

Konfigurationsbeispiel für die Integration von AnyConnect 4.0 in ISE Version 1.3

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Topologie und Fluss](#)

[Konfigurieren](#)

[WLC](#)

[ISE](#)

[Schritt 1: WLC hinzufügen](#)

[Schritt 2: Konfigurieren des VPN-Profiles](#)

[Schritt 3: Konfigurieren des NAM-Profiles](#)

[Schritt 4: Installieren der Anwendung](#)

[Schritt 5: Installieren des VPN/NAM-Profiles](#)

[Schritt 6: Konfigurieren der Statusüberprüfung](#)

[Schritt 7: Konfigurieren von AnyConnect](#)

[Schritt 8: Client-Bereitstellungsregeln](#)

[Schritt 9: Autorisierungsprofile](#)

[Schritt 10: Autorisierungsregeln](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die neuen Funktionen der Cisco Identity Services Engine (ISE) Version 1.3 beschrieben, mit denen Sie mehrere AnyConnect Secure Mobility Client-Module konfigurieren und diese automatisch für das Endgerät bereitstellen können. In diesem Dokument wird die Konfiguration von VPN-, Network Access Manager- (NAM) und Statusmodulen auf der ISE erläutert und an den Benutzer des Unternehmens weitergeleitet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ISE-Bereitstellungen, -Authentifizierung und -Autorisierung
- Konfiguration der Wireless LAN Controller (WLCs)
- Grundlegendes VPN und 802.1x-Wissen

- Konfiguration von VPN- und NAM-Profilen mit AnyConnect-Profil-Editoren

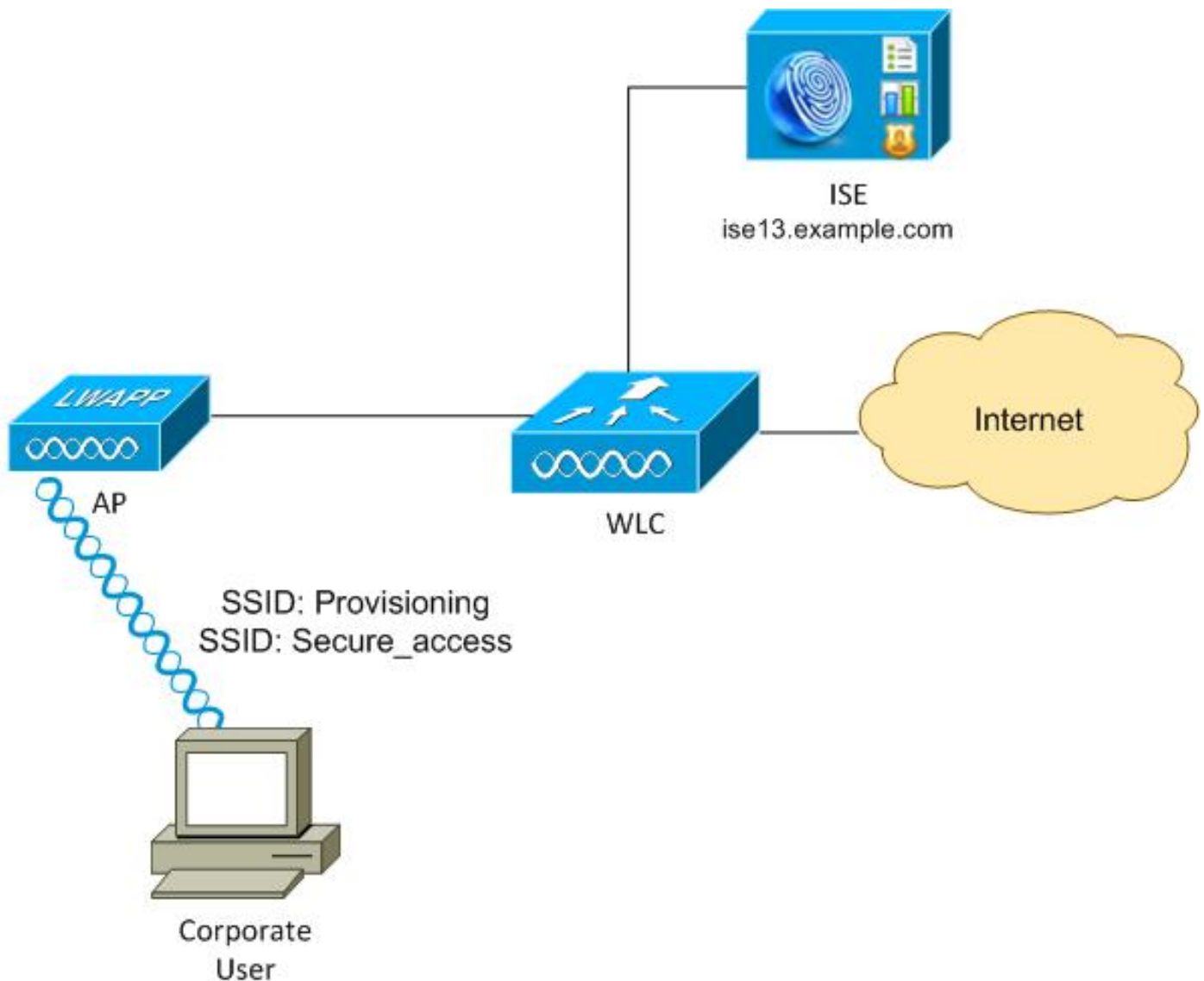
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco WLC 7.6 oder höher
- Cisco ISE Software, Versionen 1.3 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Topologie und Fluss



Hier ist der Ablauf:

Schritt 1: Firmenbenutzer greifen auf Service Set Identifier (SSID) zu: Bereitstellung. 802.1x-

Authentifizierung mit Extensible Authentication Protocol-Protected EAP (EAP-PEAP). Die **Provisioning** Authorization-Regel findet auf der ISE statt, und der Benutzer wird für AnyConnect Provisioning (über das Client Provisioning Portal) umgeleitet. Wenn AnyConnect auf dem Computer nicht erkannt wird, werden alle konfigurierten Module installiert (VPN, NAM, Posture). Zusammen mit diesem Profil wird die Konfiguration für jedes Modul angefordert.

Schritt 2: Nach der Installation von AnyConnect muss der Benutzer den PC neu starten. Nach dem Neustart wird AnyConnect ausgeführt, und die richtige SSID wird gemäß dem konfigurierten NAM-Profil (Secure_Access) automatisch verwendet. EAP-PEAP wird verwendet (z. B. kann auch Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) verwendet werden). Gleichzeitig überprüft das Posture-Modul, ob die Station den Vorgaben entspricht (überprüft, ob eine **c:\test.txt-Datei** vorhanden ist).

Schritt 3: Wenn der Status der Workstation unbekannt ist (kein Bericht vom Statusmodul), wird er dennoch zur Bereitstellung umgeleitet, da die Regel **Unknown** Authz (Unbekannte Autoren) auf der ISE angetroffen wird. Sobald die Station die Vorgaben erfüllt hat, sendet die ISE eine CoA (Change of Authorization) an den Wireless LAN Controller, was eine erneute Authentifizierung auslöst. Eine zweite Authentifizierung wird durchgeführt, und die **Compliance**-Regel wird auf die ISE angewendet, die dem Benutzer vollständigen Zugriff auf das Netzwerk ermöglicht.

Als Ergebnis wurden dem Benutzer AnyConnect-VPN-, NAM- und Statusmodule bereitgestellt, die einen einheitlichen Netzwerkzugriff ermöglichen. Ähnliche Funktionen können auf der Adaptive Security Appliance (ASA) für den VPN-Zugriff verwendet werden. Derzeit kann die ISE das Gleiche für alle Zugriffsarten mit einem sehr präzisen Ansatz tun.

Diese Funktion ist nicht auf Benutzer in Unternehmen beschränkt, sondern wird meist für diese Benutzergruppe bereitgestellt.

Konfigurieren

WLC

Der WLC ist mit zwei SSIDs konfiguriert:

- Bereitstellung - [WPA + WPA2][Auth(802.1X)]. Diese SSID wird für die AnyConnect-Bereitstellung verwendet.
- Secure_access - [WPA + WPA2][Auth(802.1X)] Diese SSID wird für den sicheren Zugriff verwendet, nachdem der Endpunkt mit dem für diese SSID konfigurierten NAM-Modul bereitgestellt wurde.

