

AnyConnect 4.0與ISE 1.3版整合配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[拓撲和流](#)

[設定](#)

[WLC](#)

[ISE](#)

[步驟1.新增WLC](#)

[步驟2.配置VPN配置檔案](#)

[步驟3.配置NAM配置檔案](#)

[步驟4.安裝應用程式](#)

[步驟5.安裝VPN/NAM配置檔案](#)

[步驟6.配置狀態](#)

[步驟7.配置AnyConnect](#)

[步驟8. 客戶端調配規則](#)

[步驟9.授權配置檔案](#)

[步驟10.授權規則](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹思科身份服務引擎(ISE)版本1.3中的新功能，通過該功能，您可以配置多個AnyConnect安全移動客戶端模組並將其自動調配到終端。本文檔介紹如何在ISE上配置VPN、網路訪問管理器(NAM)和狀態模組並將其推送到公司使用者。

必要條件

需求

思科建議您瞭解以下主題：

- ISE部署、身份驗證和授權
- 無線區域網路控制器(WLC)的組態
- 基本VPN和802.1x知識
- 使用AnyConnect配置檔案編輯器配置VPN和NAM配置檔案

採用元件

步驟3.如果站狀態未知（沒有來自狀態模組的報告），系統仍重定向該站狀態以進行調配，因為ISE上遇到**Unknown Authz**規則。一旦站台合規，ISE會向無線LAN控制器傳送授權變更(CoA)，從而觸發重新驗證。進行第二次身份驗證，並在ISE上點選**Compliant**規則，這將為使用者提供對網路的完全訪問許可權。

因此，已為使用者調配了AnyConnect VPN、NAM和狀態模組，這些模組允許統一訪問網路。類似功能可在自適應安全裝置(ASA)上用於VPN訪問。目前，ISE可以使用非常精細的方法對任何型別的訪問執行相同操作。

此功能並不限於企業使用者，但是最常見的情況可能是為該使用者組部署它。

設定

WLC

WLC配置了兩個SSID:

- 布建 — [WPA + WPA2][Auth(802.1X)]。此SSID用於AnyConnect調配。
- Secure_access - [WPA + WPA2][Auth(802.1X)]。此SSID用於在終端調配了為該SSID配置的NAM模組後進行安全訪問。

