# 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 <u>步驟1.新增WLC</u> 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

本文中的資訊係根據以下軟體和硬體版本:

- Microsoft Windows 7
- Cisco WLC版本7.6及更高版本
- Cisco ISE軟體1.3版及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

## 拓撲和流



#### 以下是流程:

**步驟1**.企業使用者訪問服務集識別符號(SSID):調配。使用可擴展身份驗證協定保護的EAP(EAP-PEAP)執行802.1x身份驗證。 在ISE上遇到**Provisioning**授權規則,使用者被重定向以進行 AnyConnect調配(通過客戶端調配門戶)。 如果在電腦上未檢測到AnyConnect,則會安裝所有配 置的模組(VPN、NAM、安全狀態)。 與配置檔案一起推送每個模組的配置。

步驟2.安裝AnyConnect後,使用者必須重新啟動PC。重新啟動後,AnyConnect將運行,並且根據 配置的NAM配置檔案(Secure\_access)自動使用正確的SSID。使用EAP-PEAP(例如,還可以使用可 擴展身份驗證協定 — 傳輸層安全(EAP-TLS))。 同時,終端安全評估模組檢查工作站是否合規(檢查 c:\test.txt檔案的存在)。 **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。

AnyConnect Profile Editor - V File Help	PN Server List			
Preferences (Part 1)	Profile: Untitled			
Backup Servers	🔒 Server List Entry			<b>=</b>
- 22 Certificate Enrolment - 22 Mobile Policy	Host Display Name (required) asav2	New Course	Additional mobile-only settings	Edt
	asav2.example.com	/ TAC		
	Cronel Pl			
	asav2.example.com/TAC			
	Backup Server List		Load Balancing Server List "Always On" is disabled. Load Balancing Fields h	ave been disabled.
	Host Address	Add	Host Address	Add
		Move Up		Delete
		Mave Down		
		Dalata		
		Delete		
	Primary Protocol	SSL •	Automatic SCEP Host	
	Standard Authentication Only (IOS gateways)		CA URL	
	Auth Method During IKE Negotiation	IXE-RSA +	Prompt For Challenge Password	
	DE Identity		CA Thumbprint	
		ОК	Cancel	

