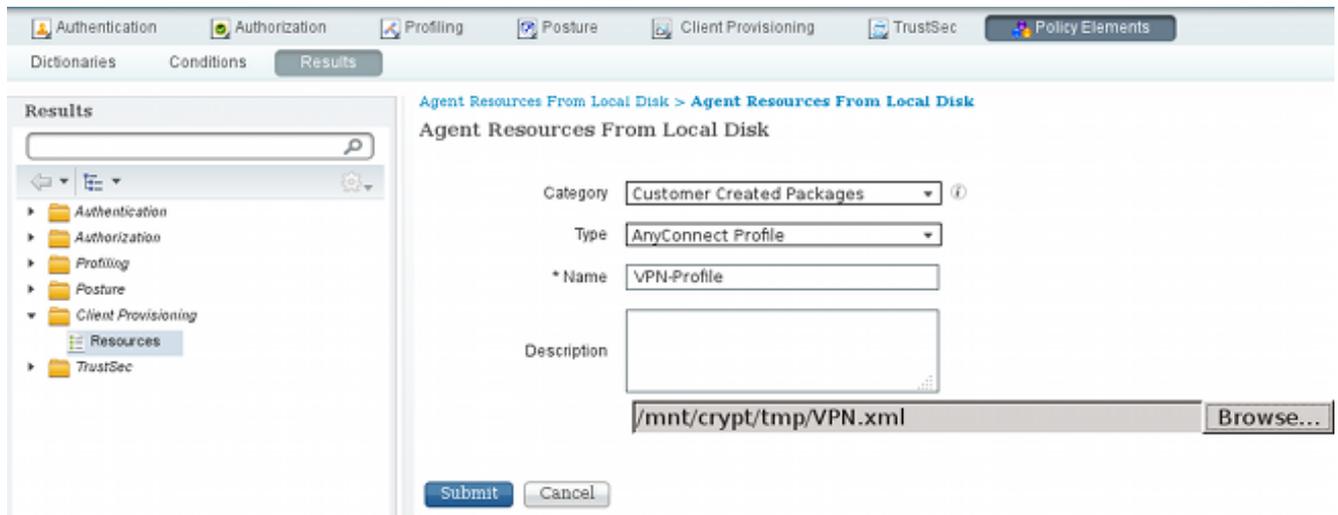
4. Ripetere il passaggio 4 per il modulo sulla conformità.

Passaggio 5. Installare il profilo VPN/NAM

1. Passare a **Policy > Results > Client Provisioning > Resources**, quindi aggiungere le risorse agente dal disco locale.
2. Selezionare Pacchetti creati dal cliente e digitare **AnyConnect Profile**. Selezionare il profilo NAM creato in precedenza (file XML):



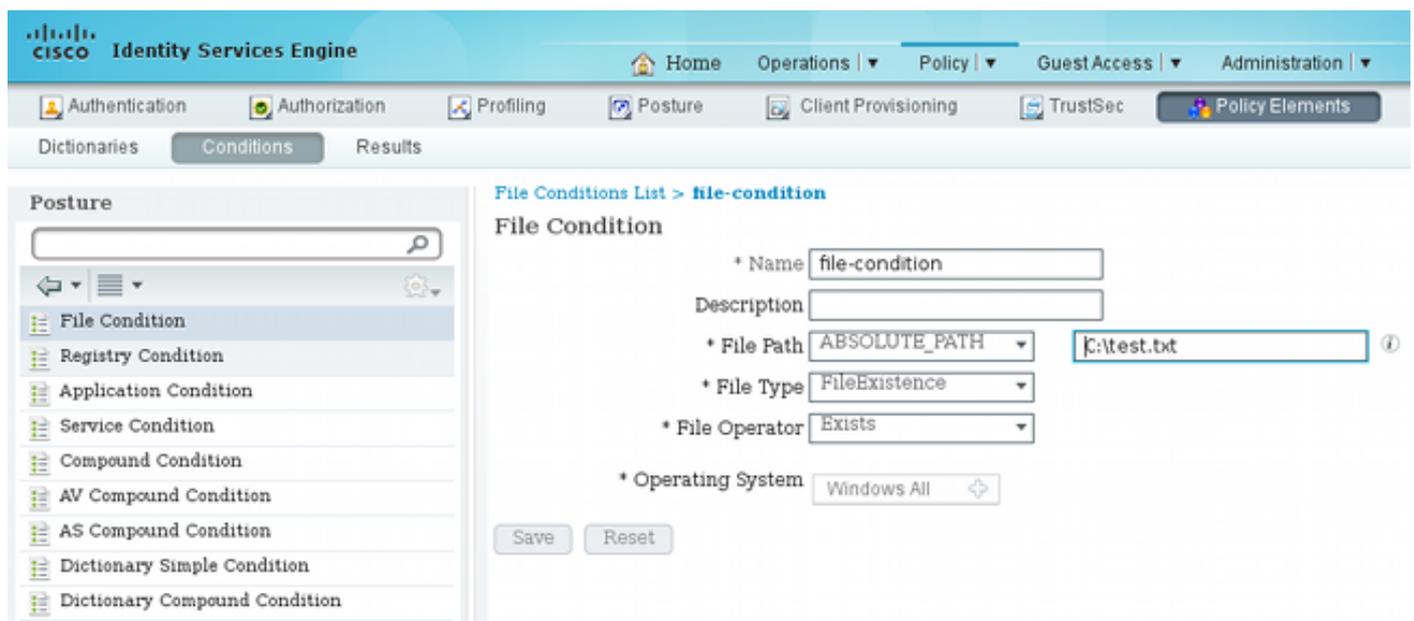
3. Ripetere una procedura simile per il profilo VPN:



Passaggio 6. Configurazione della postura

I profili NAM e VPN devono essere configurati esternamente con l'editor dei profili AnyConnect e importati nell'ISE. Ma la postura è completamente configurata ad ISE.