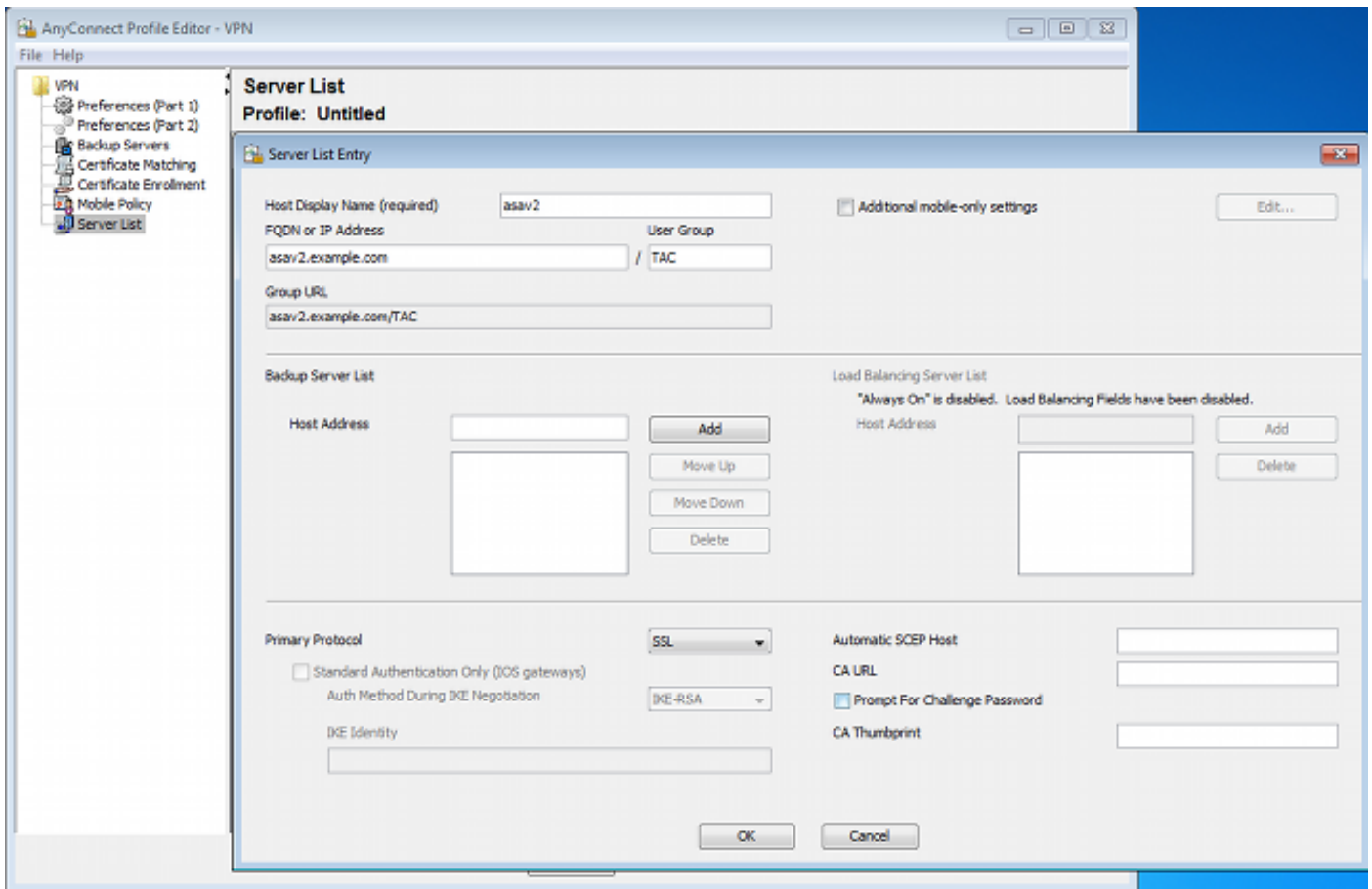
ISE

步驟1.新增WLC

將WLC新增到ISE上的網路裝置。

步驟2.配置VPN配置檔案

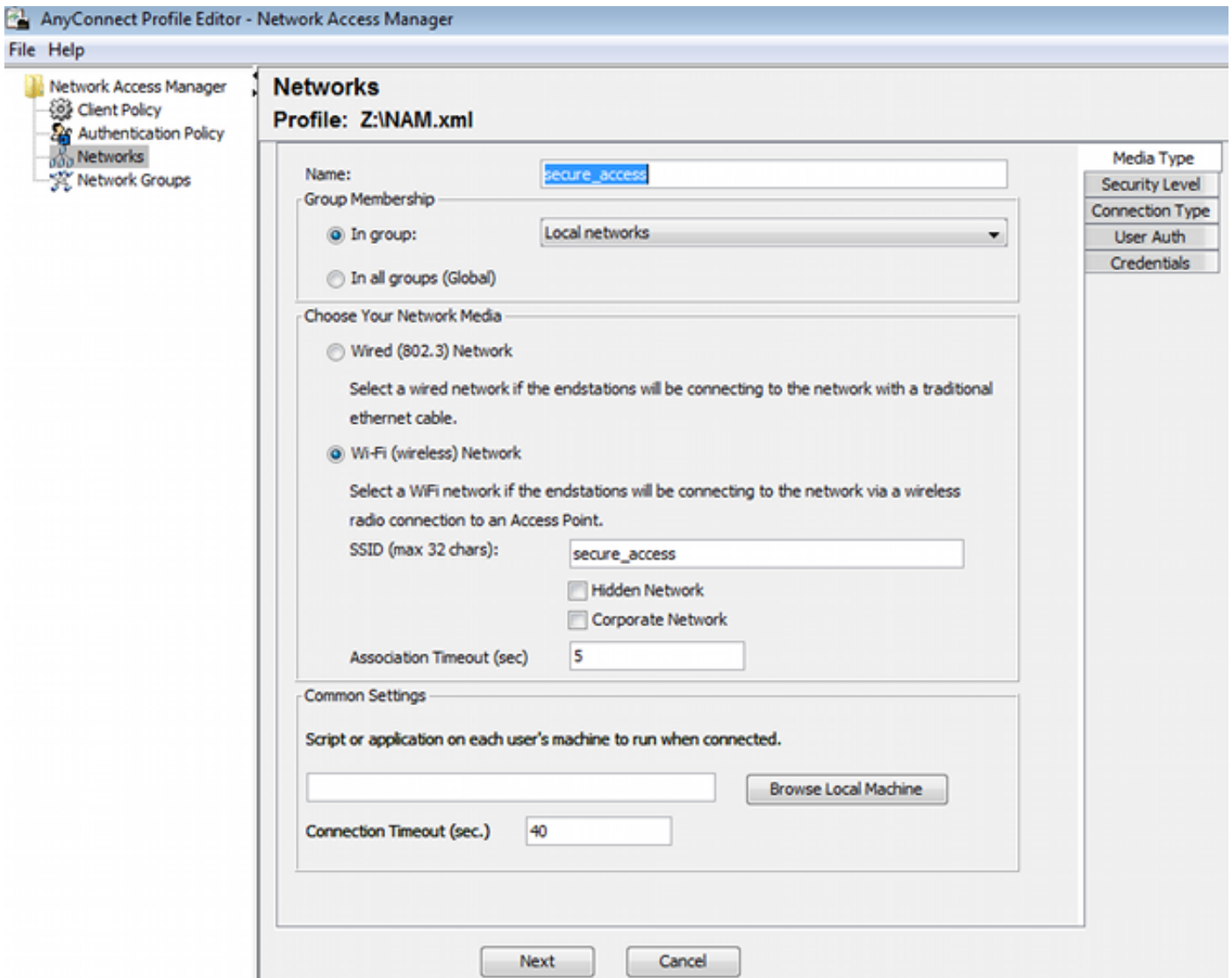
使用AnyConnect Profile Editor for VPN配置VPN配置檔案。



僅新增了一個用於VPN訪問的條目。將該XML檔案儲存到VPN.xml。

步驟3.配置NAM配置檔案

使用AnyConnect Profile Editor for NAM配置NAM配置檔案。



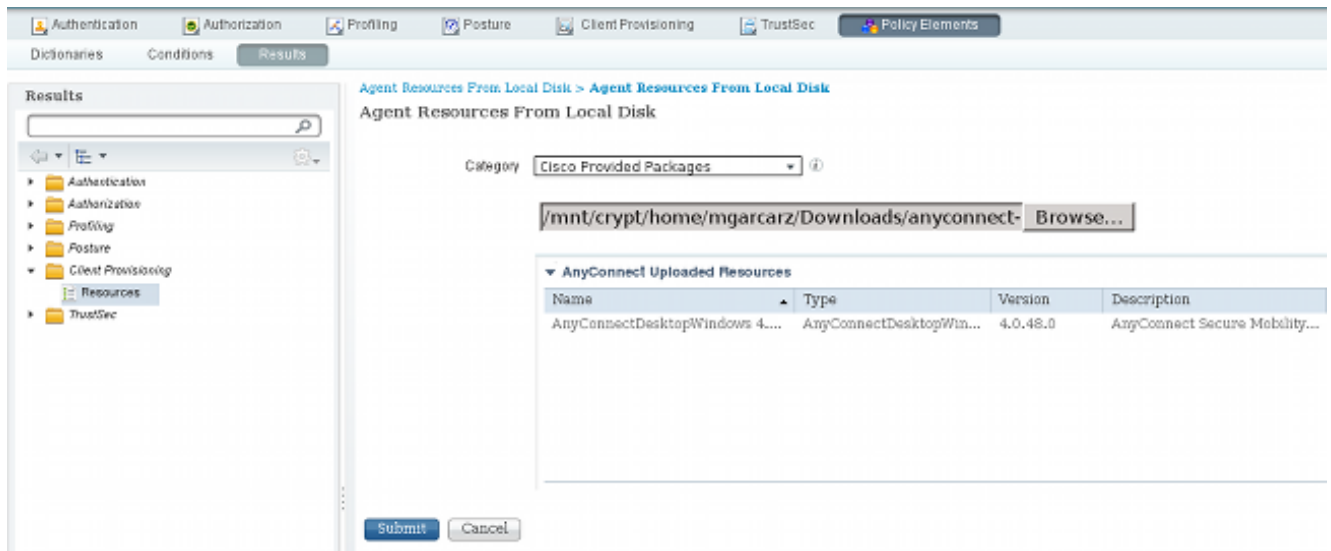
僅配置了一個SSID:secure_access。將該XML檔案儲存到NAM.xml。

步驟4.安裝應用程式

1. 從Cisco.com手動下載應用程式。

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

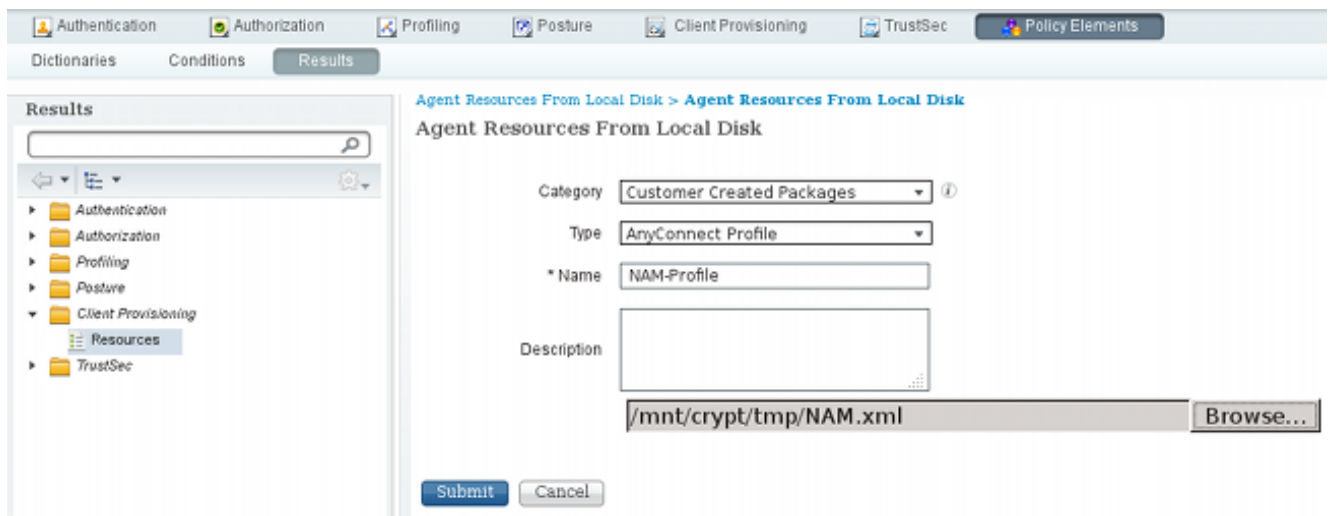
2. 在ISE上，導航到Policy > Results > Client Provisioning > Resources，並從本地磁碟新增代理資源。
3. 選擇Cisco Provided Packages (思科提供的軟體包) 並選擇anyconnect-win-4.0.00048-k9.pkg:



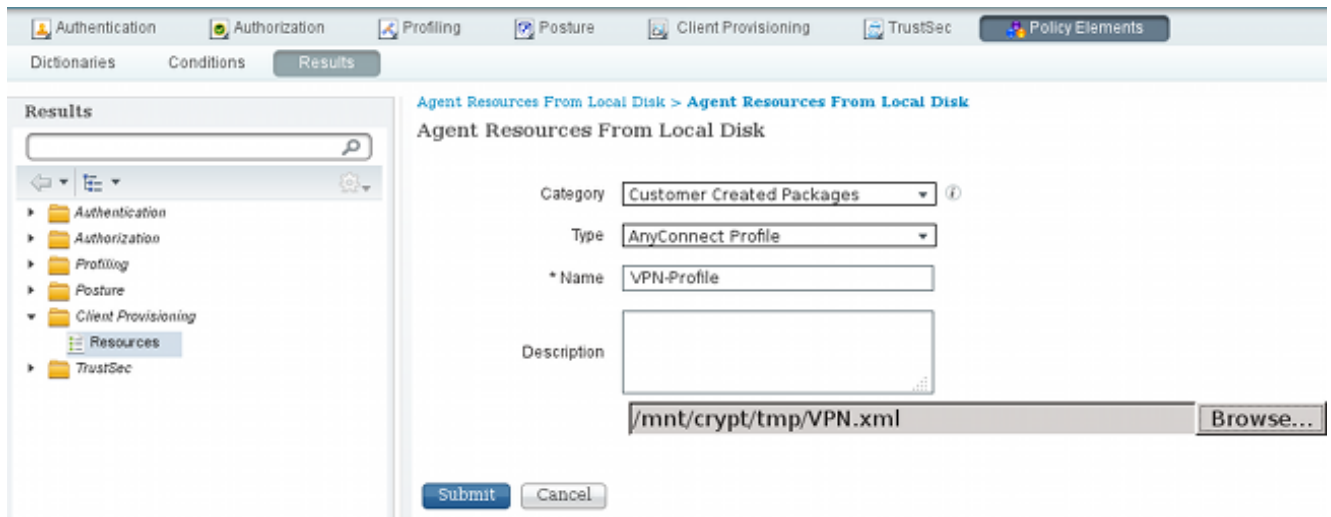
4. 對遵從性模組重複步驟4。

步驟5.安裝VPN/NAM配置檔案

1. 導航到Policy > Results > Client Provisioning > Resources，然後從本地磁碟新增代理資源。
2. 選擇Customer Created Packages並鍵入AnyConnect Profile。選擇以前建立的NAM配置檔案（XML檔案）：



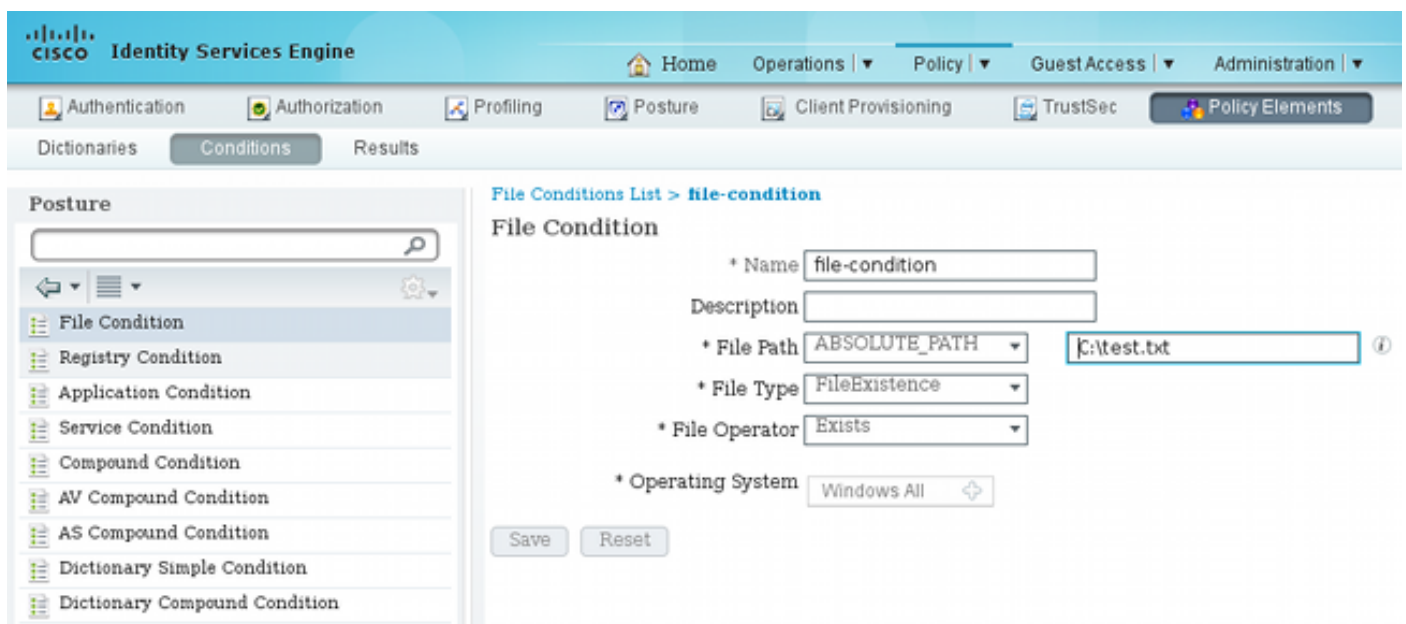
3. 對VPN配置檔案重複類似步驟：



步驟6.配置狀態

必須使用AnyConnect配置檔案編輯器在外部配置NAM和VPN配置檔案並將其匯入到ISE中。但是，安全評估在ISE上完全配置。

導航到**Policy > Conditions > Posture > File Condition**。您可以看到已建立了一個簡單的檔案存在條件。您必須擁有該檔案才能符合安全狀態模組驗證的策略：