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。

works       Name:       secure_access       Media         Group Membership <ul> <li>In all groups (Global)</li> <li>Choose Your Network Media</li> <li>Wired (802.3) Network</li> <li>Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.</li> <li>Wir-Fi (wireless) Network</li> <li>Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.</li> <li>SSID (max 32 chars):</li> <li>secure_access</li> <li>Hidden Network</li> <li>Corporate Network</li> <li>Association Timeout (sec)</li> <li>Common Settings</li> </ul> Media	t Policy entication Policy	Networks Profile: Z:\NAM.xml		
twork Groups       In an or oup:       Local networks       Security         In all groups:       Local networks       User /         In all groups (Global)       Choose Your Network Media       Creder         Wired (802.3) Network       Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.       Wir-Fi (wireless) Network         Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.       SSID (max 32 chars):       secure_access         Hidden Network       Hidden Network       Corporate Network       Corporate Network         Association Timeout (sec)       5       Common Settings	orks	Nama		Media Type
In group:       Local networks       Connectsi         In all groups (Global)       In all groups (Global)         Choose Your Network Media       Creder         Wired (802.3) Network       Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.         Wi-Fi (wireless) Network       Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.         SSID (max 32 chars):       secure_access         Hidden Network         Association Timeout (sec)       5         Common Settings	ork Groups	Group Membership	secure_access	Security Leve
<ul> <li>In group:</li></ul>			Less ashunda	Connection Typ
Creder Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): secure_access Hidden Network Association Timeout (sec) S Common Settings		In group:	Local networks	User Auth
Choose Your Network Media  Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): secure_access Hidden Network Corporate Network Association Timeout (sec) 5 Common Settings		<ul> <li>In all groups (Global)</li> </ul>		Credentials
<ul> <li>Wired (802.3) Network</li> <li>Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.</li> <li>Wi-Fi (wireless) Network</li> <li>Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.</li> <li>SSID (max 32 chars): secure_access</li> <li>Hidden Network</li> <li>Corporate Network</li> <li>Association Timeout (sec) 5</li> </ul>		Choose Your Network Media		
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.  Wii-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): SSID (max 32 chars): Hidden Network Hidden Network Association Timeout (sec) S Common Settings		Wired (802.3) Network		
ethernet cable.  Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): secure_access Hidden Network Corporate Network Association Timeout (sec) S Common Settings		Select a wired network if the	e endstations will be connecting to the network with a traditional	
Wi-Fi (wireless) Network     Select a WiFi network if the endstations will be connecting to the network via a wireless     radio connection to an Access Point.     SSID (max 32 chars):         secure_access         Hidden Network         Corporate Network     Association Timeout (sec)     5 Common Settings		ethernet cable.		
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): secure_access Hidden Network Corporate Network Association Timeout (sec) 5 Common Settings		Wi-Fi (wireless) Network		
radio connection to an Access Point. SSID (max 32 chars): secure_access Hidden Network Corporate Network Association Timeout (sec) 5 Common Settings		Select a WIFi network if the	endstations will be connecting to the network via a wireless	
SSID (max 32 chars): secure_access Hidden Network Corporate Network Association Timeout (sec) 5 Common Settings		radio connection to an Acce	ss Point.	
Hidden Network     Corporate Network     Association Timeout (sec) 5 Common Settings		SSID (max 32 chars):	secure_access	
Association Timeout (sec) 5 Common Settings			Hidden Network	
Association Timeout (sec) 5 Common Settings			Corporate Network	
Common Settings		Annaly Transfer Court	E	
Common Settings		Association Timeout (sec)	>	
		Common Settings		
Script or application on each user's machine to run when connected.		Script or application on each user's	machine to run when connected.	
Browse Local Machine			Browse Local Machine	
Connection Timesuit (sec.) 40				
Comection Imedua (sec.) 40		Connection Timeout (one )		

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-4.0.00048k9.pkg**:

Authentication  Authorization Dictionaries Conditions Results	Profiling 🔯 Posture	📓 Client Provisioning 🛛 📓 Trus	tSec 🛛 🙀 Policy Elements		
Results	Agent Resources From Loca Agent Resources Fr Category	I Disk > Agent Resources From Loca om Local Disk [Cisco Frovided Packages ]/mnt/crypt/home/mgarcarz	I Disk •] ⊕ z/Downloads/anyconn	ectBrows	se
Posture     Clent Provisioning		* AnyConnect Uploaded Resources			
1 Hesources		Name .	Туре	Version	Description
• Justine	Submit Cancel	AnyConnectDesktopWindows 4	AnyConnectDesktopWin	4.0.48.0	AnyConnect Secure Mobility

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):

🛃 Authentication 🛛 🛛	JAuthorization	🔀 Profiling	R Posture	Client Provisioning	🚞 TrustSec	Policy Elements	
Dictionaries Conditi	ions Results						
Results	<u>م</u>	Agent Re Agent	sources From Loo Resources Fr Category Type * Name Description	al Disk > Agent Resources ) rom Local Disk Customer Created Packag AnyConnect Profile NAM-Profile	From Local Disk		Browse
		Subm	it Cancel				

3. 對VPN配置檔案重複類似步驟:

🔔 Authentication 🛛 🧔 Authorization	🔀 Profiling 🛛 👩 Posture	🛃 Client Provisioning 🛛 🔂 Tr	rustSec 🙀 Policy Elements	
Dictionaries Conditions Results	)			
Results	Agent Resources From Loc Agent Resources F Category Type *Name Description	al Disk > Agent Resources From Lo rom Local Disk Customer Created Packages AnyConnect Profile VPN-Profile /mnt/crypt/tmp/VPN.xml	rcal Disk	Browse