Passare a **Criteri > Condizioni > Postura > Condizione file**. È possibile notare che è stata creata una semplice condizione per l'esistenza del file. Per essere conforme alla policy verificata dal modulo Postura, è necessario disporre di tale file:



Questa condizione viene utilizzata per un requisito:

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

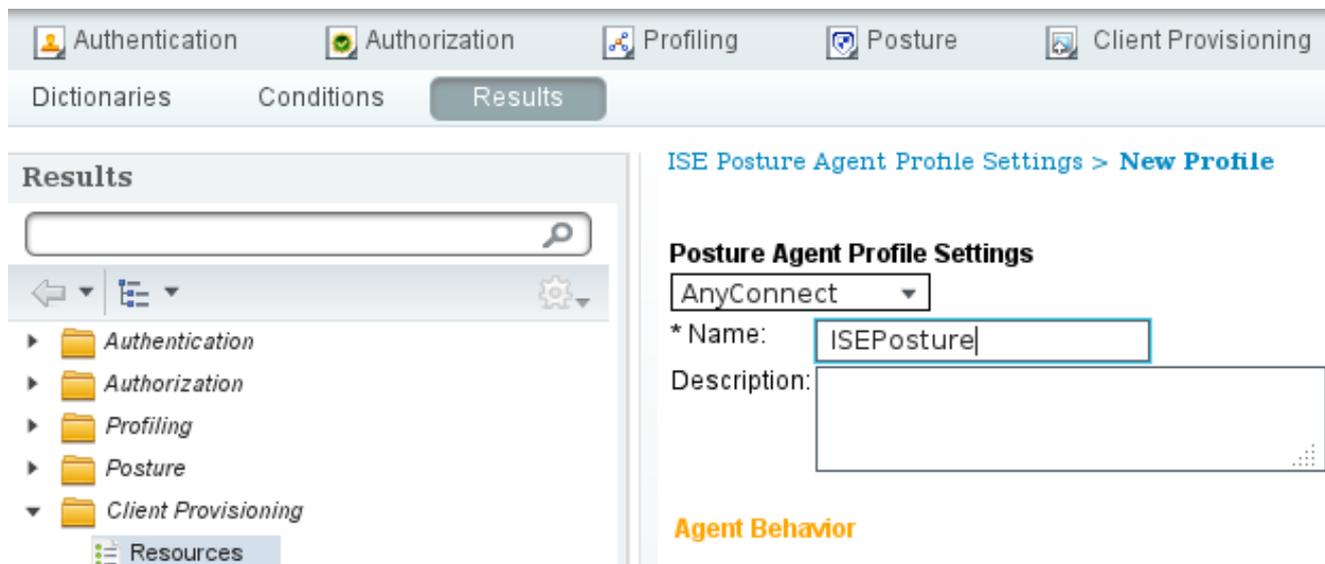
Il requisito è utilizzato nei criteri di postura per i sistemi Microsoft Windows:

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

Per ulteriori informazioni sulla configurazione della postura, consultare il documento [Posture Services nella Guida alla configurazione di Cisco ISE](#).

Quando il criterio di postura è pronto, è necessario aggiungere la configurazione dell'agente di postura.

1. Selezionare **Policy > Results > Client Provisioning > Resources** e aggiungere Network Admission Control (NAC) Agent o AnyConnect Agent Posture Profile.
2. Selezionare AnyConnect (è stato utilizzato un nuovo modulo Posture di ISE versione 1.3 anziché il vecchio agente NAC):



3. Dalla sezione Posture Protocol, non dimenticare di aggiungere * per consentire all'agente di connettersi a tutti i server.

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

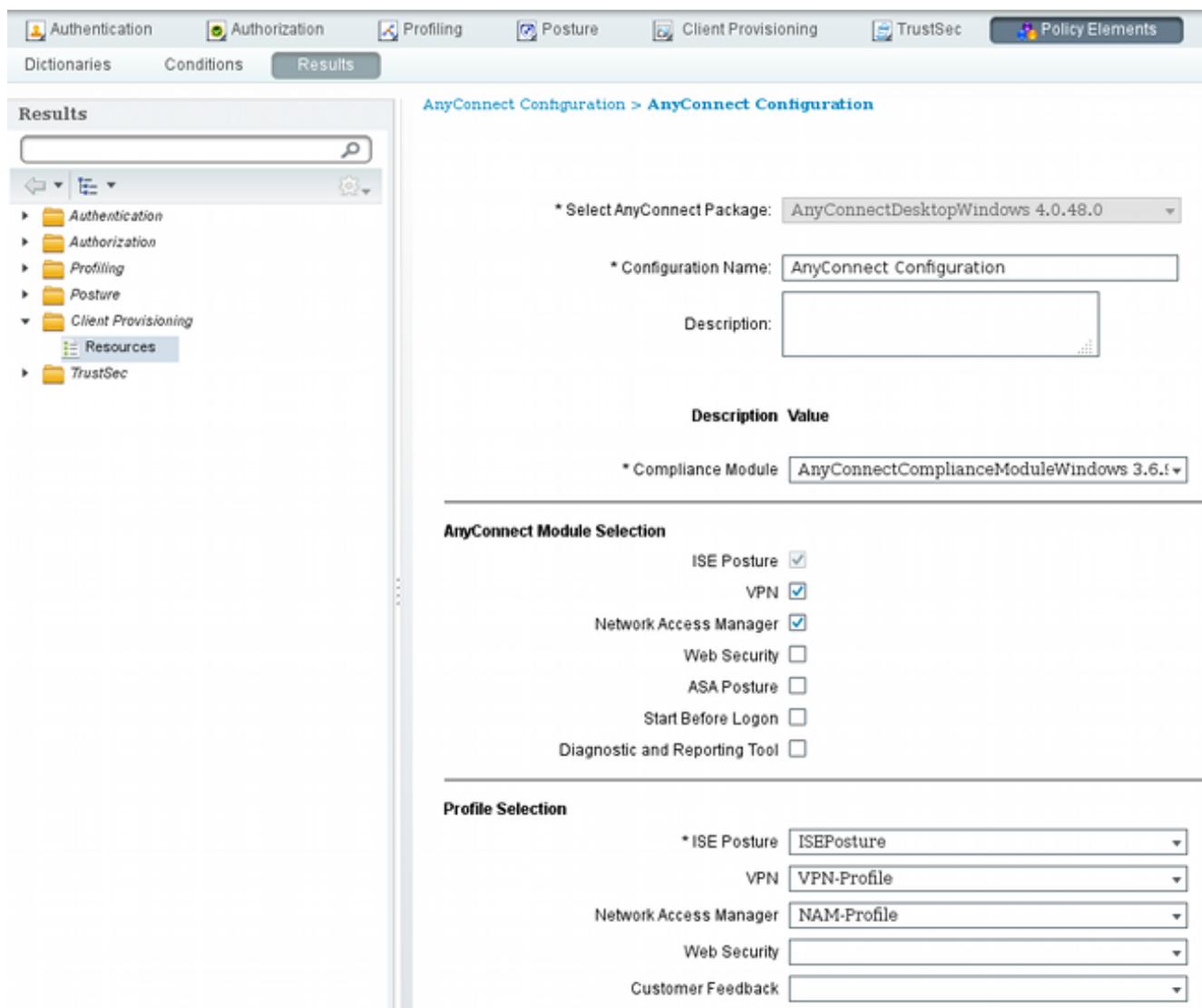
4. Se il campo Regole nome server viene lasciato vuoto, ISE non salva le impostazioni e segnala questo errore:

Server name rules: valid value is required

Passaggio 7. Configurazione di AnyConnect

In questa fase, sono state configurate tutte le applicazioni (AnyConnect) e la configurazione del profilo per tutti i moduli (VPN, NAM e Posture). È ora di unirle.