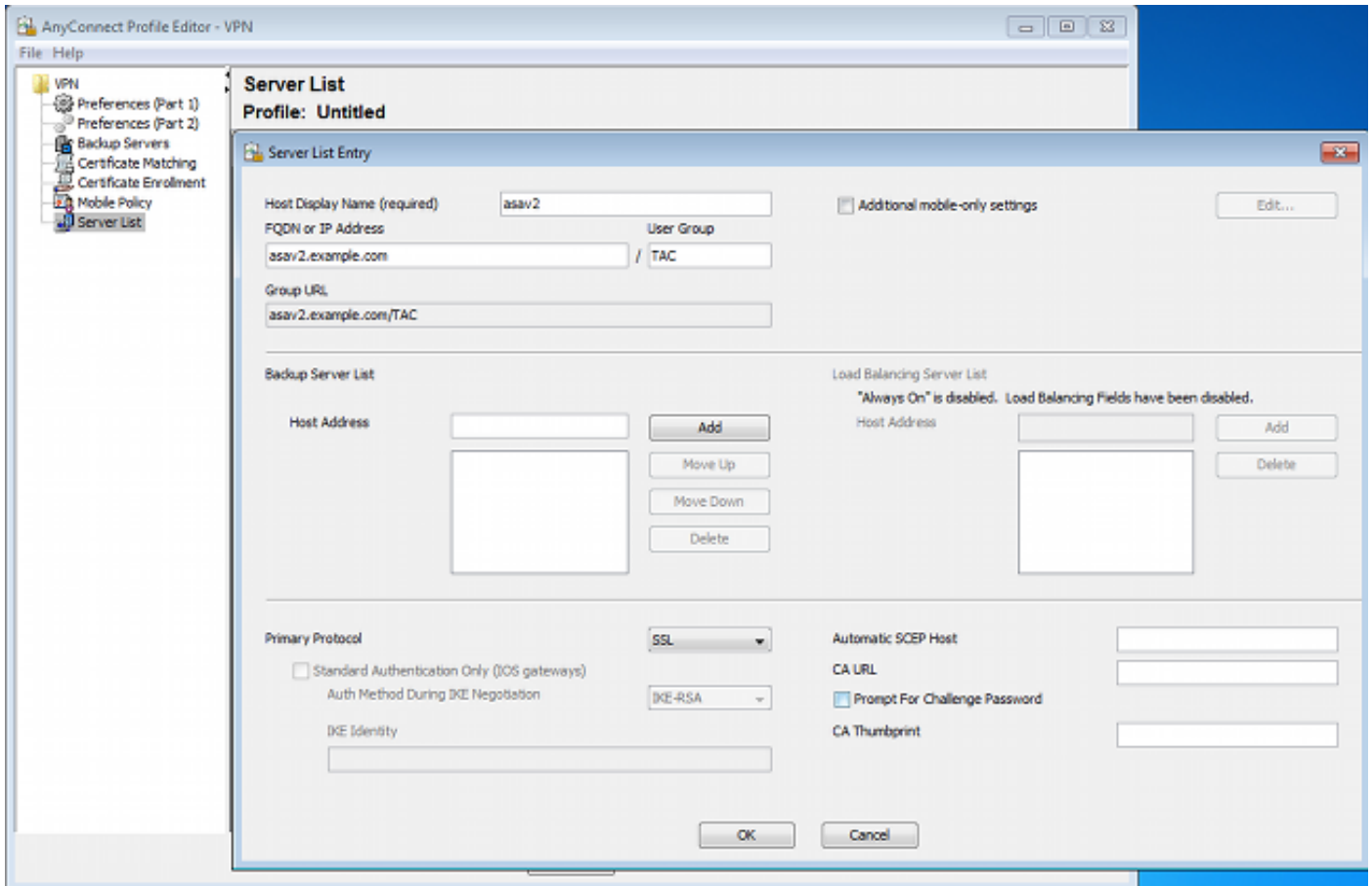
ISE

Schritt 1: WLC hinzufügen

Fügen Sie den WLC den Netzwerkgeräten auf der ISE hinzu.

Schritt 2: Konfigurieren des VPN-Profiles

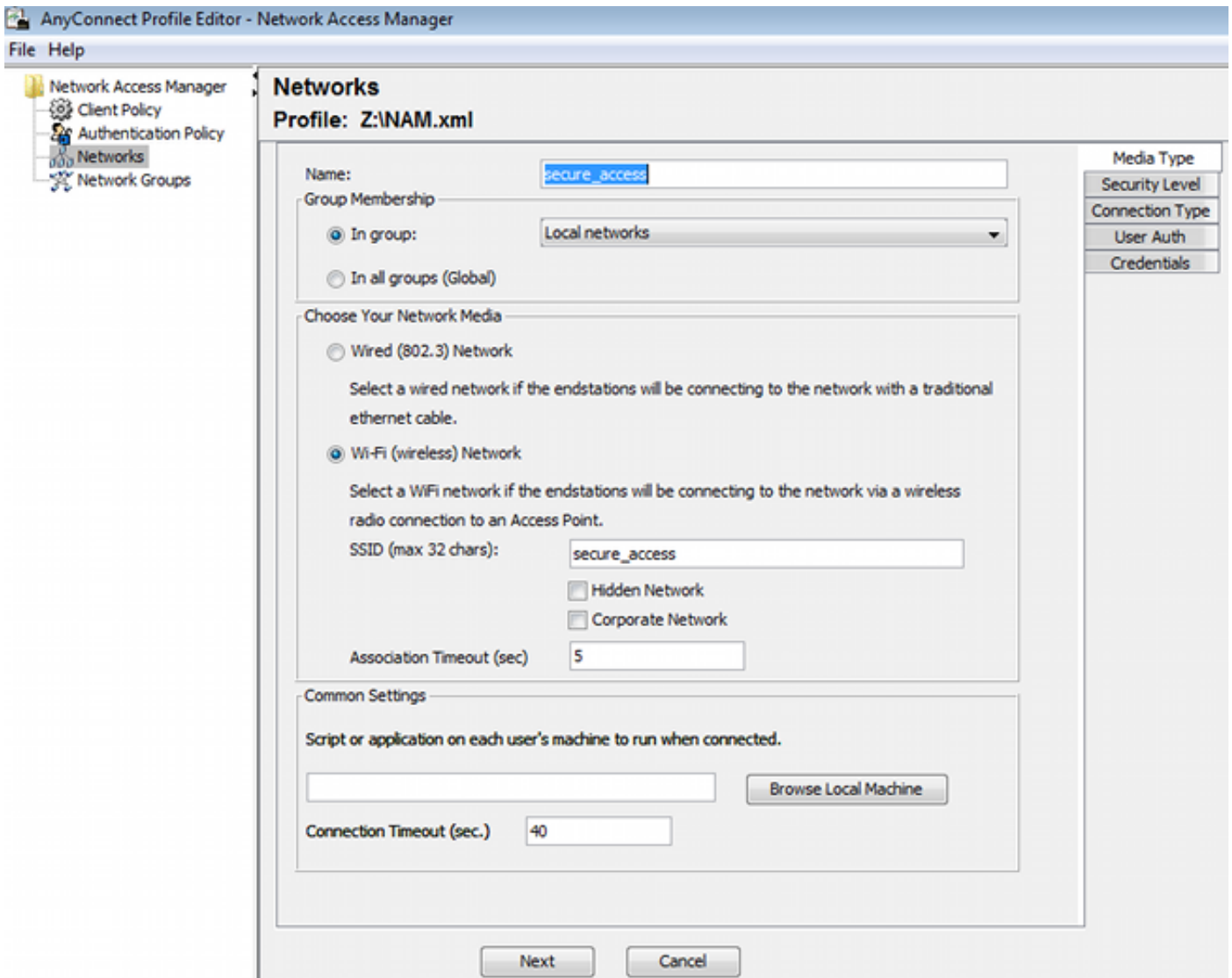
Konfigurieren Sie das VPN-Profil mit dem AnyConnect Profile Editor für VPN.



Für den VPN-Zugriff wurde nur ein Eintrag hinzugefügt. Speichern Sie die XML-Datei in **VPN.xml**.

Schritt 3: Konfigurieren des NAM-Profiles

Konfigurieren Sie das NAM-Profil mit dem AnyConnect Profile Editor für NAM.