此條件用於需求：

| 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 |

此要求用於Microsoft Windows系統的終端安全評估策略：

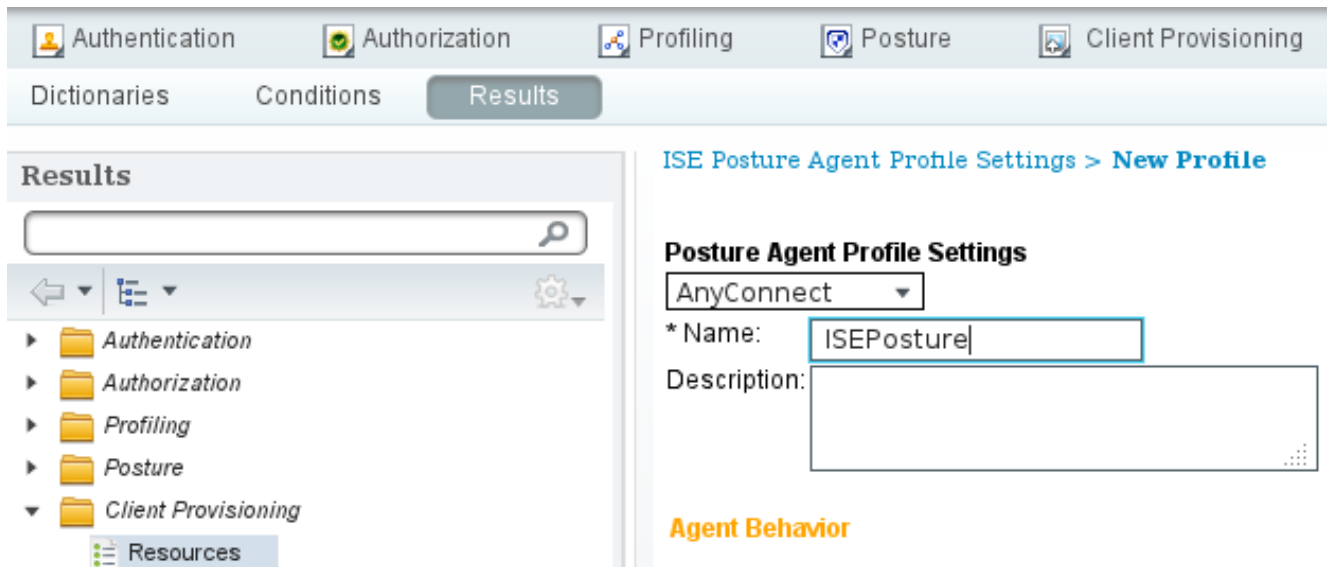
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

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

有關終端安全評估配置的詳細資訊，請參閱[思科ISE配置指南上的終端安全評估服務](#)。

狀態策略就緒後，是時候新增狀態代理配置了。

1. 導覽至Policy > Results > Client Provisioning > Resources，然後新增網路認可控制(NAC)代理或AnyConnect Agent狀態設定檔。
2. 選擇AnyConnect (已使用ISE版本1.3中的新終端安全評估模組，而不是舊的NAC代理)：



3. 在Posture Protocol部分，不要忘記新增*以允許代理連線到所有伺服器。

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 |

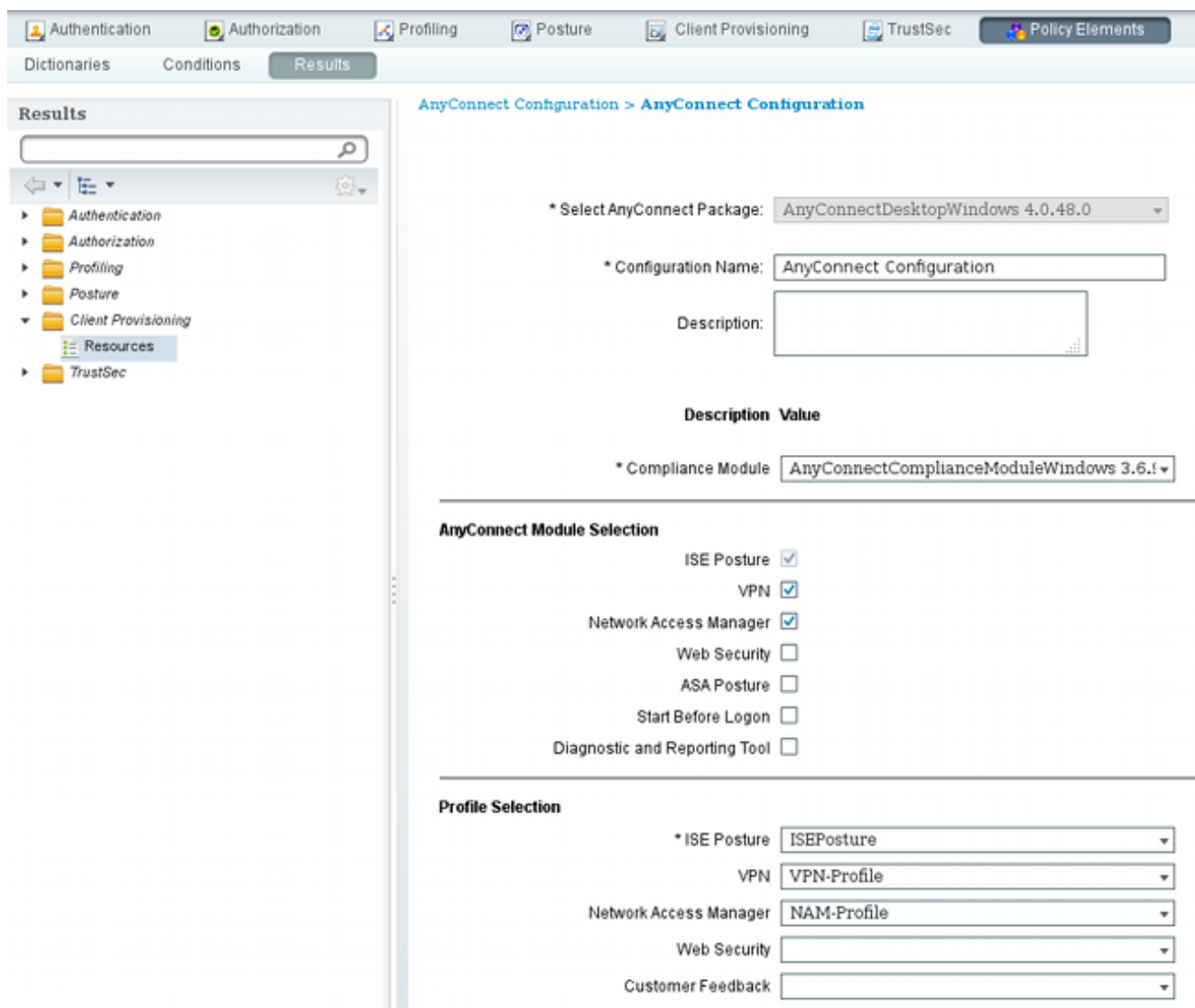
4. 如果「伺服器名稱規則」欄位為空，ISE不儲存設定並報告以下錯誤：

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

步驟7.配置AnyConnect

在這個階段，所有應用程式(AnyConnect)和所有模組 (VPN、NAM和狀態) 的配置檔案配置都已配置。是時候把它綁在一起了。

1. 導航到Policy > Results > Client Provisioning > Resources，然後新增AnyConnect Configuration。
2. 配置名稱並選擇合規性模組和所有所需的AnyConnect模組 (VPN、NAM和安全狀態)。
3. 在配置檔案選擇中，選擇之前為每個模組配置的配置檔案。