1. Selezionare **Policy > Results > Client Provisioning > Resources**, quindi aggiungere AnyConnect Configuration.
2. Configurare il nome e selezionare il modulo di conformità e tutti i moduli AnyConnect richiesti (VPN, NAM e Posture).
3. In Selezione profilo, scegliere il profilo configurato in precedenza per ciascun modulo.



4. Il modulo VPN è obbligatorio per il corretto funzionamento di tutti gli altri moduli. Anche se il modulo VPN non è selezionato per l'installazione, verrà premuto e installato sul client. Se non si desidera utilizzare la VPN, è possibile configurare un profilo speciale per la VPN che nasconda l'interfaccia utente del modulo VPN. Le righe seguenti devono essere aggiunte al file **VPN.xml**:

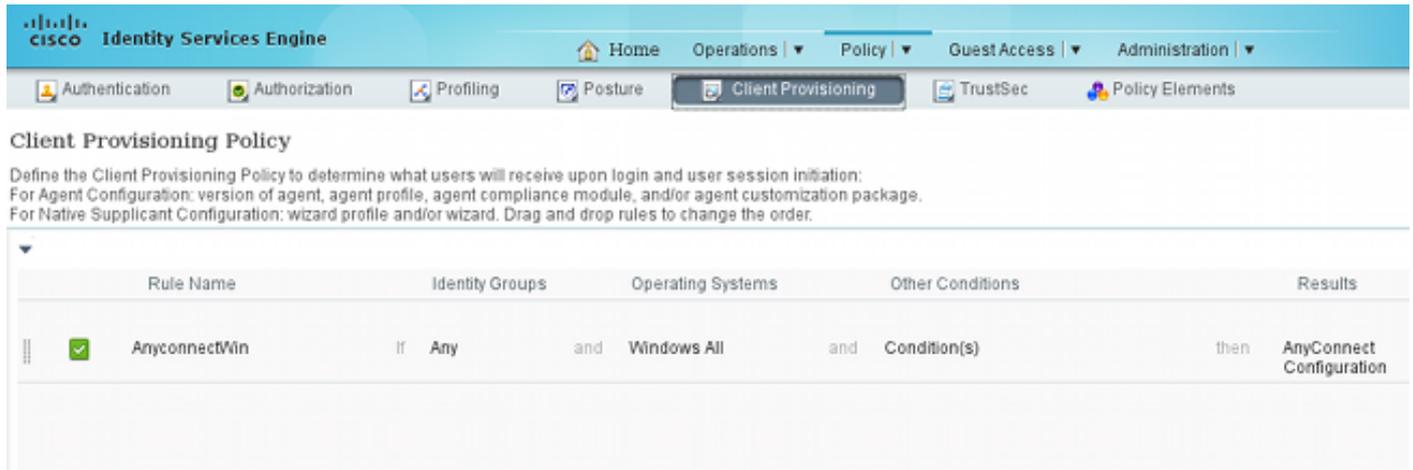
```
<ClientInitialization>
```

```
</ClientInitialization>
```

5. Questo tipo di profilo viene installato anche quando si utilizza **Setup.exe** dal pacchetto iso (**anyconnect-win-3.1.06073-pre-deploy-k9.iso**). Quindi, il profilo **VPNDisable_ServiceProfile.xml** per VPN viene installato insieme alla configurazione, che disabilita l'interfaccia utente per il modulo VPN.

Passaggio 8. Regole di provisioning client

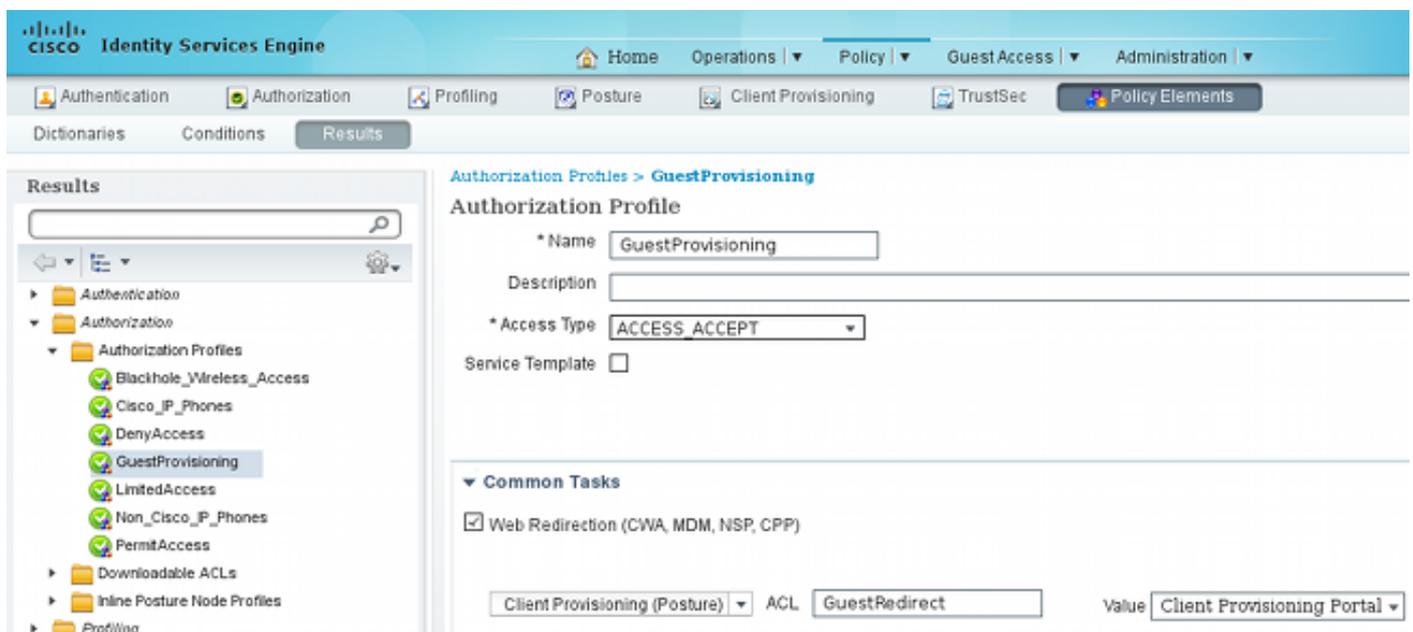
Nelle regole di provisioning client, fare riferimento alla configurazione AnyConnect creata nel passaggio 7:



Le regole di provisioning client determinano quale applicazione verrà sottoposta a push nel client. È necessaria una sola regola per puntare alla configurazione creata nel passaggio 7. In questo modo, tutti gli endpoint di Microsoft Windows reindirizzati per il provisioning client utilizzeranno la configurazione AnyConnect con tutti i moduli e i profili.

Passaggio 9. Profili di autorizzazione

È necessario creare il profilo di autorizzazione per il provisioning client. Viene utilizzato il portale di provisioning client predefinito:



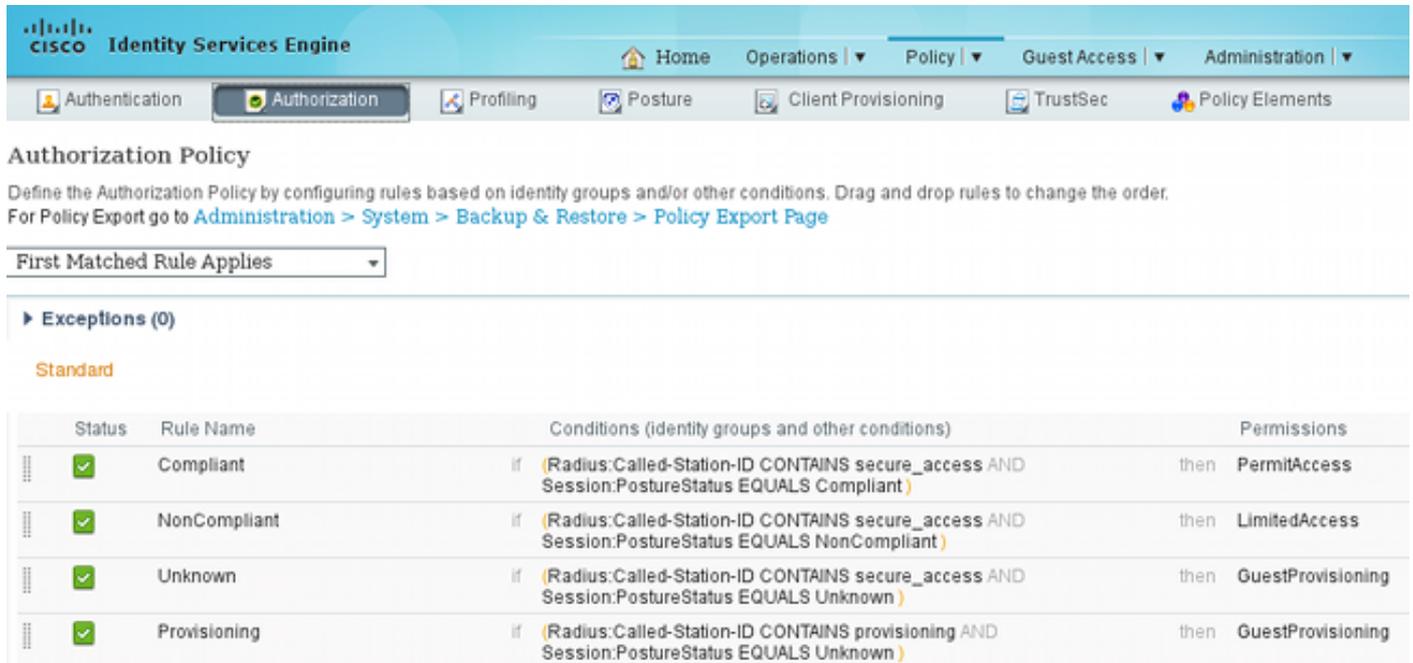
Questo profilo impone il reindirizzamento degli utenti per il provisioning al portale di provisioning client predefinito. Questo portale valuta i criteri di provisioning client (regole create nel passaggio 8). I profili di autorizzazione sono i risultati delle regole di autorizzazione configurate nel passo 10.

Access Control List (ACL) GuestRedirect è il nome dell'ACL definito sul WLC. Questo ACL decide quale traffico deve essere reindirizzato ad ISE. Per ulteriori informazioni, fare riferimento all'[esempio di autenticazione Web centrale con uno switch e configurazione di Identity Services Engine](#).

Esiste inoltre un altro profilo di autorizzazione che fornisce l'accesso limitato alla rete (DACL, Limited Network Access) per gli utenti non conformi (denominato Accesso limitato).

Passaggio 10. Regole di autorizzazione

Tutte queste regole sono combinate in quattro regole di autorizzazione:



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)