### 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:

cisco Identity Services Engine		🛕 Home	Operations   🔻	Policy   🔻	Guest Access   🔻	Administration   🔻
🛃 Authentication 🛛 🧔 Authorization	K Profiling	👩 Posture	👸 Client Provis	sioning	📑 TrustSec 🛛 🥅	Policy Elements
Dictionaries Conditions Results						
Posture	File Condi File Cor	tions List > file-on idition Desc + Fi + File * File Op * Operating to Reset	ription file-cond ription le Path ABSOLU le Type FileExist perator Exists System Windows	Ition TE_PATH ence	▼ [C:\test.txt ▼ ▼	

此條件用於需求:

cisco Identity Services Engine	🏠 Home Operatio	ns 💌 Policy 💌 Guest Access	s 💌 Administration 💌	
🛓 Authentication 🛛 🧕 Authorization 🔀	Profiling 💽 Posture 🔂 Clie	nt Provisioning 📑 TrustSec	Policy Elements	
Dictionaries Conditions Results				
Results	Requirements			
٩	Name	Operating Systems	Conditions	Remediation Actions
(□ • E •	51. D	1. INC. 1. INC.		
Authentication	Fliekequirement	107 WINDOWS AIL	metir file-condition	else Message Text Only
Profiling	Any_AV_Installation_Win	for Windows All	metif ANY_av_win_inst	else Message Text Only
▼ Posture ▶ amediatian Actiona	Any_A/_Definition_Win	for Windows All	metif ANY_av_win_def	else Any#vDefRemediationWi n
E Requirements	Any_AS_Installation_Win	for Windows All	metif ANY_as_win_inst	else Message Text Only
<ul> <li>TrustSec</li> </ul>	Any_AS_Definition_Win	for Windows All	metif ANY_as_win_def	else AnyASDerRemediationWi n
	Any_A/_Installation_Mac	for Mat OSX	metif ANY_av_mac_inst	else Message Text Only
	Any_A/_Definition_Mac	for Mac OSX.	metif ANY_av_mac_def	else Any#VDefRemediationMa c
	Any_AS_installation_Mac	for Mac OSX	metif ANY_as_mac_inst	else Message Text Only
:	Any_AS_Definition_Mac	for Mac OSX	metif ANY_as_mac_def	else AnyASDefRemediationMa c

## 此要求用於Microsoft Windows系統的終端安全評估策略:

cisco Identity Ser	vices Engine		🏠 Home	Operations   •	Policy   •	Guest Access	Administration		
🛓 Authentication	<ul> <li>Authorization</li> </ul>	🔀 Profiling	😿 Posture	🛐 Client Provi	sioning	🚞 TrustSec	🐥 Policy Elements		
Posture Policy Define the Posture Policy k	y configuring rules base	d on operating sy	stem and/or other c	onditions.					
÷									
Status Rule Na	me	Ide	entity Groups	Operating S	ystems	Other Cond	itions		Requirements
<table-cell> File</table-cell>		If Any		and Windows A	I			then	FileRequirement

有關終端安全評估配置的詳細資訊,請參閱<u>思科ISE配置指南上的終端安全評估服務</u>。

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):

ዿ Authentication	👩 Auth	orization	K	Profiling	💽 Posture	🔊 Cliei	nt Provisioning
Dictionaries	Conditions	Results					
Results				ISE Posture	Agent Profile S	settings > N	ew Profile
		<b>م</b> نة	)	Posture Age	ent Profile Settin	ngs	
Authentication	n	10 C		* Name:	ISEPosture		]
Authorization				Description:			
🕨 🚞 Profiling							
Posture							
🔻 🚞 Client Provisi	oning			Agent Beha	vior		
E Resources							

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	120 secs	
Discovery host		
* Server name rules	4	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。