4. VPN模組是所有其他模組正常運行的必備模組。即使未選擇安裝VPN模組，也會將其推入並安裝到客戶端上。如果您不想使用VPN，可以為VPN配置一個特殊配置檔案，該配置檔案隱藏VPN模組的使用者介面。這些行應新增到VPN.xml檔案中：

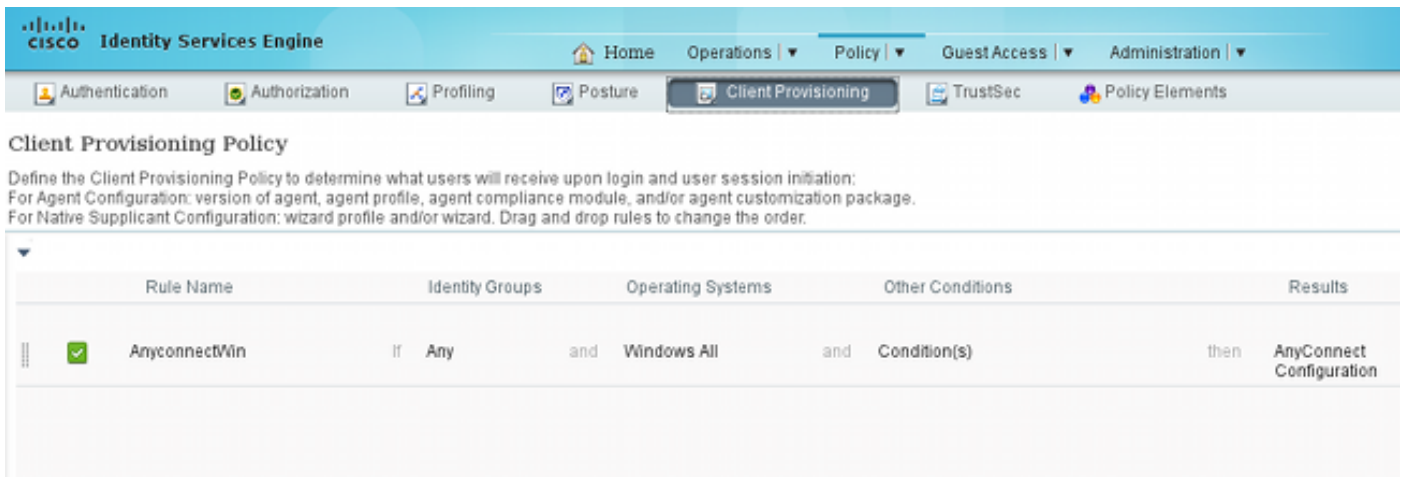
```
<ClientInitialization>
```

```
</ClientInitialization>
```

5. 當您使用iso程式包(anyconnect-win-3.1.06073-pre-deploy-k9.iso)中的Setup.exe時，也會安裝此類配置檔案。然後，會隨配置一起安裝VPN的VPNDisable_ServiceProfile.xml配置檔案，從而禁用VPN模組的使用者介面。

步驟8. 客戶端調配規則

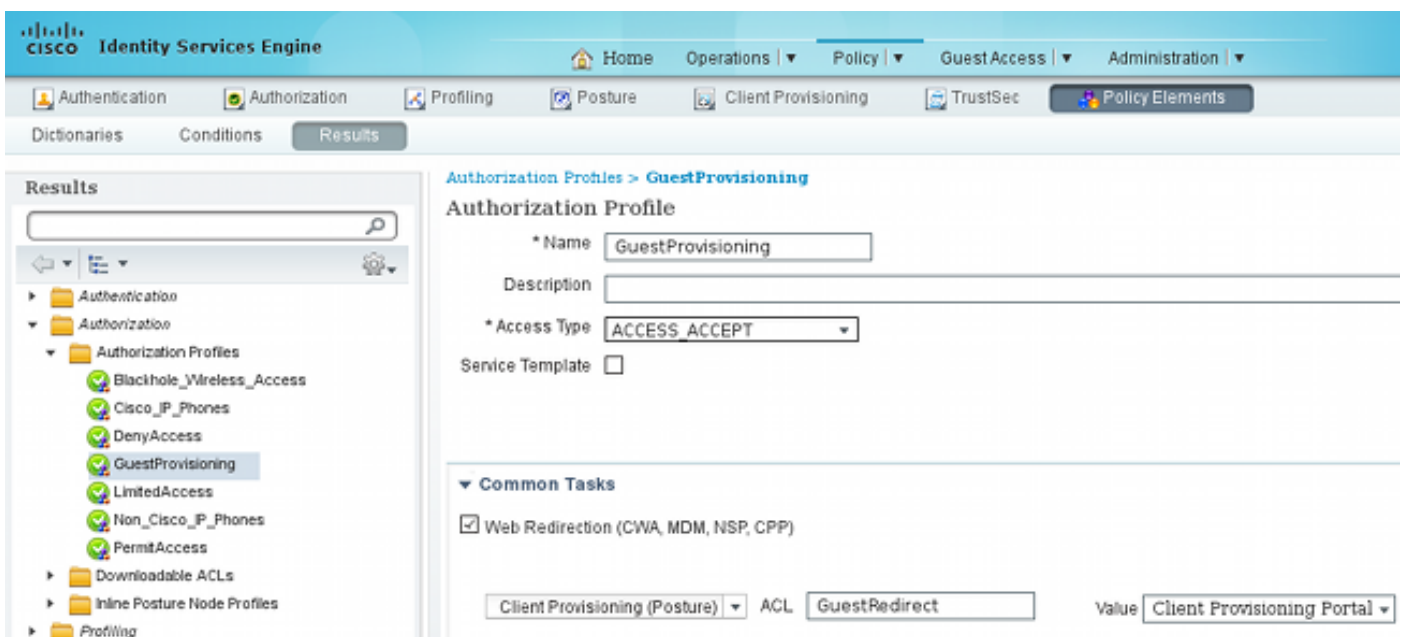
應在客戶端調配規則中引用步驟7中建立的AnyConnect配置：



客戶端調配規則決定要將哪個應用程式推送到客戶端。此處只需要一條規則，其結果指向步驟7中建立的配置。這樣，重定向到客戶端預配的所有Microsoft Windows端點將使用AnyConnect配置以及所有模組和配置檔案。

步驟9.授權配置檔案

需要建立客戶端調配的授權配置檔案。使用預設客戶端調配門戶：



此配置檔案強制將使用者重定向以調配到預設客戶端調配門戶。此門戶評估客戶端調配策略（在步驟8中建立的規則）。授權配置檔案是在步驟10中配置的授權規則的結果。

GuestRedirect Access Control List(ACL)是在WLC上定義的ACL的名稱。此ACL決定應將哪些流量重定向到ISE。如需詳細資訊，請參閱[使用交換機和身分識別服務引擎的中央Web驗證組態範例](#)。