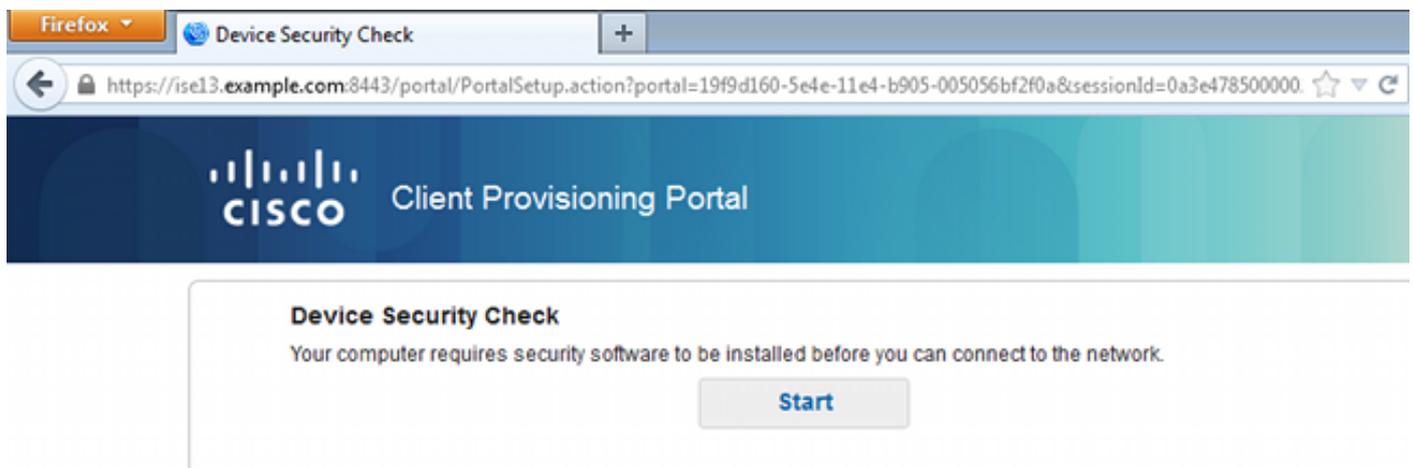
Standard

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

Per prima cosa ci si connette al SSID di provisioning e si viene reindirizzati per il provisioning a un portale di provisioning client predefinito (regola denominata Provisioning). Una volta effettuata la connessione al SSID **Secure_access**, il reindirizzamento per il provisioning viene eseguito se non viene ricevuto alcun report dal modulo Posture da ISE (regola denominata Unknown). Una volta che l'endpoint è completamente conforme, viene concesso l'accesso completo (nome regola Conforme). Se l'endpoint viene segnalato come non conforme, dispone di un accesso di rete limitato (regola denominata NonConforme).

Verifica

L'utente viene associato al SSID di provisioning, tenta di accedere a qualsiasi pagina Web e viene reindirizzato al portale di provisioning client:



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

Poiché AnyConnect non viene rilevato, viene chiesto di installarlo:

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

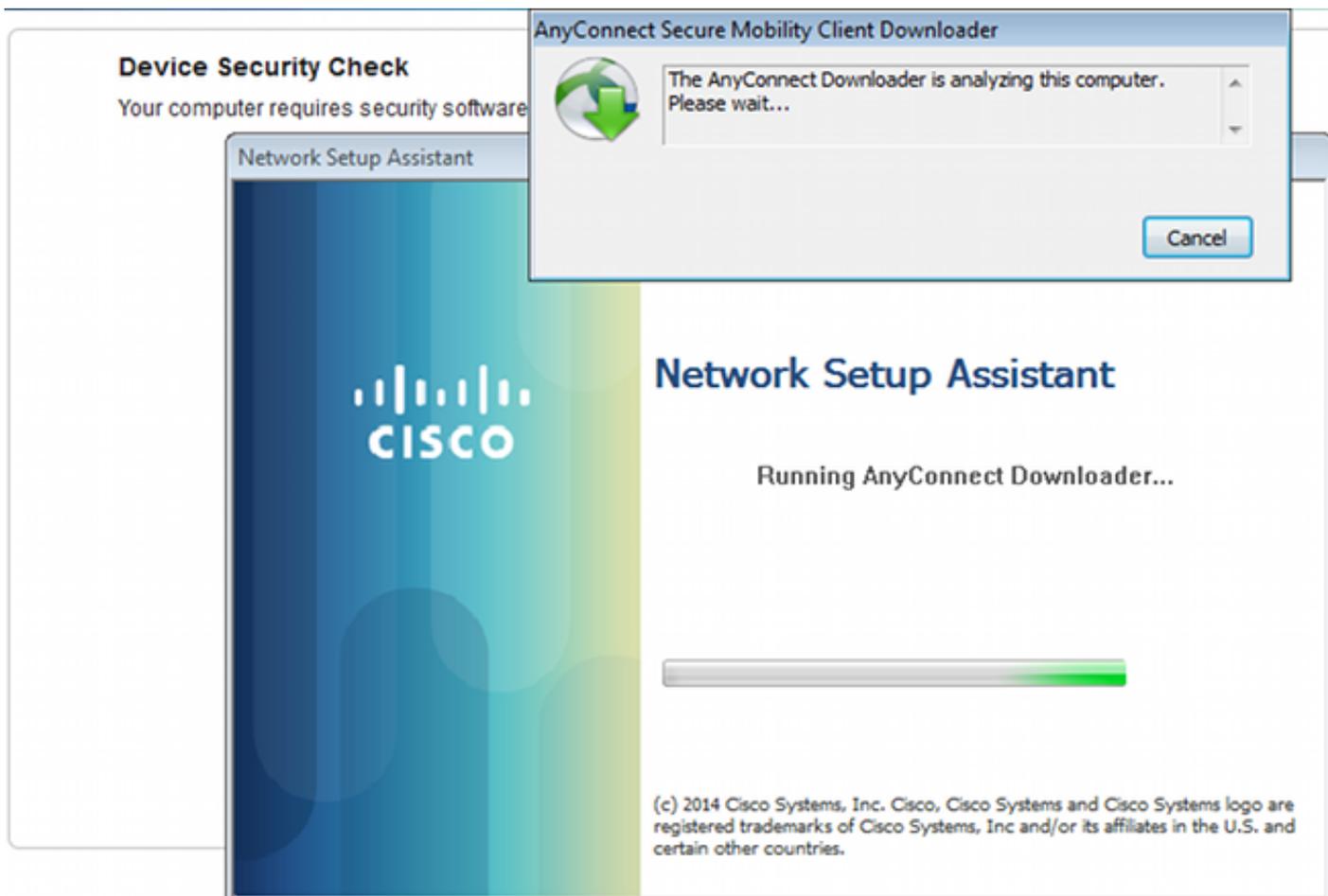
1. You must install AnyConnect to check your device before accessing the network. [Click here to download and install AnyConnect](#)
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan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