Authentication Suthorization	Reprofiling Resture Client Provision	oning 📄 TrustSec 💦 Policy Elements
Dictionaries Conditions Results		
Results	AnyConnect Configuration > AnyConnect Con	nfiguration
Authentication  Authorization	* Select AnyConnect Package:	AnyConnectDesktopWindows 4.0.48.0 *
Profiling     Posture	* Configuration Name:	AnyConnect Configuration
Client Provisioning     E Resources	Description:	
<ul> <li>TrustSec</li> </ul>	Description	Value
	* Compliance Module	AnyConnectComplianceModuleWindows 3.6.: *
	AnyConnect Module Selection	
	ISE Posture	×
	VPN	
	Network Access Manager	
	Web Security	
	ASA Posture	
	Start Before Logon	
	Diagnostic and Reporting Tool	
	Profile Selection	
	* ISE Posture	ISEPosture *
	VPN	VPN-Profile *
	Network Access Manager	NAM-Profile *
	Web Security	T
	Customer Feedback	

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:

ntity Services Engine		A Home	Operations   •	Policy	Guest Access	Administration	
ation 💿 Authorization	🛃 Profiling	Posture	Client Pro	wisioning	📺 TrustSec	🐥 Policy Elements	
isioning Policy							
t Provisioning Policy to determin puration: version of agent, agent	e what users wi profile, agent co	Il receive upon login a mpliance module, and	nd user session in Vor agent customic	itiation: zation packag	θ.		
icant Configuration: wizard profi	ie andror wizard.	. Drag and drop rules t	o change the orde	r.			
Rule Name	Identity C	Groups Ope	ating Systems	01	her Conditions		Results
AnyconnectViin	If Any	and Wind	iows All	and Co	ndition(s)	then	AnyConnect Configuration
	ntity Services Engine ation  Authorization isioning Policy t Provisioning Policy to determin juration: version of agent, agent licant Configuration: wizard profi Rule Name AnyconnectMin	ntity Services Engine ation  Authorization  Profiling isioning Policy t Provisioning Policy to determine what users wi puration: version of agent, agent profile, agent co licant Configuration: wizard profile and/or wizard Rule Name Identity C AnyconnectWin If Any	Itity Services Engine       Itome         ation       Authorization       Profiling       Posture         isioning Policy       Itomage of agent, agent profile, agent compliance module, and licant Configuration: wizard profile and/or wizard. Drag and drop rules to Rule Name       Identity Groups       Open         AnyconnectWin       If       Any       and       Wind	Initity Services Engine       Image: None       Operations         ation       Authorization       Profiling       Posture       Client Profiling         isioning Policy         t Provisioning Policy to determine what users will receive upon login and user session in juration: version of agent, agent profile, agent compliance module, and/or agent customit licent Configuration: wizard profile and/or wizard. Drag and drop rules to change the order         Rule Name       Identity Groups       Operating Systems         AnyconnectMin       If       Any       and	Inity Services Engine       Image: None Operations in Policy in Po	Initive Services Engine       Image: None Operations I + Policy I + Guest Access         ation       Authorization       Profiling       Posture       Client Provisioning       TrustSec         isioning Policy       It is a point of agent, agent profile, agent compliance module, and/or agent customization package, licant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.       It is and/or agent systems       Other Conditions         Rule Name       Identity Groups       Operating Systems       Other Conditions         AnyconnectWin       If Any       and Windows All       and Condition(s)	Initity Services Engine       Image: Notice of the service of the servi

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:

cisco Identity Services Engine	🟠 Home	Operations    Policy	Guest Access   •	Administration   •	
🛃 Authentication 🛛 👩 Authorization 🔀 Profiling	👩 Posture	👸 Client Provisioning	📄 TrustSec 🛛 🗧	Policy Elements	
Dictionaries Conditions Results					
Results Autho Autho	rization Profiles > Gu orization Profile *Name Guest Description Access Type Access Ice Template	restProvisioning Provisioning S_ACCEPT *			
Imited Access     ✓ C       Imited Access     ✓ C       Imited Access     ✓ V       Imited Access     ✓ V       Imited Access     ✓ Imited Access       Imited Access <td>ommon Tasks Veb Redirection (CWA, Client Provisioning (P)</td> <td>MDM, NSP, CPP) osture) 💌 ACL GuestRedir</td> <td>ect</td> <td>Value Client Provisionin</td> <td>ıg Portal +</td>	ommon Tasks Veb Redirection (CWA, Client Provisioning (P)	MDM, NSP, CPP) osture) 💌 ACL GuestRedir	ect	Value Client Provisionin	ıg Portal +