還有另一個授權配置檔案為非合規使用者（稱為LimitedAccess）提供有限網路訪問(DACL)。

步驟10.授權規則

所有這些規則合併為四個授權規則：

CISCO Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentication | **Authorization** | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

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 |

首先連線到調配SSID，然後重定向至預設客戶端調配門戶（名為調配的規則）。連線到 **Secure_access** SSID後，如果ISE未收到來自終端安全評估模組的報告（名為Unknown的規則），它仍會重定向以進行調配。終端完全合規後，將授予完全訪問許可權（符合規則名稱）。如果終端報告為不合規的，則其網路訪問受到限制（名為NonCompliant的規則）。

驗證

您與調配SSID關聯，嘗試訪問任何網頁，然後重定向到客戶端調配門戶：

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

由於未檢測到AnyConnect，因此要求您安裝：

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

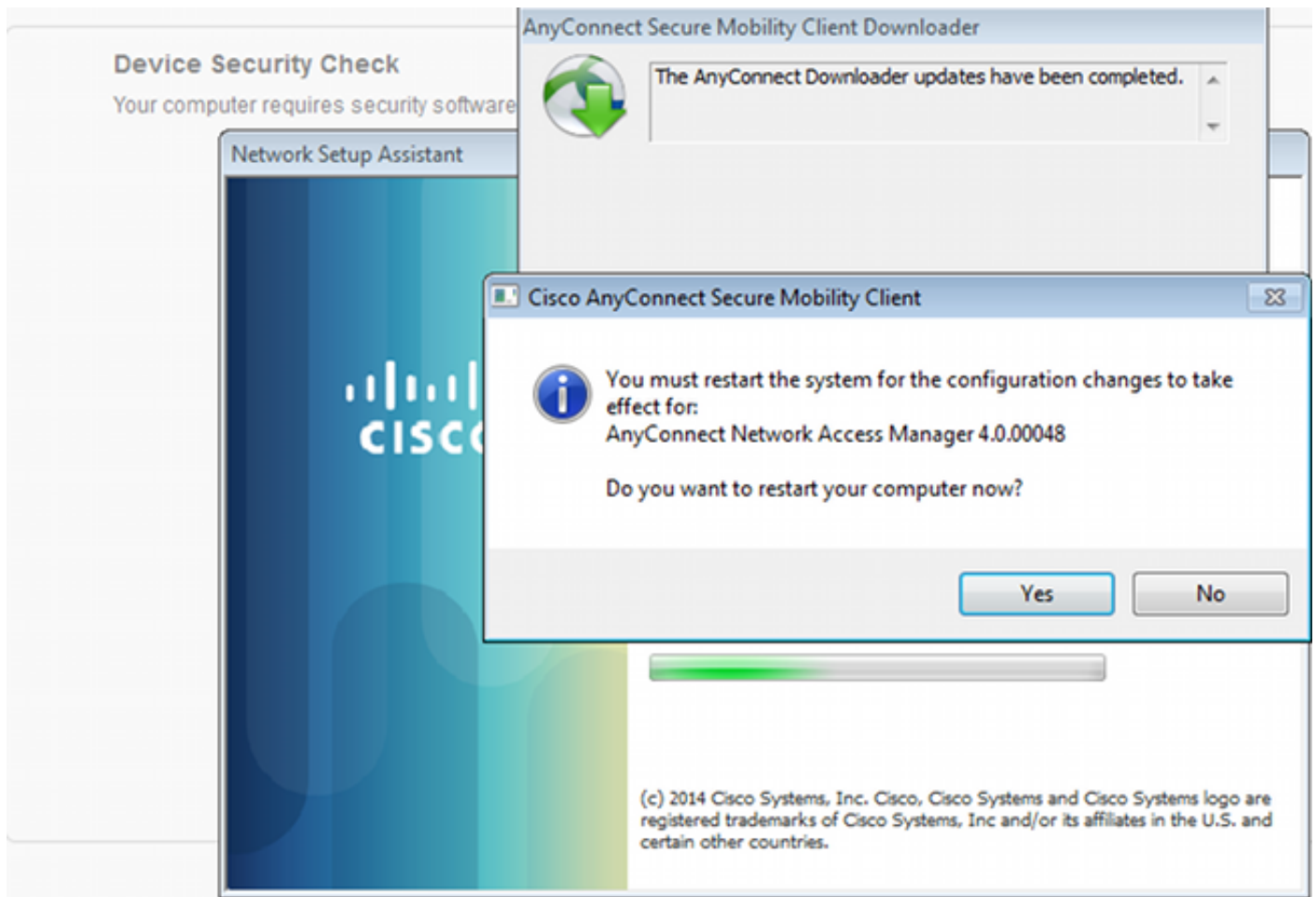
+ Remind me what to do next

下載一個名為Network Setup Assistant的小型應用程式，它負責整個安裝過程。請注意，它與1.2版中的Network Setup Assistant不同。