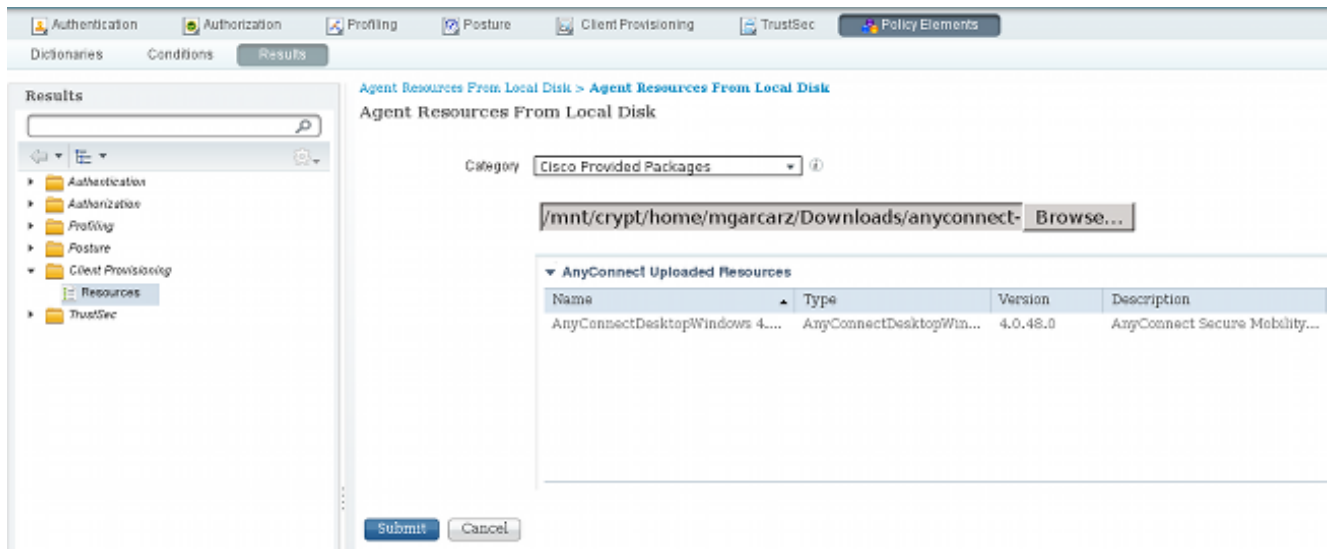
Es wurde nur eine SSID konfiguriert: **secure_access**. Speichern Sie die XML-Datei in **NAM.xml**.

Schritt 4: Installieren der Anwendung

1. Laden Sie die Anwendung manuell von Cisco.com herunter.

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

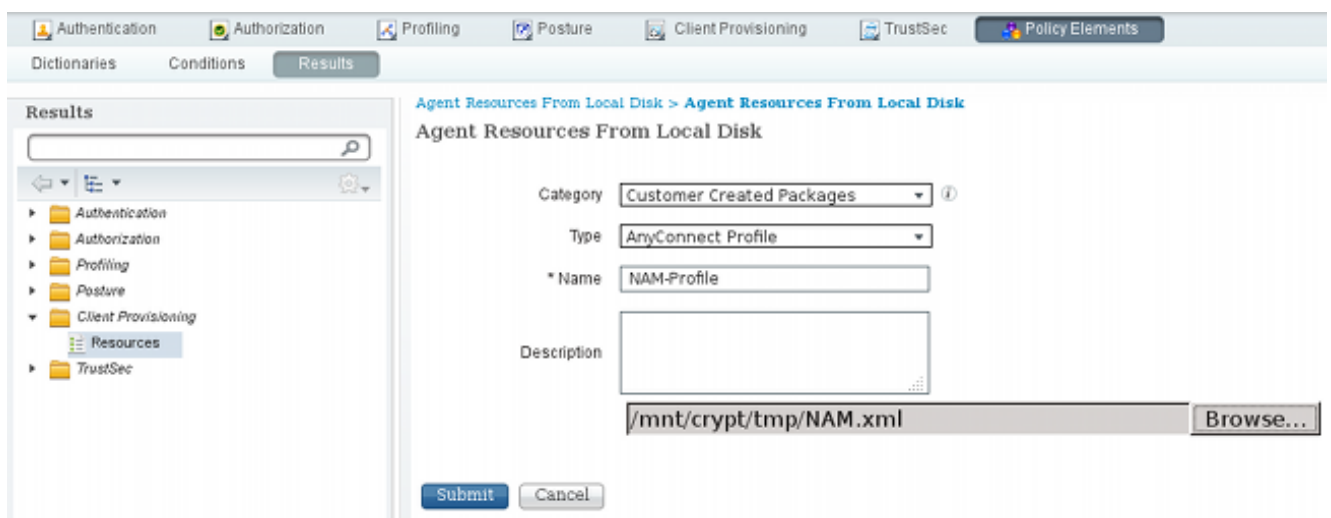
2. Navigieren Sie auf der ISE zu **Richtlinien > Ergebnisse > Client Provisioning > Resources**, und fügen Sie Agent Resources from Local Disk hinzu.
3. Wählen Sie Cisco Provided Packages (Von Cisco bereitgestellte Pakete) aus, und wählen Sie **anyconnect-win-4.0.0048-k9.pkg** aus:



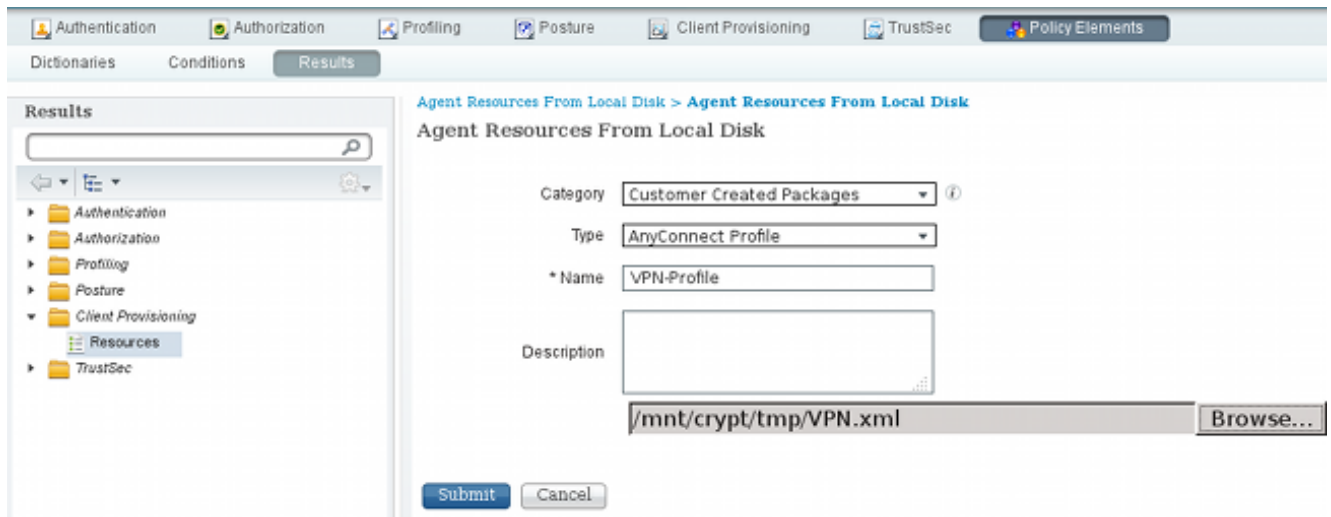
4. Wiederholen Sie Schritt 4 für das Compliance-Modul.

Schritt 5: Installieren des VPN/NAM-Profiles

1. Navigieren Sie zu **Richtlinien > Ergebnisse > Client Provisioning > Resources**, und fügen Sie Agent Resources from Local Disk hinzu.
2. Wählen Sie vom Kunden erstellte Pakete aus, und geben Sie **AnyConnect Profile** ein. Wählen Sie das zuvor erstellte NAM-Profil (XML-Datei) aus:



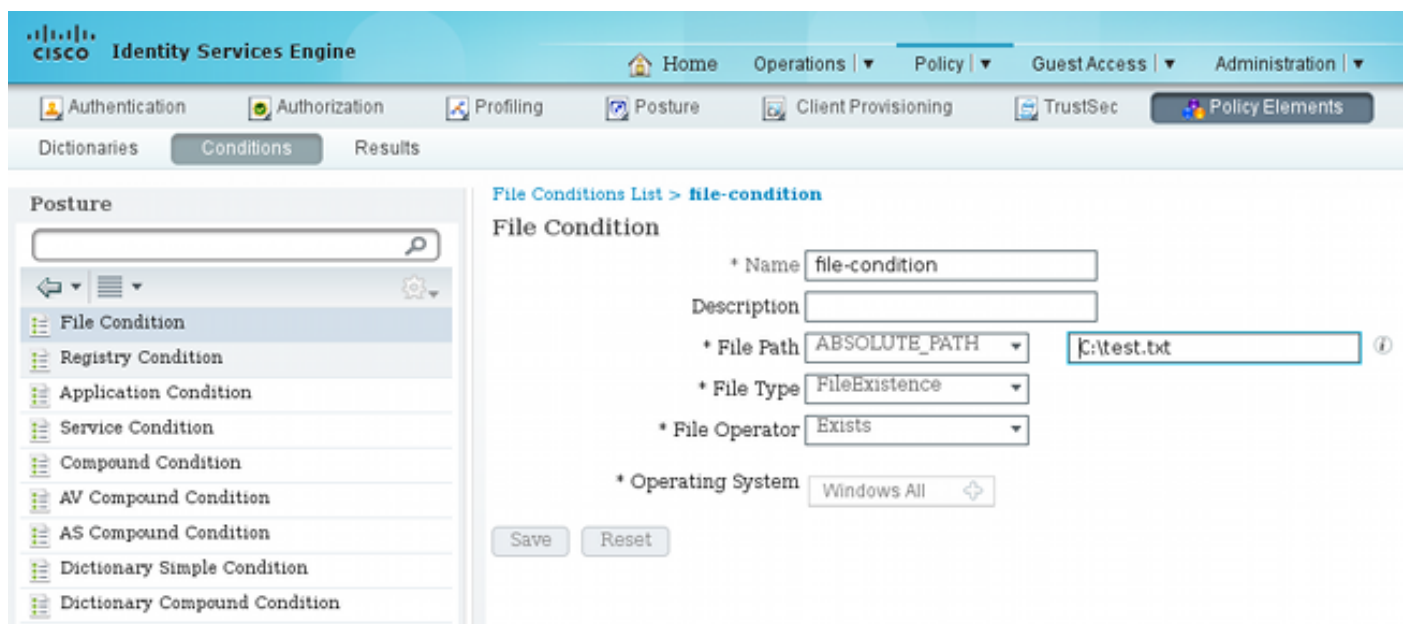
3. Wiederholen Sie ähnliche Schritte für das VPN-Profil:



Schritt 6: Konfigurieren der Statusüberprüfung

NAM- und VPN-Profile müssen extern mit dem AnyConnect-Profil-Editor konfiguriert und in die ISE importiert werden. Der Status ist jedoch vollständig auf der ISE konfiguriert.

Navigieren Sie zu **Richtlinien > Bedingungen > Status > Dateibedingung**. Sie können sehen, dass eine einfache Bedingung für das Vorhandensein einer Datei erstellt wurde. Sie müssen diese Datei haben, um die Richtlinien zu erfüllen, die vom Posture-Modul überprüft wurden:



Diese Bedingung wird für eine Anforderung verwendet:

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

Die Anforderung wird in der Statusrichtlinie für Microsoft Windows-Systeme verwendet:

Posture Policy

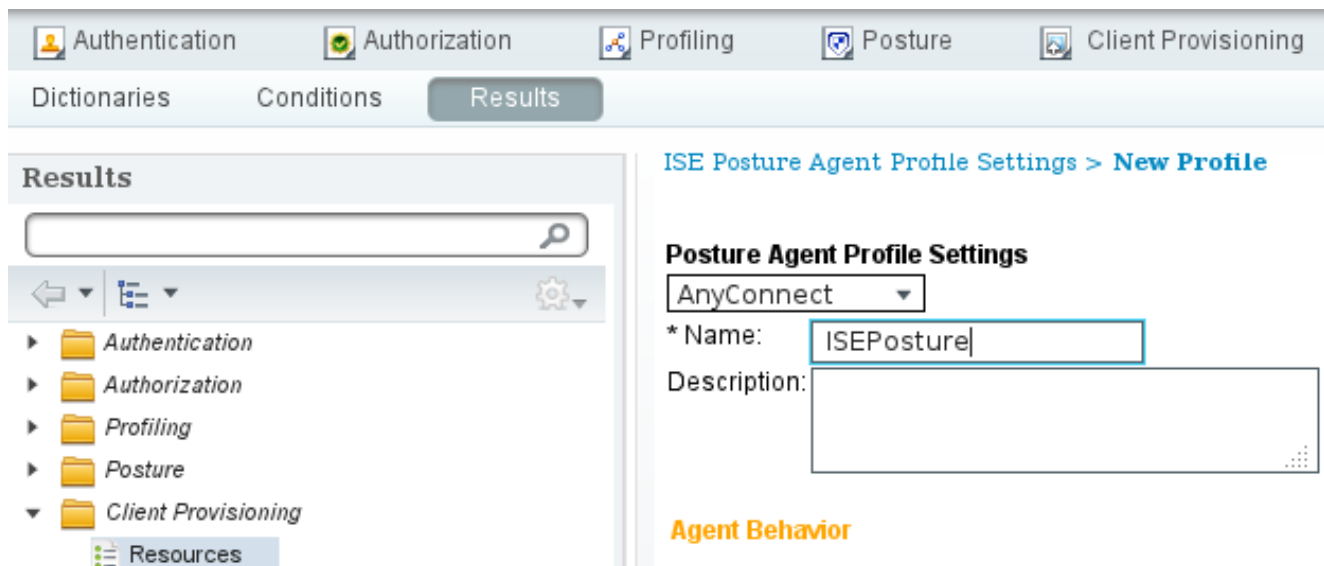
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
<input checked="" type="checkbox"/>	File	if Any	and Windows All	then	FileRequirement

Weitere Informationen zur Statuskonfiguration finden Sie [im Cisco ISE-Konfigurationshandbuch](#) unter [Statusservices](#).

Wenn die Status-Richtlinie bereit ist, ist es an der Zeit, die Status-Agent-Konfiguration hinzuzufügen.

1. Navigieren Sie zu **Richtlinien > Ergebnisse > Client Provisioning > Resources**, und fügen Sie Network Admission Control (NAC) Agent oder AnyConnect Agent Posture Profile hinzu.
2. Wählen Sie AnyConnect aus (ein neues Statusmodul aus ISE Version 1.3 wurde anstelle des alten NAC Agent verwendet):



3. Vergessen Sie nicht, im Abschnitt Posture Protocol * hinzuzufügen*, damit der Agent eine Verbindung zu allen Servern herstellen kann.

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

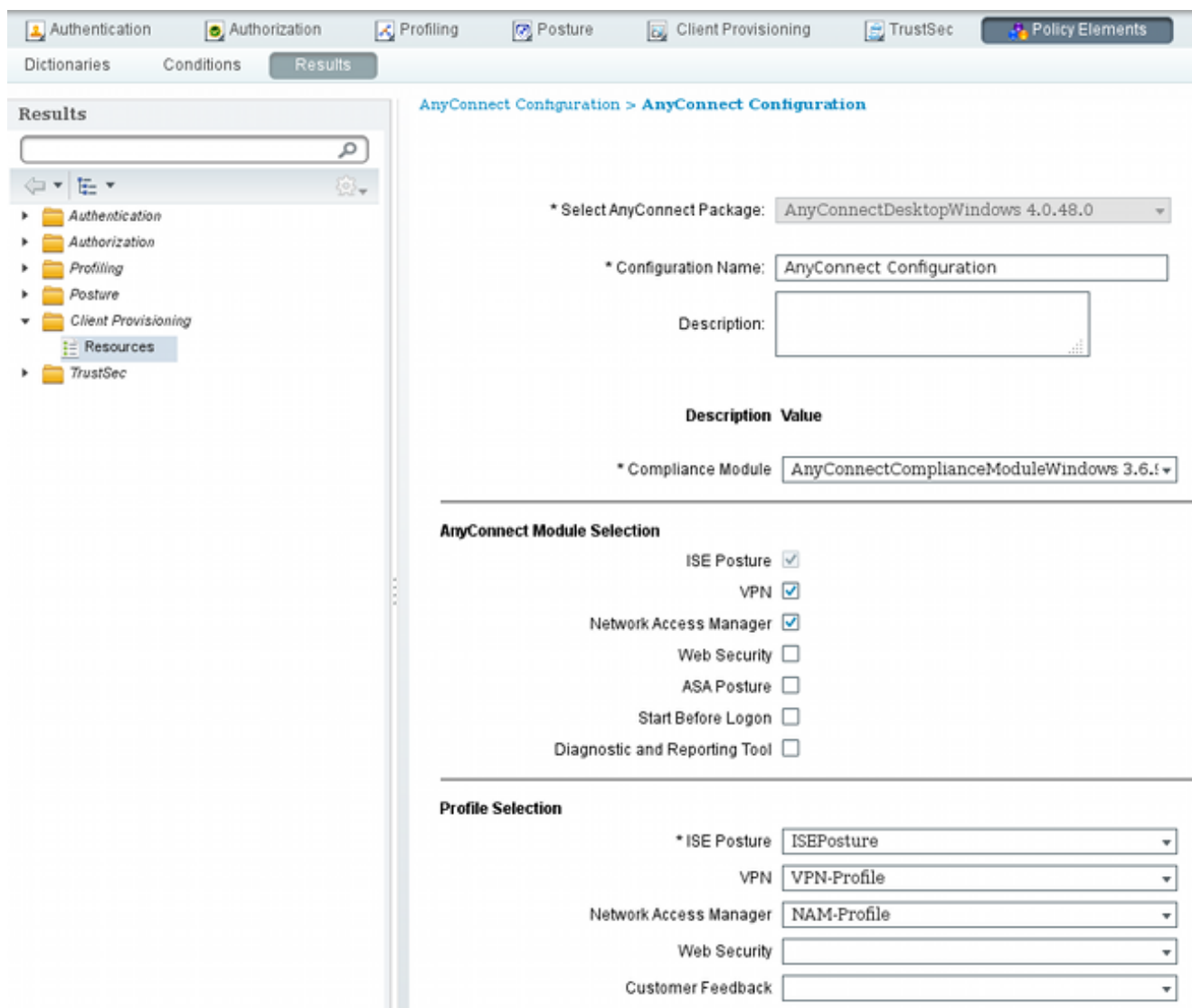
4. Wenn das Feld Servername-Regeln leer bleibt, speichert die ISE keine Einstellungen und meldet diesen Fehler:

Server name rules: valid value is required

Schritt 7: Konfigurieren von AnyConnect

In dieser Phase wurden alle Anwendungen (AnyConnect) und die Profilkonfiguration für alle Module (VPN, NAM und Status) konfiguriert. Es ist an der Zeit, sie zusammenzubinden.