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

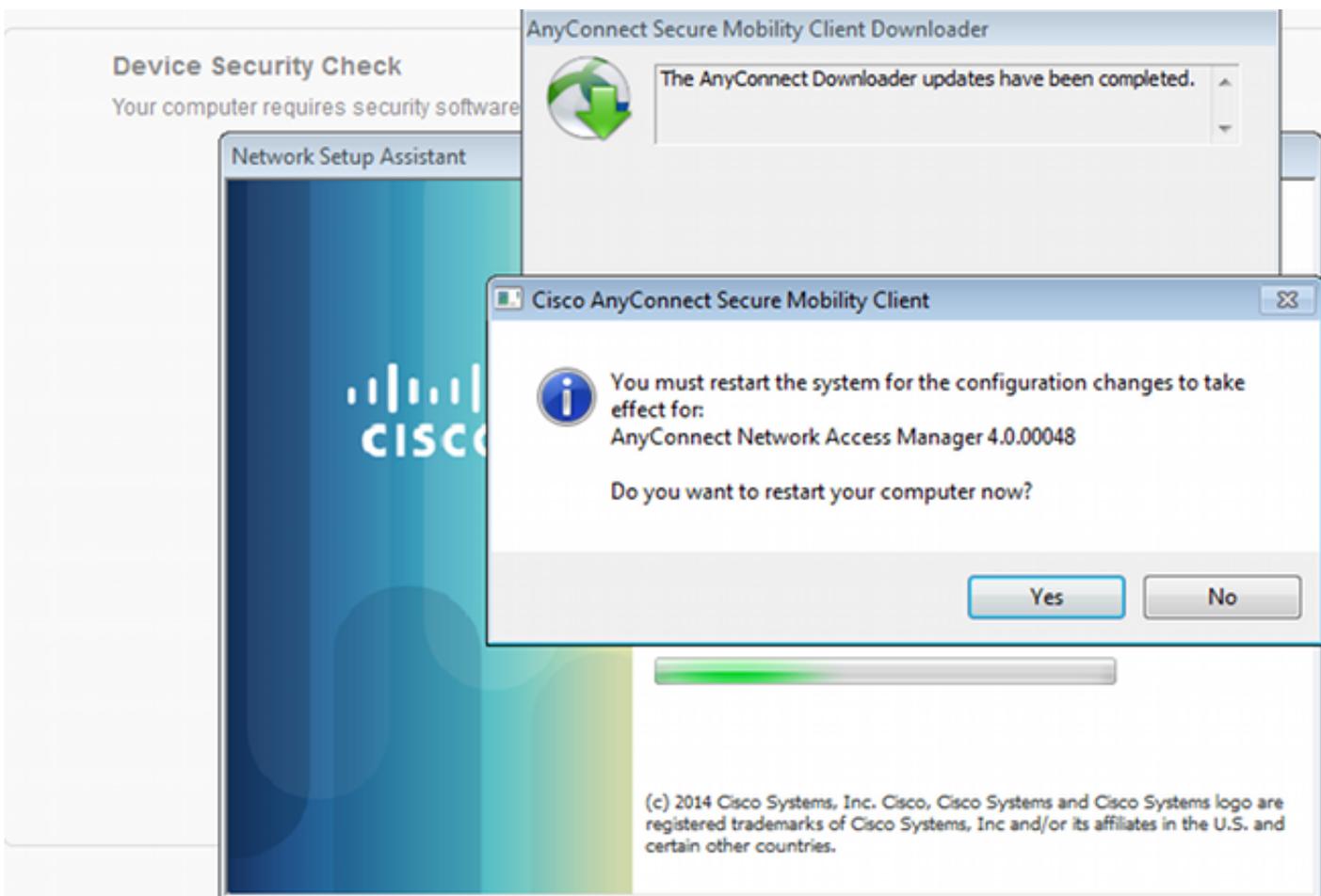
 You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

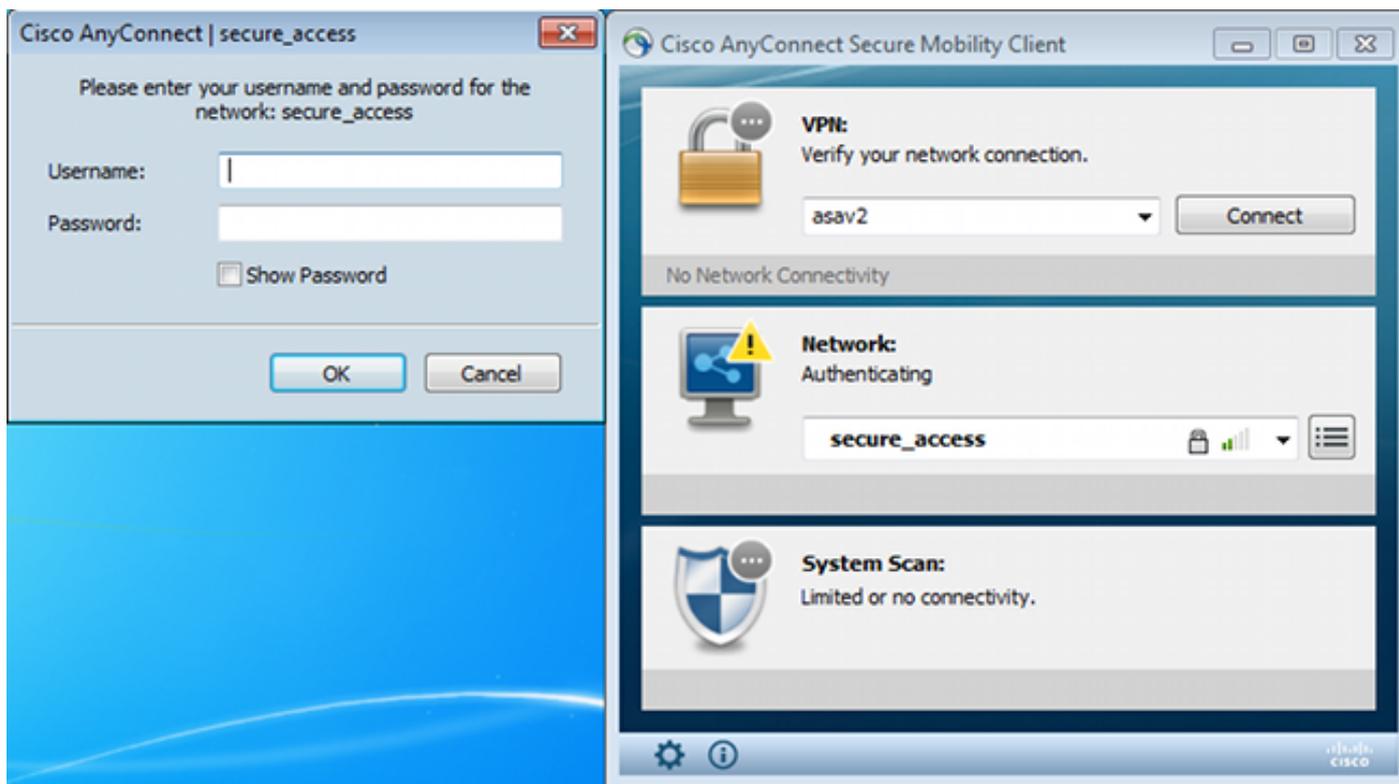
Viene scaricata una piccola applicazione denominata Assistente installazione di rete, responsabile dell'intero processo di installazione. Si noti che è diverso da Network Setup Assistant nella versione 1.2.