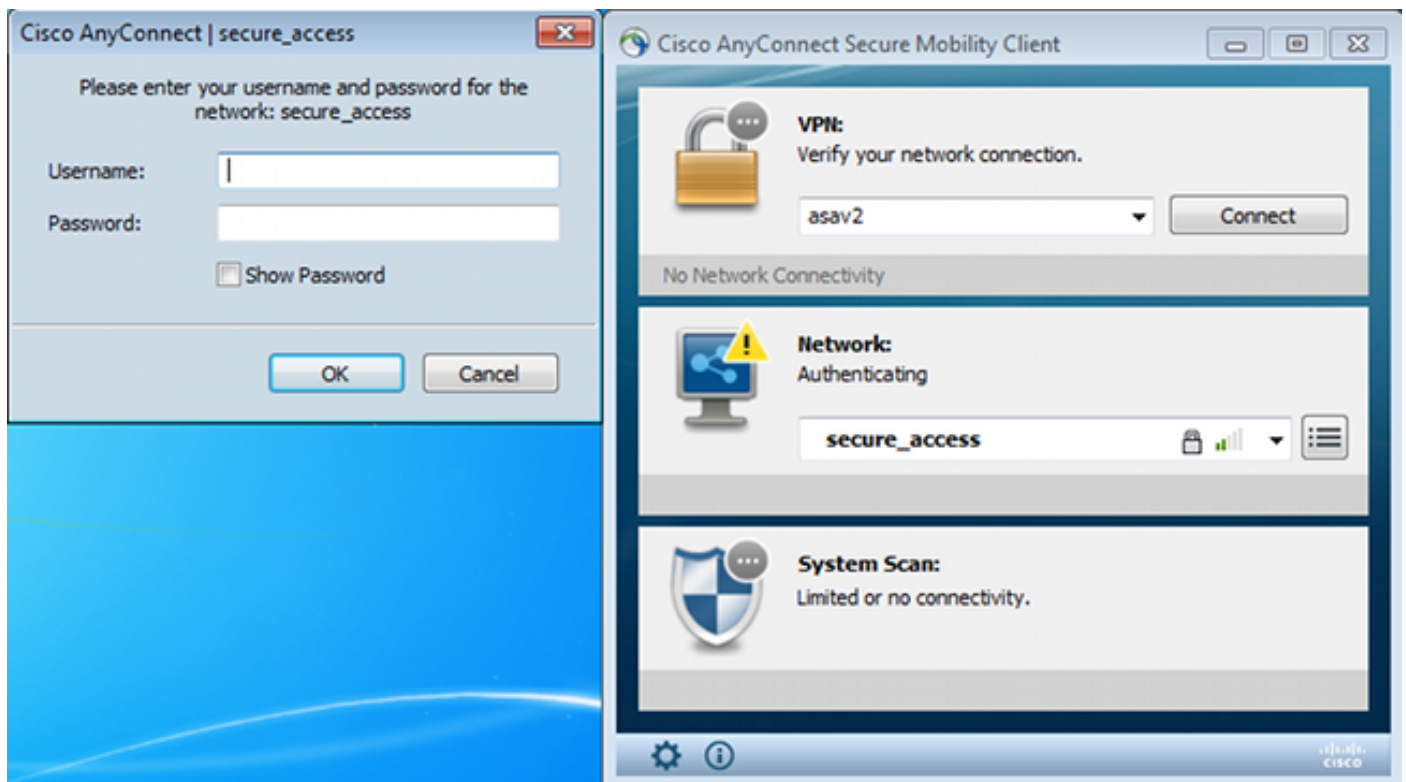


The screenshot shows the Network Setup Assistant interface. On the left, a 'Device Security Check' panel indicates that security software is required. The main window displays the Cisco logo and the text 'Network Setup Assistant' and 'Running AnyConnect Downloader...'. A progress bar is visible below the text. An 'AnyConnect Secure Mobility Client Downloader' dialog box is overlaid on top, showing a green circular arrow icon and the message: 'The AnyConnect Downloader is analyzing this computer. Please wait...'. A 'Cancel' button is located in the bottom right corner of the dialog box. At the bottom of the main window, there is a copyright notice: '(c) 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.'