1. Navigieren Sie zu **Richtlinien > Ergebnisse > Client Provisioning > Resources**, und fügen Sie AnyConnect Configuration hinzu.
2. Konfigurieren Sie den Namen, und wählen Sie das Compliance-Modul und alle erforderlichen AnyConnect-Module (VPN, NAM und Status) aus.
3. Wählen Sie in Profile Selection (Profilauswahl) das Profil aus, das zuvor für jedes Modul konfiguriert wurde.



4. Das VPN-Modul ist für die korrekte Funktion aller anderen Module obligatorisch. Auch wenn das VPN-Modul nicht für die Installation ausgewählt ist, wird es auf den Client übertragen und installiert. Wenn Sie kein VPN verwenden möchten, können Sie ein spezielles VPN-Profil konfigurieren, das die Benutzeroberfläche für das VPN-Modul verbirgt. Diese Profile sollten der **Datei VPN.xml** hinzugefügt werden:

```
<ClientInitialization>
```

```
</ClientInitialization>
```

5. Diese Art von Profil wird auch installiert, wenn Sie **Setup.exe** aus dem ISO-Paket (**anyconnect-win-3.1.06073-pre-deploy-k9.iso**) verwenden. Anschließend wird das **VPNDisable_ServiceProfile.xml**-Profil für VPN zusammen mit der Konfiguration installiert, wodurch die Benutzeroberfläche für das VPN-Modul deaktiviert wird.

Schritt 8: Client-Bereitstellungsregeln

Auf die in Schritt 7 erstellte AnyConnect-Konfiguration sollte in den Client-Bereitstellungsregeln verwiesen werden:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. Below this, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The main content area is titled "Client Provisioning Policy" and contains a table with the following columns: Rule Name, Identity Groups, Operating Systems, Other Conditions, and Results. A single rule is listed with the name "AnyconnectWin", which is checked with a green box. The rule conditions are "If Any" (Identity Groups), "and Windows All" (Operating Systems), and "and Condition(s)" (Other Conditions). The result is "then AnyConnect Configuration".

Client-Bereitstellungsregeln legen fest, welche Anwendung an den Client weitergeleitet wird. Hier ist nur eine Regel erforderlich, die auf die in Schritt 7 erstellte Konfiguration verweist. Auf diese Weise verwenden alle Microsoft Windows-Endpunkte, die für die Client-Bereitstellung umgeleitet werden, die AnyConnect-Konfiguration mit allen Modulen und Profilen.

Schritt 9: Autorisierungsprofile

Das Autorisierungsprofil für die Client-Bereitstellung muss erstellt werden. Das Standard-Client Provisioning Portal wird verwendet:

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Profile. The top navigation bar is the same as in the previous screenshot. Below it, there are tabs for Dictionaries, Conditions, and Results. The main content area is titled "Authorization Profiles > GuestProvisioning" and "Authorization Profile". The profile name is "GuestProvisioning". The description field is empty. The access type is set to "ACCESS_ACCEPT". The service template checkbox is unchecked. Under "Common Tasks", the "Web Redirection (CWA, MDM, NSP, CPP)" checkbox is checked. At the bottom, there are fields for "Client Provisioning (Posture)" (set to "ACL"), "GuestRedirect", and "Value" (set to "Client Provisioning Portal").

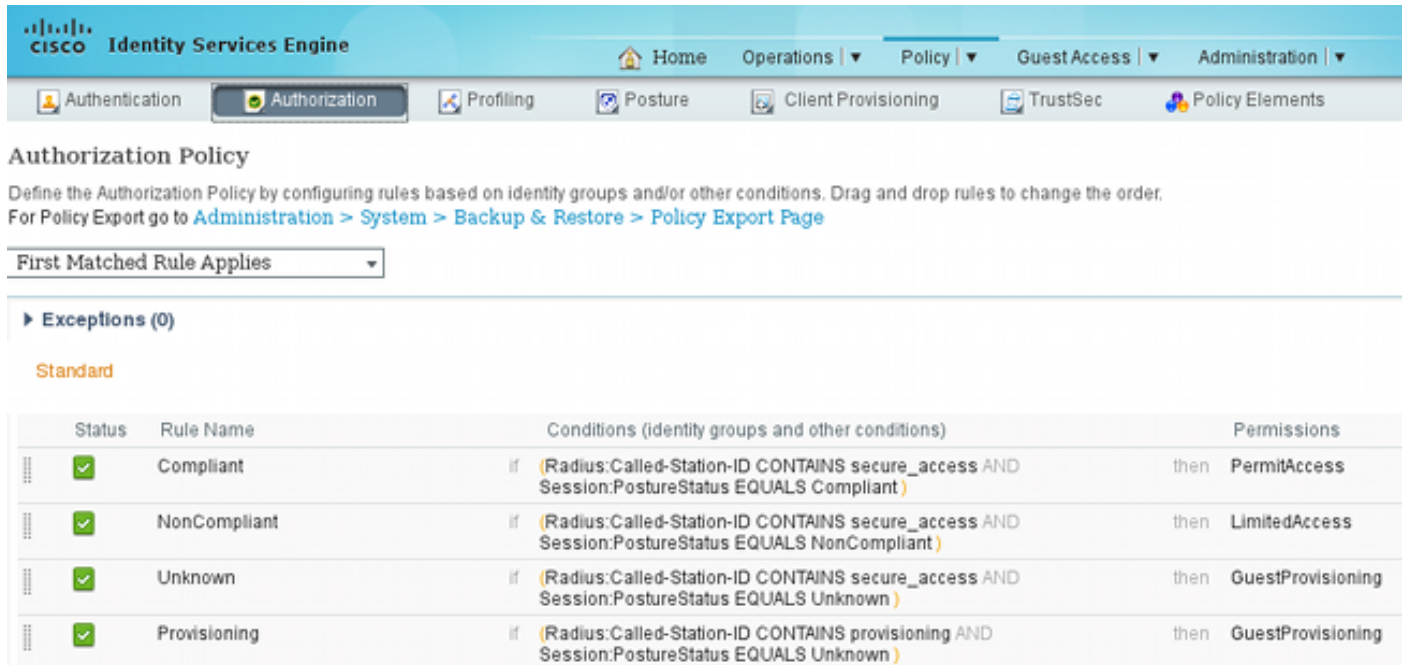
Dieses Profil erzwingt die Umleitung der Benutzer zur Bereitstellung an das Standard-Client-Bereitstellungsportal. Dieses Portal evaluiert die Client Provisioning Policy (Regeln, die in Schritt 8 erstellt wurden). Autorisierungsprofile sind die Ergebnisse der in Schritt 10 konfigurierten Autorisierungsregeln.

GuestRedirect Access Control List (ACL) ist der Name der auf dem WLC definierten ACL. Diese ACL legt fest, welcher Datenverkehr an die ISE umgeleitet werden soll. Weitere Informationen finden Sie unter [Konfigurationsbeispiel](#) für die [zentrale Webauthentifizierung mit einem Switch und der Identity Services Engine](#).

Es gibt auch ein weiteres Autorisierungsprofil, das den begrenzten Netzwerkzugriff (DACL) für nicht konforme Benutzer (LimitedAccess genannt) bereitstellt.