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<u>使用交換機和身分識別服務引擎的中央Web驗證組態範例</u>。

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 Id	entity Services Engine		🟠 Home	Operations   •	Policy   🔻	Guest Access	▼ Ad	Iministration   •
🔔 Authenti	cation 💽 Authorization	🔀 Profiling	💽 Posture	闝 Client Provis	sioning	💼 TrustSec	🐥 Poi	licy Elements
Authorizat	ion Policy							
Define the Auth For Policy Expo	orization Policy by configuring ru rt go to Administration > Sys	iles based on identif tem > Backup &	y groups and/or othe Restore > Policy E	r conditions. Drag a xport Page	and drop rule:	s to change the orde	er.	
First Matche	d Rule Applies 👻							
▶ Exception	is (0)							
Standard								
Status	Rule Name	c	onditions (identity gr	oups and other con	ditions)			Permissions
	Compliant	if (F Se	adius:Called-Station	-ID CONTAINS sec EQUALS Complia	ure_access / nt)	ND	then	PermitAccess
	NonCompliant	if (R Se	adius:Called-Station	-ID CONTAINS sec EQUALS NonCorr	ure_access / pliant)	ND	then	LimitedAccess
	Unknown	if (R Se	adius:Called-Station	-ID CONTAINS sec EQUALS Unknows	ure_access /	ND	then	GuestProvisioning
	Provisioning	if (R Se	adius:Called-Station	-ID CONTAINS prov EQUALS Unknown	risioning AND n )		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 🔻	Several Security Check +
← A https:/	/ise13.example.com:8443/portal/PortalSetup.action?portal=19f9d160-5e4e-11e4-b905-005056bf2f0a&sessionId=0a3e478500000. 🖧 🛡 C
	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



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。



## 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):

Cisco AnyConne	ct   secure_access	S Cisco AnyConnect Secure Mobility Client
Please enter Username: Password:	r your username and password for the network: secure_access	VPII: Verify your network connection. asav2 Connect
	Show Password	No Network Connectivity
	OK Cancel	Network: Authenticating secure_access
		System Scan: Limited or no connectivity.

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:

🕥 Cisco AnyCo	nnect Secure Mobility Client	- • •
	VPN: Ready to connect. asav2	▼ Connect
	Network: Connected (10.221.0.250) secure_access	iii - Iiii
	System Scan: Checking requirement 1 of 1.	
<b>\$</b> (i)		ajiajia cisco

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:

🕥 Cisco AnyCo	nnect Secure Mobility Client	
	VPN: Ready to connect. asav2	Connect
	Network: Connected (10.221.0.250) secure_access	- 111 -
	System Scan: Compliant. Network access allowed.	
<b>\$</b> (i)		altalta cisco

## 還可以驗證詳細資訊(滿足FileRequirement):

0	Cisco AnyConnect Secure Mobility Client							•	×
	cisco AnyConnec	ct	Secu	re Mo	obility Cl	ient			1
	Status Overview		System S	can					
	VPN	1	Preferences	Statistics	Security Products	Scan Summary	Message History	_	
	Network		Require	U; d	pdates		Status		
	System Scan >		1 (	9 Fi	leRequirement		Done		
			1						