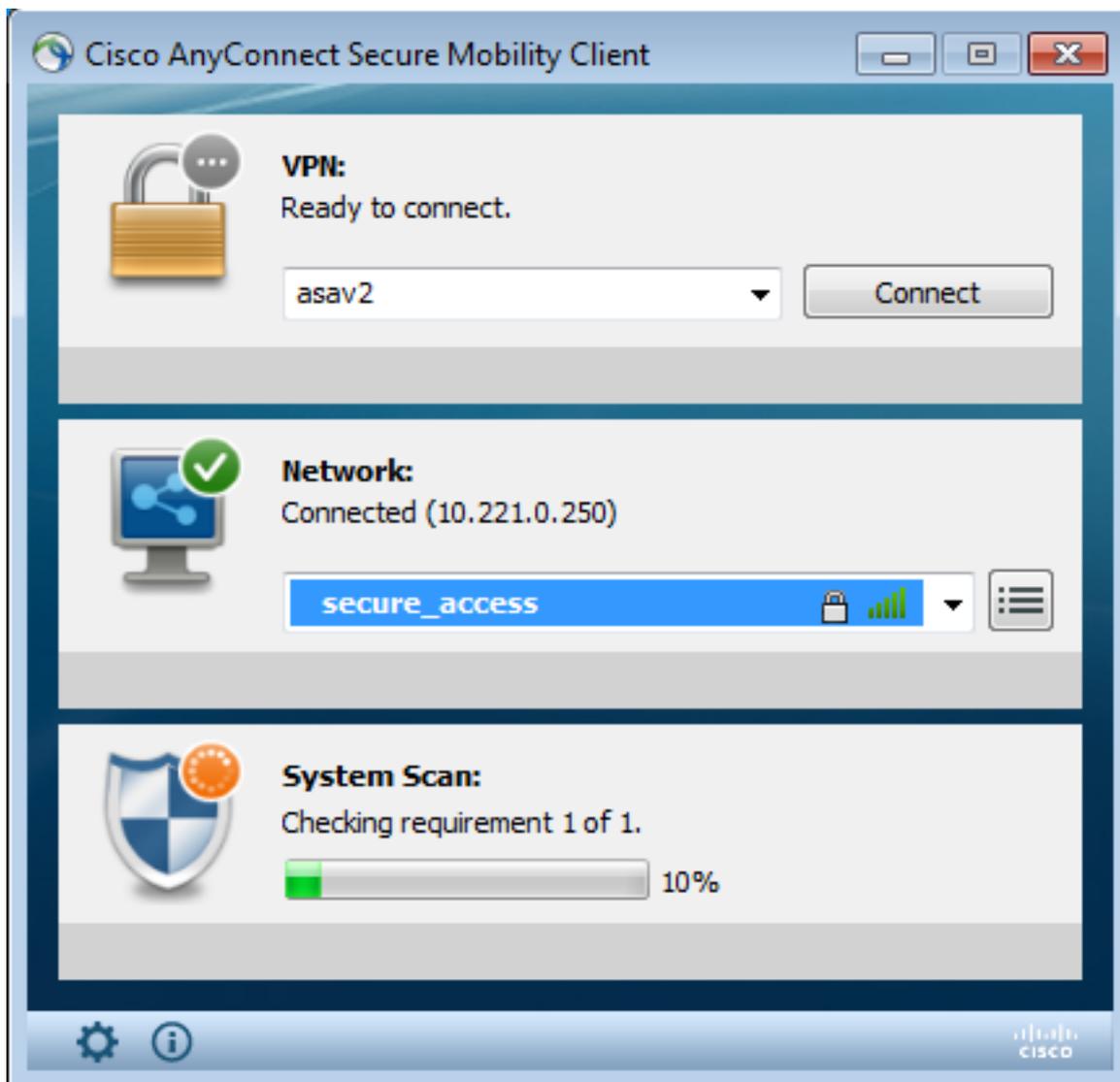
Tutti i moduli (VPN, NAM e Posture) sono installati e configurati. È necessario riavviare il PC:



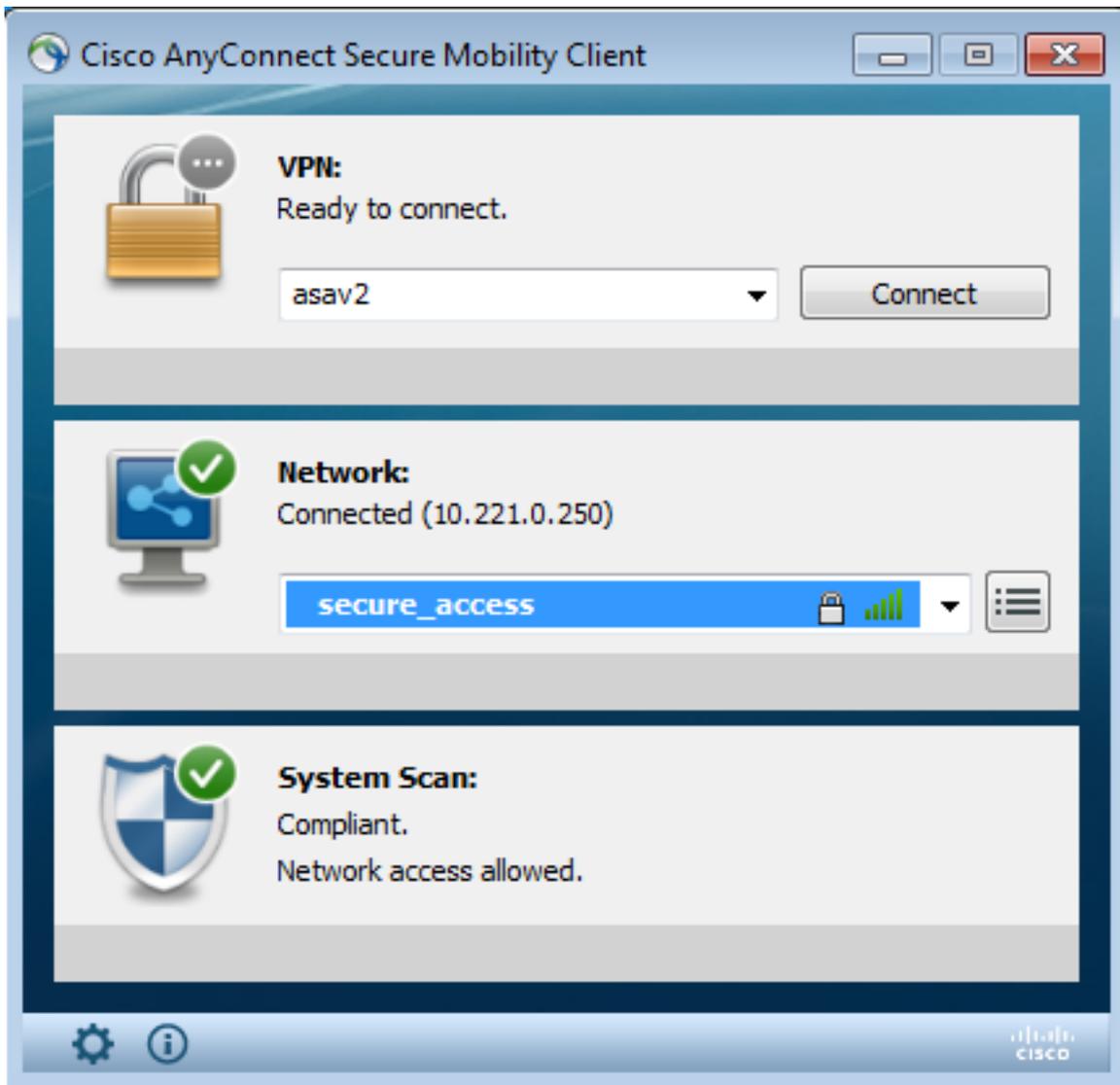
Dopo il riavvio, AnyConnect viene eseguito automaticamente e NAM tenta di associarsi a SSID secure_access (in base al profilo configurato). Il profilo VPN è installato correttamente (voce asav2 per VPN):



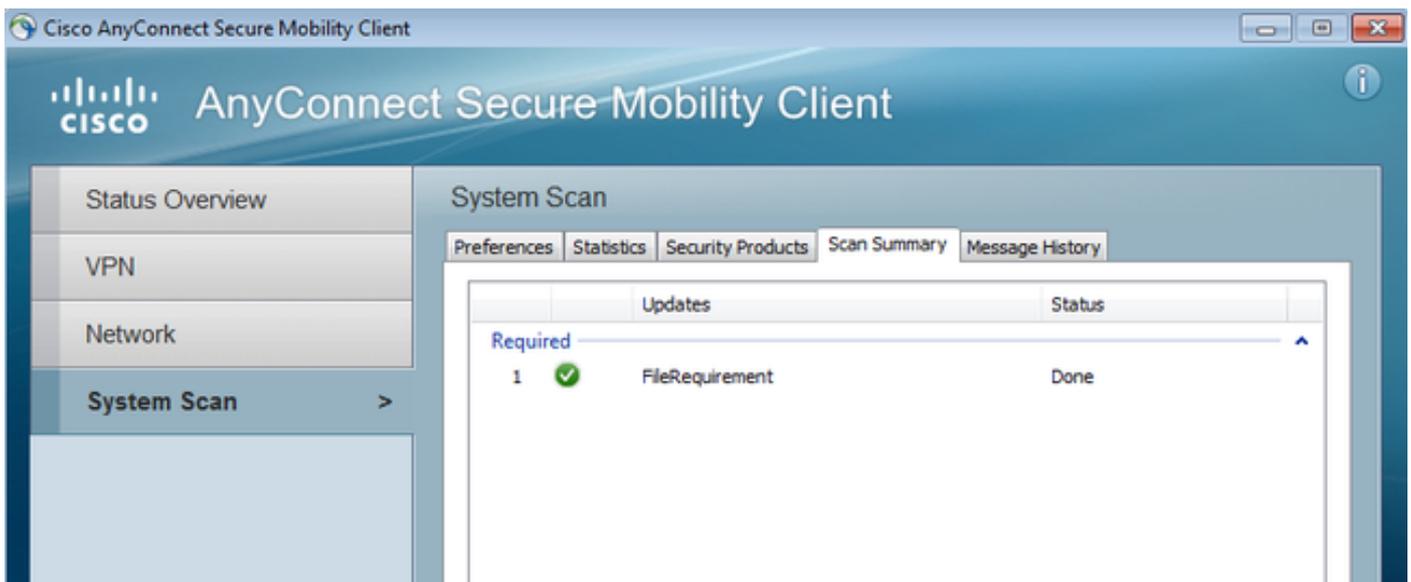
Dopo l'autenticazione, AnyConnect scarica gli aggiornamenti e le regole di postura per cui viene eseguita la verifica:



In questa fase, l'accesso potrebbe essere ancora limitato (ad ISE si applica la regola di autorizzazione sconosciuta). Una volta che la stazione è conforme, ciò viene segnalato dal modulo Postura:



È inoltre possibile verificare i dettagli (FileRequirement è soddisfatto):



In Cronologia messaggi vengono illustrati i passaggi dettagliati:

```
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.

```

Il report viene inviato all'ISE, che a sua volta attiva il cambio di autorizzazione. La seconda autenticazione rileva la regola Conforme e viene concesso l'accesso completo alla rete. Se il report sulla postura viene inviato mentre è ancora associato al SSID di provisioning, questi log vengono visualizzati su ISE:

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

Il rapporto Postura indica:

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2014-11-16 09:23:25.8	Success		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	Success		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	Success		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	Success		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

I report dettagliati mostrano il requisito del file soddisfatto:

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		

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- [Guida alla configurazione dei servizi di postura di Cisco ISE](#)
- [Guida per l'amministratore di Cisco ISE 1.3](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)