Schritt 10: Autorisierungsregeln

Alle werden in vier Autorisierungsregeln zusammengefasst:



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)

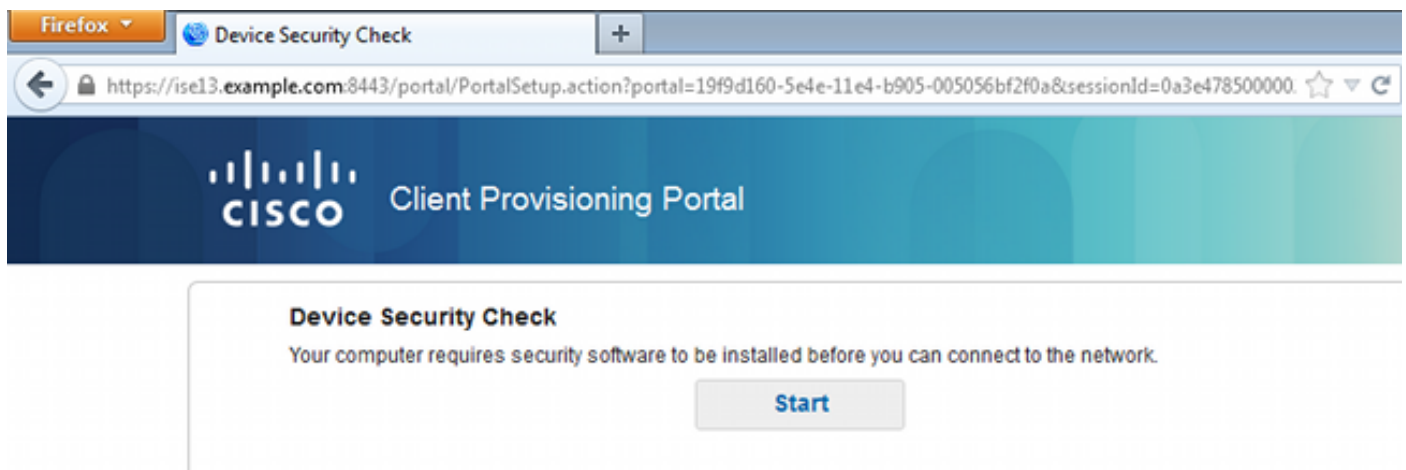
Standard

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

Zuerst stellen Sie eine Verbindung zum Provisioning SSID her und werden zur Bereitstellung an ein Standard-Client Provisioning Portal (Regel namens Provisioning) umgeleitet. Wenn Sie eine Verbindung mit der **Secure_Access** SSID herstellen, wird die Bereitstellung trotzdem umgeleitet, wenn kein Bericht des Statusmoduls von der ISE empfangen wird (Regel mit dem Namen Unknown). Sobald der Endpunkt vollständig kompatibel ist, wird der vollständige Zugriff gewährt (Regelname erfüllt). Wenn der Endpunkt als nicht konform gemeldet wird, verfügt er über eingeschränkten Netzwerkzugriff (Regel heißt "NonCompliant").

Überprüfen

Sie ordnen sich der Provisioning SSID zu, versuchen, auf eine beliebige Webseite zuzugreifen, und werden an das Client Provisioning Portal umgeleitet:



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

Da AnyConnect nicht erkannt wird, werden Sie zur Installation aufgefordert:

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

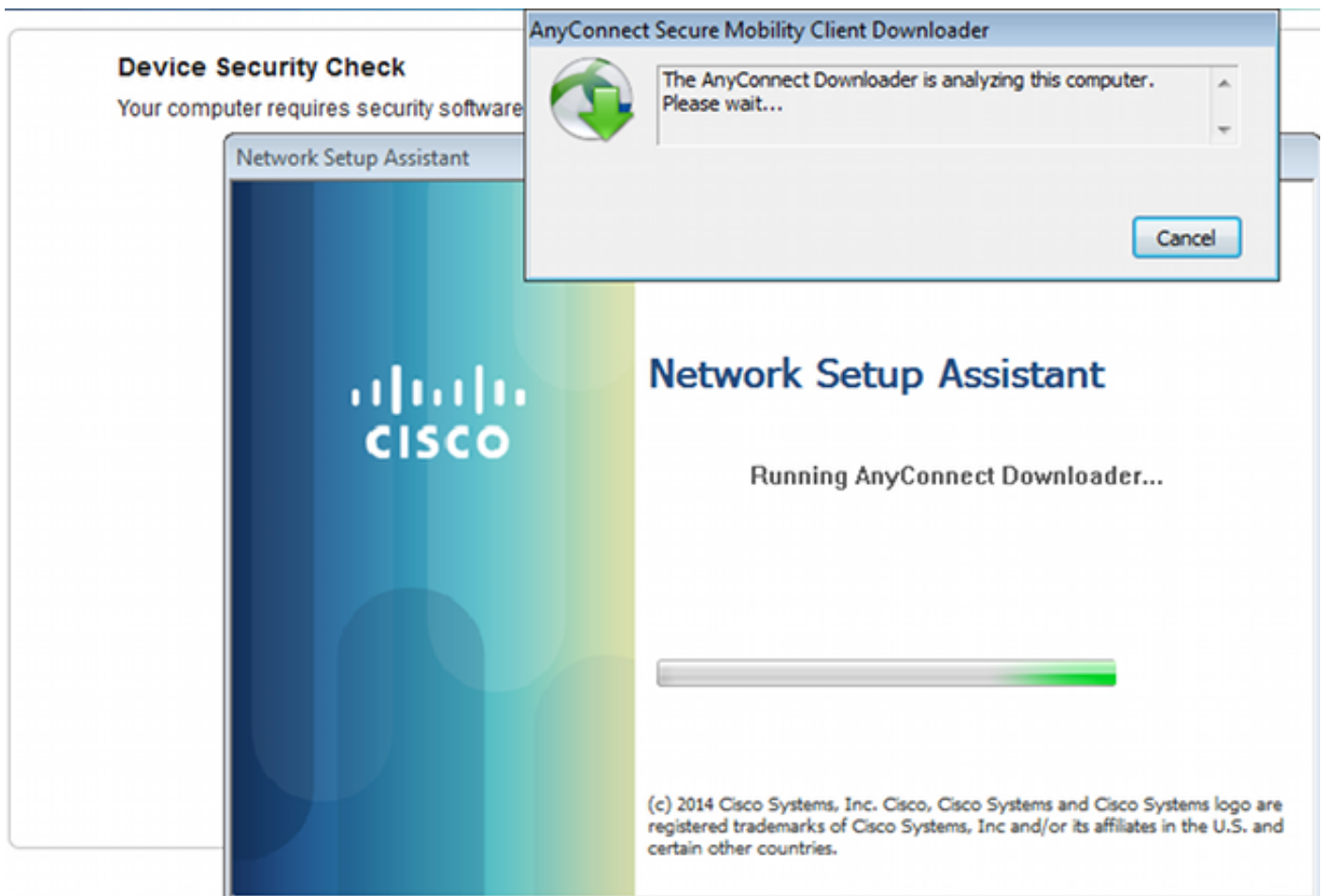
1. You must install AnyConnect to check your device before accessing the network. [Click here to download and install AnyConnect](#)
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan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

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

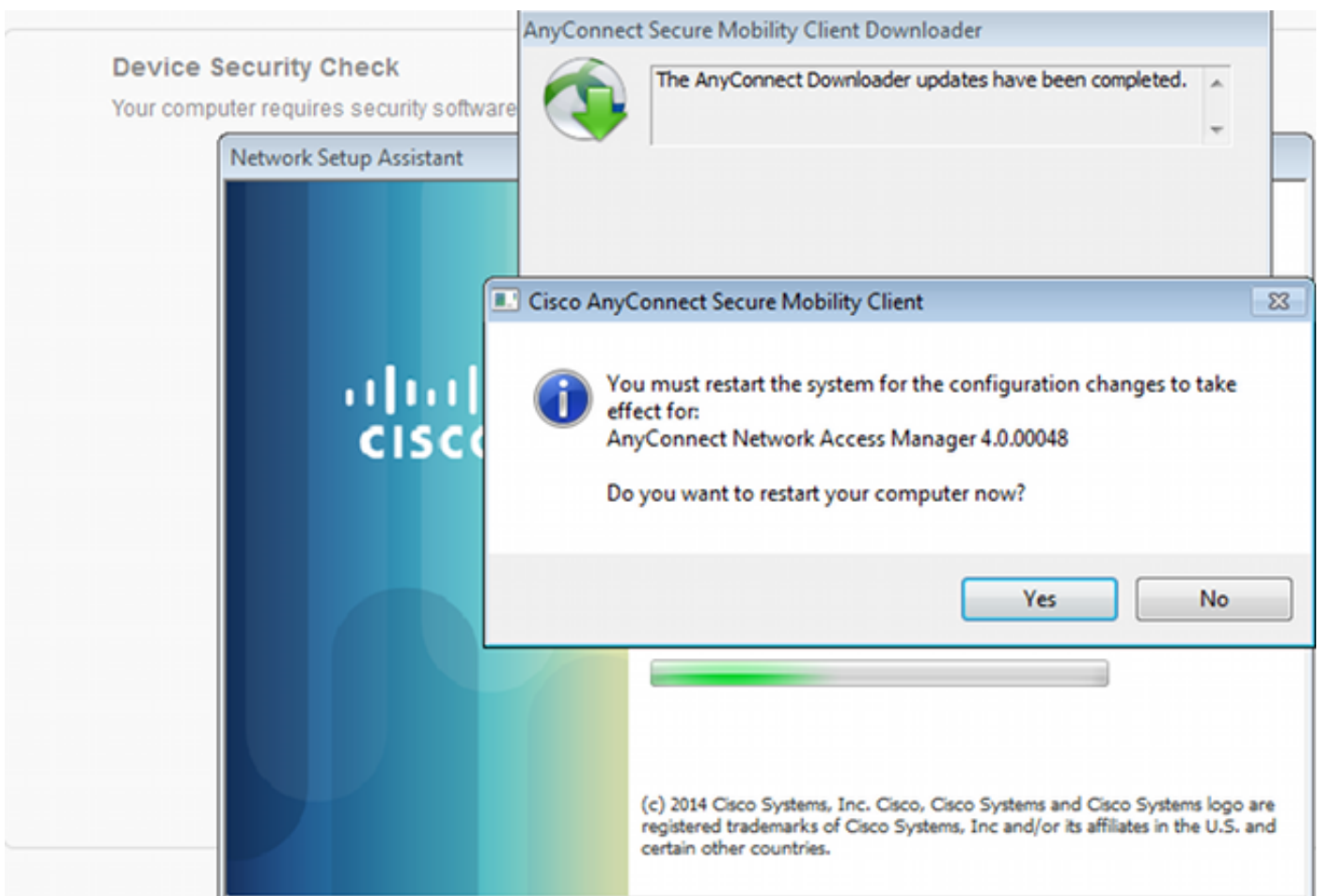
 You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