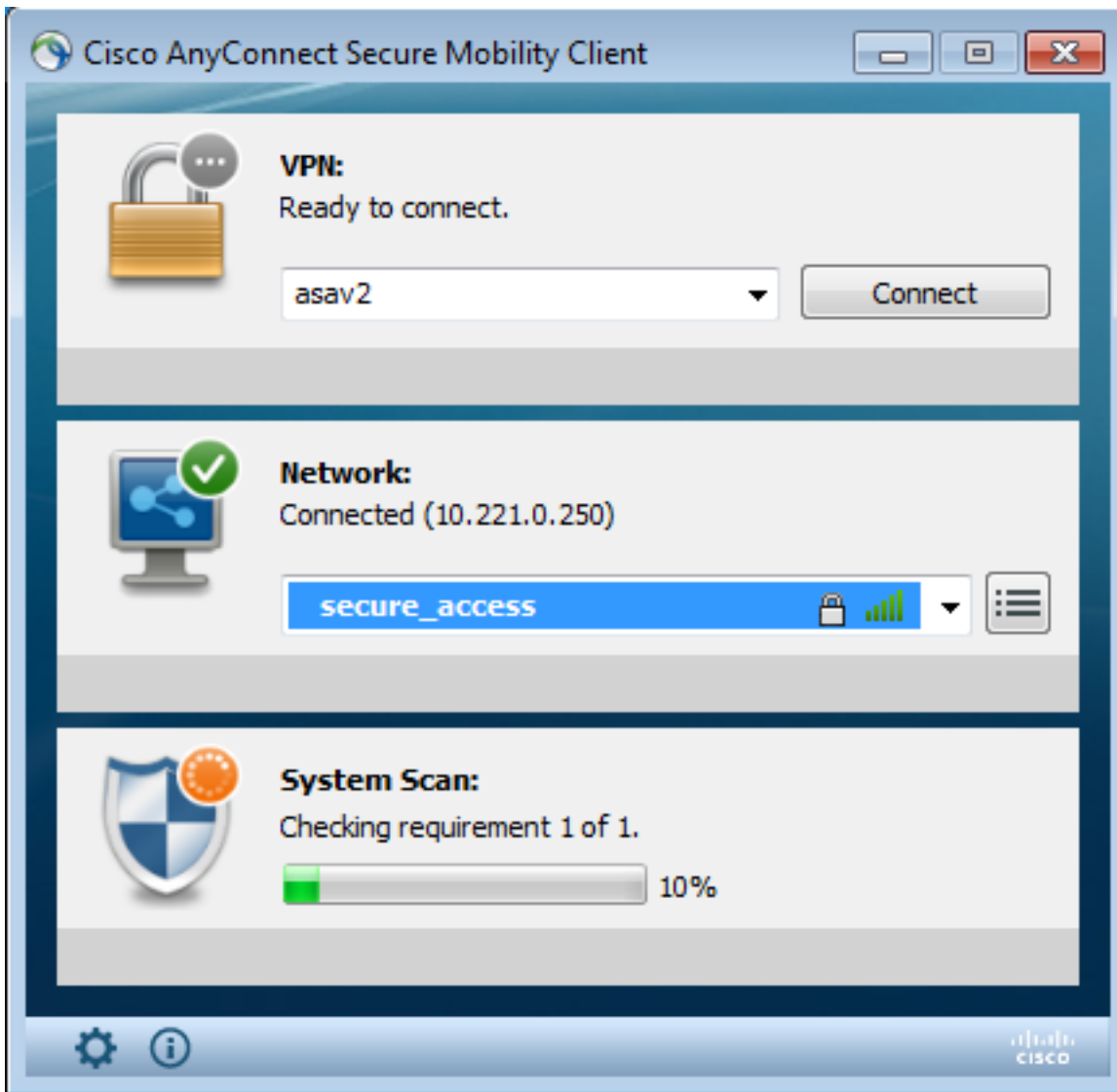
所有模組 (VPN、NAM和狀態) 均已安裝和配置。您必須重新啟動電腦：



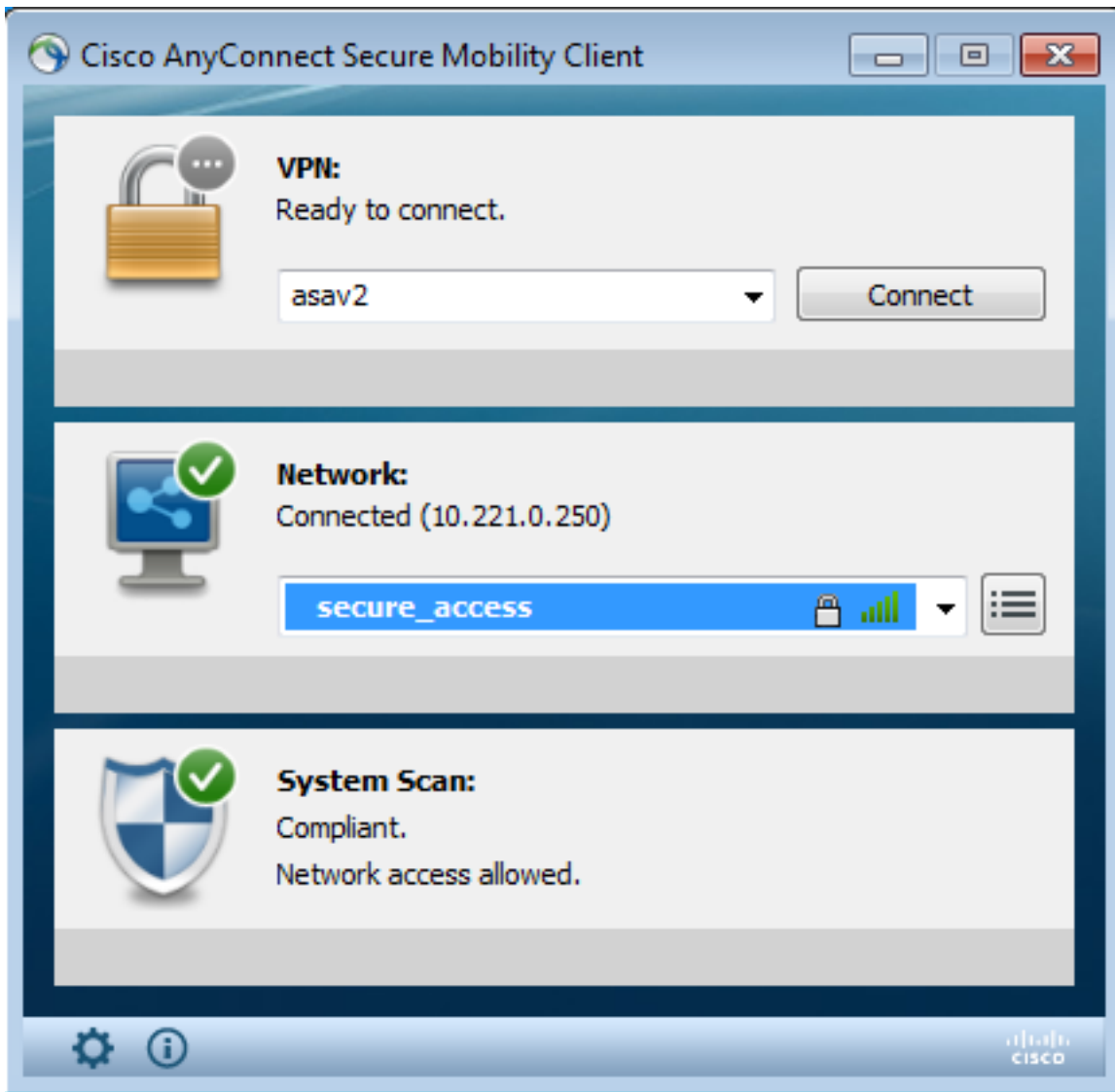
重新啟動後，將自動執行AnyConnect，且NAM會嘗試與secure_access SSID關聯（根據配置的配置檔案）。請注意VPN配置檔案已正確安裝（VPN的asav2條目）：



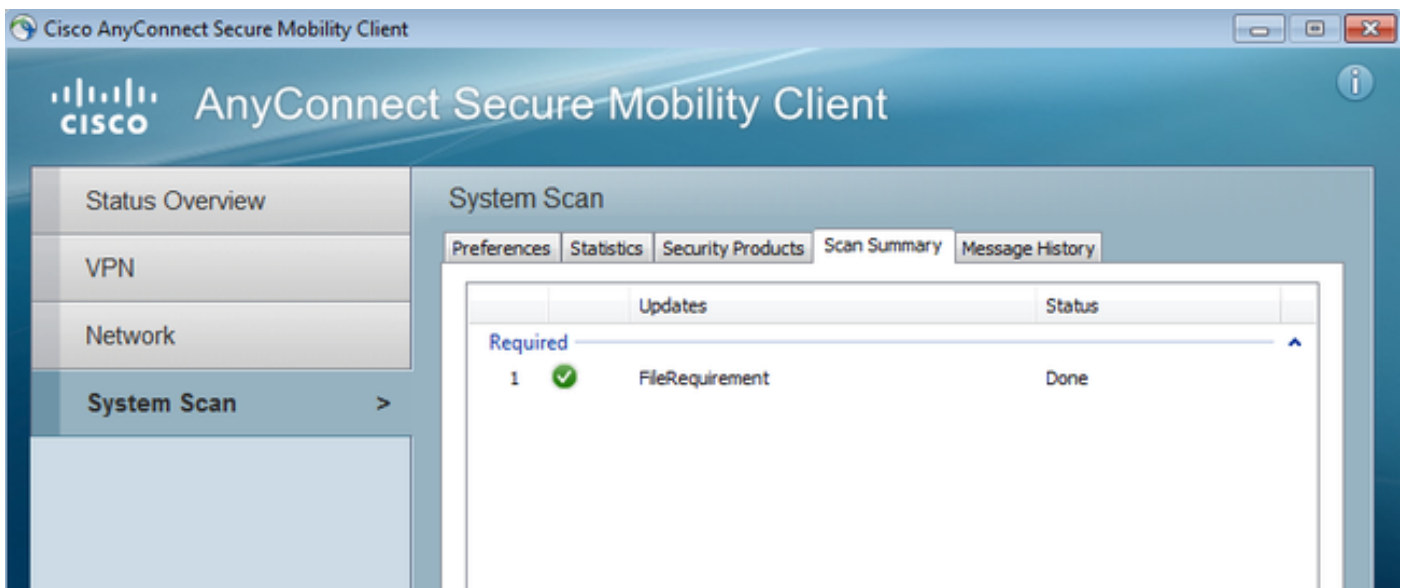
身份驗證後，AnyConnect將下載更新並執行驗證的終端安全評估規則：



在此階段，可能存在有限的訪問許可權（您在ISE上遇到未知授權規則）。一旦站台合規，安全狀態模組將報告此情況：



還可以驗證詳細資訊 (滿足FileRequirement) :



消息歷史記錄顯示詳細步驟 :

```
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.

```

成功的報告傳送到ISE，ISE觸發授權更改。第二個身份驗證遇到Compliant規則，並授予完整網路訪問許可權。如果在仍與調配SSID關聯時傳送終端安全評估報告，則在ISE上看到以下日誌：

| Time | Status | Det... | R... | 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 | Default => Compliant | PermitAccess | WLC1 | 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 | Default => Compliant | PermitAccess | WLC1 | Compliant | ise13 | Dynamic Authorization succeeded |
| 2014-11-16 09:31:35... | 🔴 | | | admin | CB-4A:00:15-6A:DC | Default => Provisioning | GuestProvisioning | WLC1 | Pending | ise13 | Authentication failed |
| 2014-11-16 09:29:34... | 🟢 | | | cisco | CB-4A:00:15-6A:DC | Default => Provisioning | GuestProvisioning | WLC1 | Pending | ise13 | Authentication succeeded |

狀態報告顯示：

| 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:DC | 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:DC | 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:DC | 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:DC | 10.221.0.250 | Windows 7 Ultimate 64-bit | AnyConnect... | Received a posture report from an endpoint |

詳細報告顯示滿足的FileRequirement:

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 | | |

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [思科ISE上的終端安全評估服務配置指南](#)
- [思科ISE 1.3管理員指南](#)
- [技術支援與文件 - Cisco Systems](#)