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:

aliada cisco	Identity Ser	vices Engine			A Home 0	perations   • Policy   •	OuestAccess + Ad	ministration   •		Lower We	need a 1 mans 1 agent 1 Codont 1
0.4.1	hantications	E Reports	ie,	Endpoint Prot	ection Service 🛛 🍾	Troubleshoot					
Misconfigured Supplicants (2) Misconfigured Network Devices (2)							RADIUS Drops (2) Client Stopped Responding (2)			ed Responding @	
					· ·						-
G Shee	A Live Sessions	🙀 Add or I	lemove C	olumna 💌 🤣	Refresh 😨 Reset Rej	peat Counts				Refresh Ever	y1 minute * Show Latest 20 r
Time		Status Al • Del	t R	identity 2	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Posture Status	Server ®	Event ®
2014-11	-16 09:32:07.		0 0	cisco	C0:44.00:15:6A.DC				Compliant	ise13	Session Rate is Raited
2014-11	-16 09:32:07.	- 🖬 🔡	ò	cisco	C0:44.00:15:64.DC	Default >> Compliant	PermitAccess	WLC1	Compliant	isel3	Authentication succeeded
2014-11	-16 09:32:07.	. 🖬 👘	ò		C0:44.00:15:6A.DC			WLC1	Compliant	ise13	Dynamic Authorization succeeded
2014-11	-16 09:31:35.	. 0	ò	admin	C0:44.00:15:64.DC			WLC1		ise13	Authentication failed
2014-11	16 09:29:34.	. 🖬 👘	ò	cisco	C0:44:00:15:64:DC	Default >> Provisioning	GuestProvisioning	WLC1	Pending	ise13	Authentication succeeded

### 狀態報告顯示:

abab							Louise Marsing	A 1997 1	aleas y Legent y Poellack D
CISCO Identity Services Engine	🏠 Home	Operation	s i • Polo	· · · · · ·	cess I . Administratio	• [ •			Seta
Authentications Reports 20	ndpoint Protection Service	Trutte	host						
Report Selector	Posture Detail Assess	nent							🙀 Favorite 🛛 🙆 Export
Favorites									Generated at 2014
ISE Reports	From 11/16/2014 12:00:00 A	M1o 11/16/20	14 09:27:56 AB	4					Fage of 3 to Resolution
<ul> <li>Auth Services Status</li> </ul>	Logged At 5	itatus Def	al PRA	identity	Endpoint ID	P Address	Endpoint OS	Agent	Message
Braparta	2014-11-16 09:23-25.8	2	NA	cisco	C0:44:00:15:64:D	10.221.0.250	Windows 7 Utsmate 64-64	AnyConnect	Received a posture report from an endpoint
<ul> <li>Deployment Status</li> <li>12 reports</li> </ul>	2014-11-16 09-18-42-2	<b>2</b>	NA	cisco	C0.44.00 15.64.0	10.221.0.250	Windows 7 Ultimate 64-64	AnyConnect	Received a posture report from an endpoint
v Endpoints and Users	2014-11-16-09-16-59-6		NA	cisco	C0:44.00 15:64.0	10.221.0.250	Windows 7 Ultimate 64-64	AnyConnect	Received a posture report from an endpoint
Client Provisioning	2014-11-16 09:15:17.4		NA	disco	C0-44-00-15-64-D	10.221.0.250	Windows 7 Utimate 64-bit	AnyConnect	Received a posture report from an endpoint
Current Active Sessions									
Endpoint Protection Service Audit									
External Mobile Device Management									
Posture Detail Assessment VP Piters -									

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:	0a3e4785	000002a354685ee	e2			
Client Operating Syste	m: Windows 7	7 Ultimate 64-bit				
Client NAC Agent:	AnyConne	ct Posture Agent fo	r Window	s 4.0.00048		
PRA Enforcement:	0					
CoA:	Received a	a posture report fro	m an end	point		
PRA Grace Time:	0					
PRA Interval:	0					
PRA Action:	N/A					
User Agreement Statu	s: NotEnable	d				
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:	2014-11-1	6 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
- <u>思科ISE 1.3管理員指南</u>
- 技術支援與文件 Cisco Systems