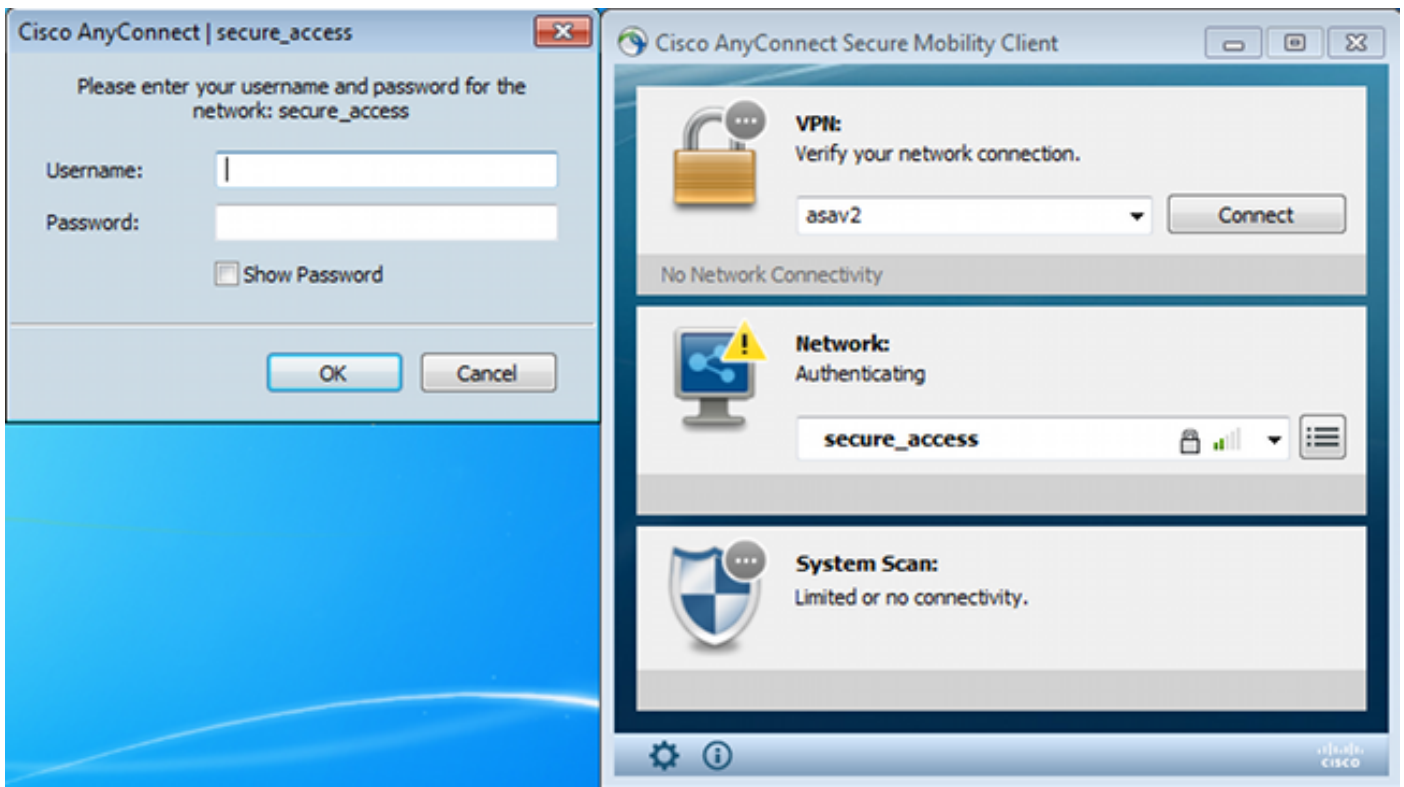
Eine kleine Anwendung namens Network Setup Assistant, die für den gesamten Installationsprozess verantwortlich ist, wird heruntergeladen. Beachten Sie, dass es sich in Version 1.2 von dem Network Setup Assistant unterscheidet.



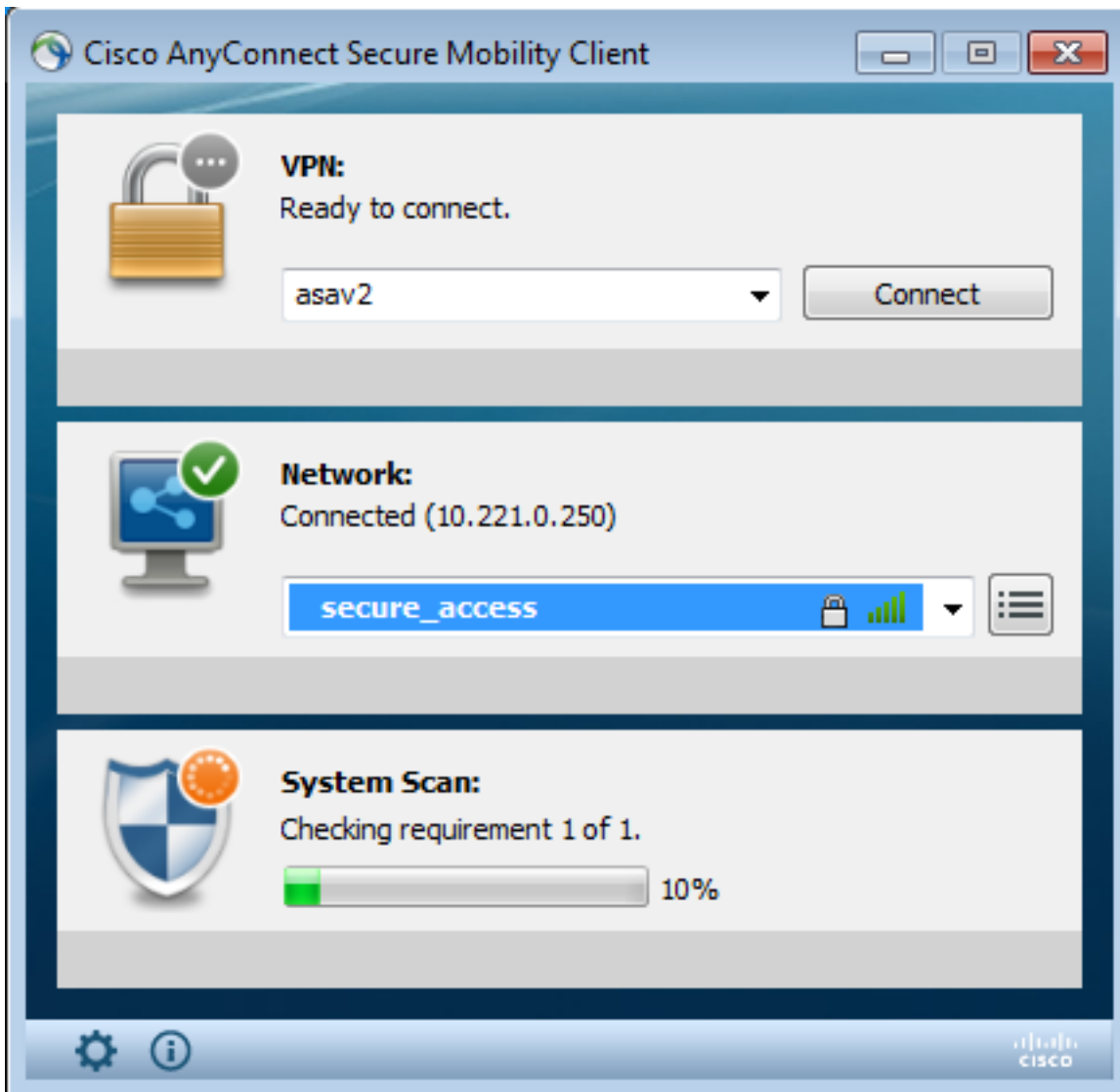
Alle Module (VPN, NAM und Status) werden installiert und konfiguriert. Sie müssen Ihren Computer neu starten:



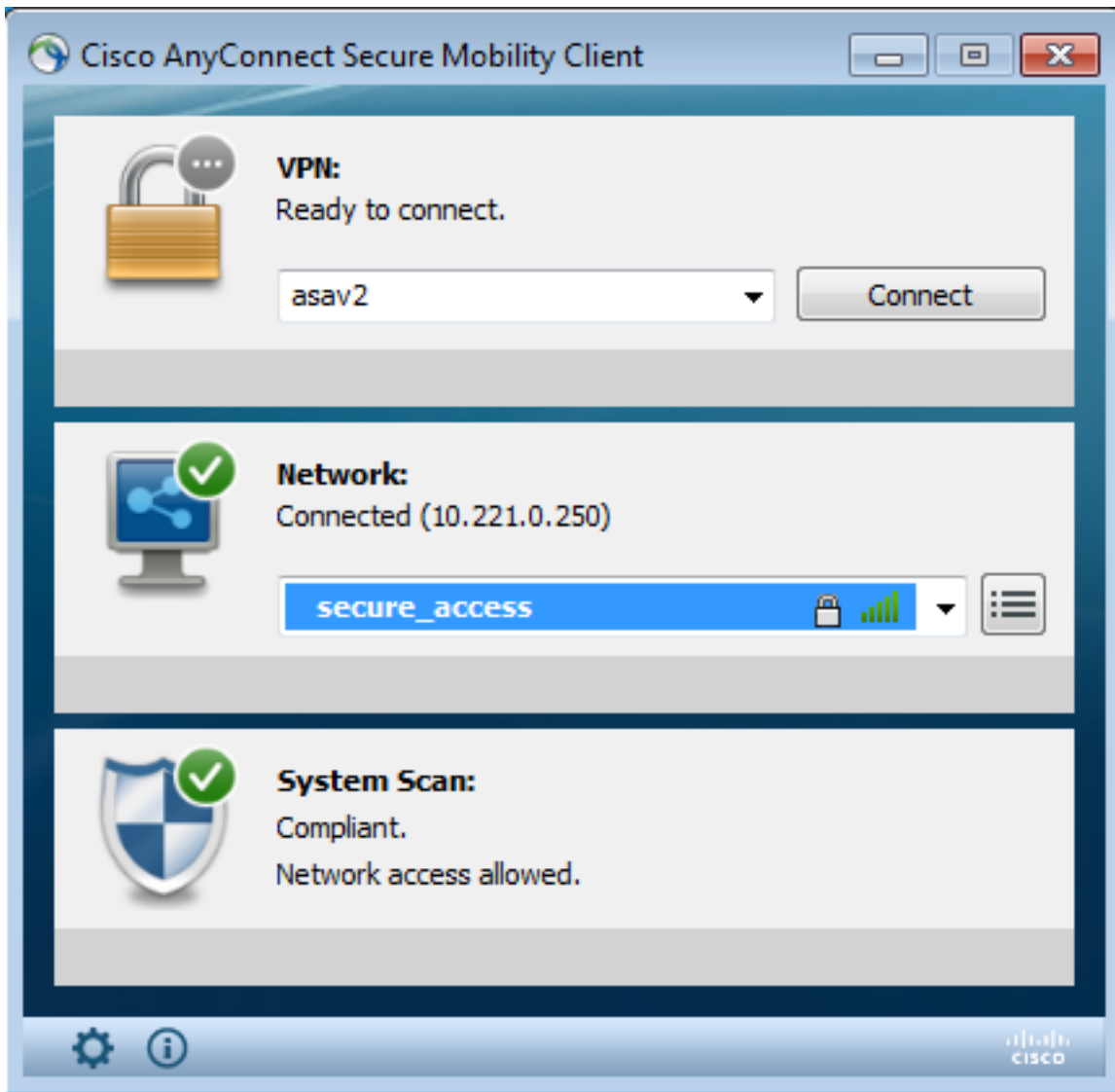
Nach dem Neustart wird AnyConnect automatisch ausgeführt, und NAM versucht, eine Verbindung zur sicheren_Zugriff-SSID herzustellen (entsprechend dem konfigurierten Profil). Beachten Sie, dass das VPN-Profil korrekt installiert ist (ASAV2-Eintrag für VPN):



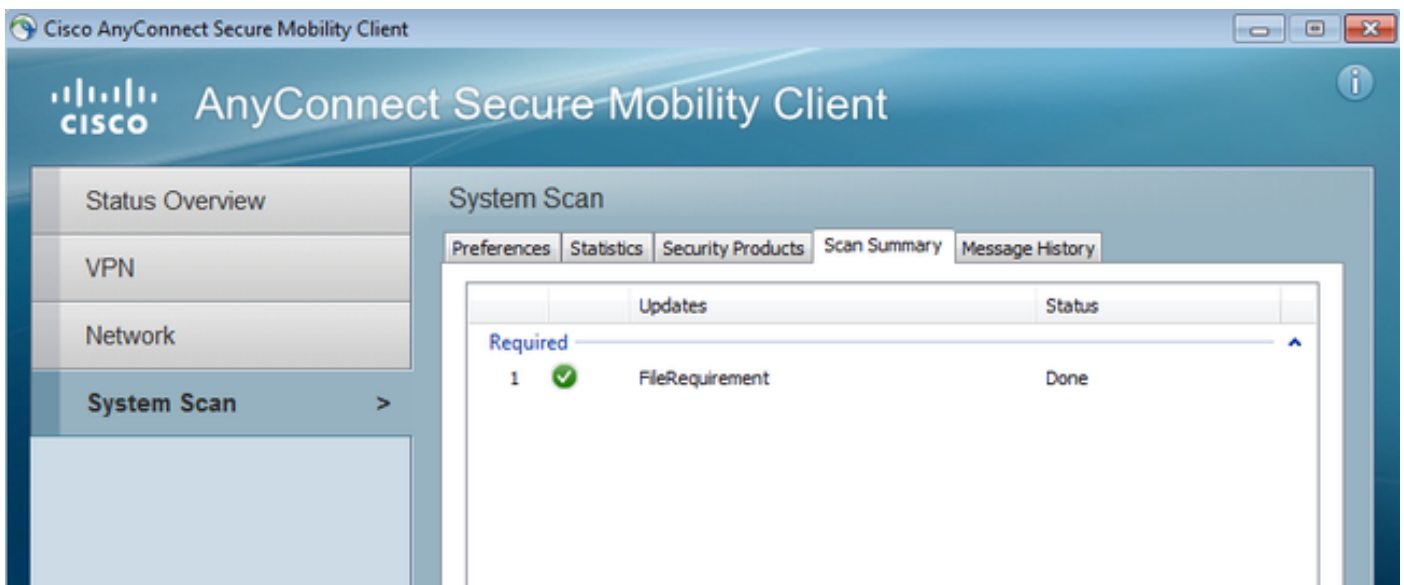
Nach der Authentifizierung lädt AnyConnect Aktualisierungen sowie Statusregeln herunter, für die eine Überprüfung durchgeführt wird:



In dieser Phase kann der Zugriff weiterhin eingeschränkt sein (Sie sehen die Unknown Authorization-Regel auf der ISE). Sobald die Station den Vorgaben entspricht, wird sie vom Posture-Modul gemeldet:



Die Details können ebenfalls überprüft werden (die FileRequirement-Anweisung ist erfüllt):



Der Nachrichtenverlauf zeigt detaillierte Schritte:

```
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.**

Der erfolgreiche Bericht wird an die ISE gesendet, was den Autorisierungswechsel auslöst. Bei der zweiten Authentifizierung wird die Compliance-Regel beachtet, und der vollständige Netzwerkzugriff wird gewährt. Wenn der Statusbericht gesendet wird, während er weiterhin der Provisioning SSID zugeordnet ist, werden diese Protokolle auf der ISE angezeigt:

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

Der Statusbericht zeigt Folgendes an:

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

Detaillierte Berichte zeigen die erfüllte FileRequirement an:

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		

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Statusservices im Cisco ISE-Konfigurationsleitfaden](#)
- [Cisco ISE 1.3 Administratorhandbuch](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)