# Intégration d'AnyConnect 4.0 avec l'exemple de configuration de version 1.3 ISE

## Contenu

Introduction Conditions préalables Conditions requises Composants utilisés Topologie et écoulement Configurer WLC ISE Étape 1. Ajoutez le WLC Étape 2. Configurez le profil VPN Étape 3. Configurez le profil NAM Étape 4. Installez l'application Étape 5. Installez le profil VPN/NAM Étape 6. Configurez la posture Étape 7. Configurez AnyConnect Étape 8. Règles de ravitaillement de client Étape 9. Profils d'autorisation Étape 10. Règles d'autorisation Vérifier Dépanner Informations connexes

## Introduction

Ce document décrit la nouvelle fonctionnalité dans la version 1.3 du Logiciel Cisco Identity Services Engine (ISE) qui te permet pour configurer plusieurs modules sécurisés de client de mobilité d'AnyConnect et pour provision les automatiquement au point final. Ce document présente comment configurer des modules VPN, de gestionnaire d'accès au réseau (NAM), et de posture sur ISE et les pousser à l'utilisateur en entreprise.

# Conditions préalables

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiements, authentification, et autorisation ISE
- Configuration des contrôleurs LAN Sans fil (WLCs)
- La connaissance de base VPN et de 802.1x

• La configuration des profils VPN et NAM avec AnyConnect profilent des éditeurs

#### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Version 7.6 et ultérieures de Cisco WLC
- Logiciel de Cisco ISE, versions 1.3 et ultérieures

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurezvous que vous comprenez l'effet potentiel de toute commande.

## Topologie et écoulement



Voici l'écoulement :

Étape 1. Identifiant SSID (Service Set Identifier) d'acceses d'utilisateur en entreprise :

Ravitaillement. Exécute l'authentification de 802.1x avec l'EAP Protocol-protégé par authentification extensible (EAP-PEAP). La règle d'autorisation de **ravitaillement** est produite sur ISE et l'utilisateur est réorienté pour le ravitaillement d'AnyConnect (par l'intermédiaire du ravitaillement de client Protal). Si AnyConnect n'est pas détecté sur l'ordinateur, tous les modules configurés sont installés (VPN, NAM, posture). Avec ce profil, la configuration pour chaque module est poussée.

Étape 2. Une fois qu'AnyConnect est installé, l'utilisateur doit redémarrer le PC. Après que la réinitialisation, AnyConnect fonctionne et le SSID correct est automatiquement utilisé selon le profil configuré NAM (Secure\_access). EAP-PEAP est utilisé (comme exemple, le Protocol-transport Layer Security (EAP-TLS) d'authentification extensible pourrait être également utilisé). En même temps, le module de posture vérifie si la station est conforme (vérifie l'existence du fichier de c:\test.txt).

**Étape 3.** Si l'état de posture de station est inconnu (aucun état de module de posture), il est encore réorienté pour le ravitaillement, parce que la règle d'Authz d'**inconnu** est produite sur ISE. Une fois que la station est conforme, ISE envoie une modification de l'autorisation (CoA) au contrôleur LAN Sans fil, qui déclenche la ré-authentification. Une deuxième authentification se produit, et la règle **conforme** est frappée sur ISE, qui fournira à l'utilisateur l'accès complet au réseau.

En conséquence, l'utilisateur provisioned avec AnyConnect VPN, NAM, et modules de posture qui tiennent compte de l'accès unifié au réseau. La fonctionnalité semblable peut être utilisée sur l'appliance de sécurité adaptable (ASA) pour l'accès VPN. Actuellement, ISE peut faire la même chose pour n'importe quel type d'accès avec une approche très granulaire.

Cette fonctionnalité n'est pas limitée aux utilisateurs en entreprise, mais elle est probablement la plus commune pour la déployer pour ce groupe d'utilisateurs.

## Configurer

## WLC

Le WLC est configuré avec deux SSID :

- Ravitaillement [WPA + WPA2][Auth(802.1X)]. Ce SSID est utilisé pour le ravitaillement d'AnyConnect.
- Secure\_access [WPA + WPA2][Auth(802.1X)]. Ce SSID est utilisé pour l'accès sécurisé après que le point final provisioned avec le module NAM qui est configuré pour ce SSID.

#### ISE

#### Étape 1. Ajoutez le WLC

Ajoutez le WLC aux périphériques de réseau sur ISE.

#### Étape 2. Configurez le profil VPN

Configurez le profil VPN avec l'éditeur de profil d'AnyConnect pour le VPN.

AnyConnect Profile Editor - V File Help VPN Preferences (Part 1) Preferences (Part 1)	PN Server List Profile: Untitled			
Certificate Envolvent	Host Display Name (required) asav2 FQDN or IP Address asav2.example.com Group URI. asav2.example.com/TAC	User Group / TAC	Additional mobile-only settings	Edt
	Backup Server List Host Address	Add Move Up Move Down Delete	Load Balancing Server List "Always On" is disabled. Load Balancing Fields Host Address	have been disabled. Add Delete
	Primary Protocol Standard Authentication Only (ICS gateways) Auth Method During IXE Negotiation DRE Identity	SSL • DE-RSA •	Automatic SCEP Host CA URL Prompt For Challenge Password CA Thumbprint	

Seulement une entrée a été ajoutée pour l'accès VPN. Sauf que fichier XML à VPN.xml.

#### Étape 3. Configurez le profil NAM

Configurez le profil NAM avec l'éditeur de profil d'AnyConnect pour NAM.

S Name:		
- Nama-		Media Ty
Groups Group Membership	secure_access	Security L
droup Hendership	la de la della d	Connection
In group:	Local networks	User Au
<ul> <li>In all groups (Global)</li> </ul>	)	Credenti
Choose Your Network Medi	a	
Wired (802.3) Netwo	ark	
Select a wired netwo	ork if the endstations will be connecting to the network with a traditional	
ethernet cable.		
Wi-Fi (wireless) Netv	vork	
Select a W/Fi networ	k if the endstations will be connecting to the network via a wireless	
radio connection to a	an Access Point.	
SSID (max 32 chars)		
	Secure_access	
	Hidden Network	
	Corporate Network	
Association Timeout	(sec) 5	
Common Settings		
Script or application on eac	h user's machine to run when connected.	
	Browse Local Machine	
Connection Timeout (sec.)	40	

Seulement un SSID a été configuré : secure\_access. Sauf que fichier XML à NAM.xml.

#### Étape 4. Installez l'application

1. Téléchargez l'application manuellement de Cisco.com.

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

- 2. Sur ISE, naviguez vers la **stratégie > les résultats > le ravitaillement > les ressources de client**, et ajoutez les ressources en agent à partir du disque local.
- 3. Choisissez Cisco a fourni des modules et sélectionne l'anyconnect-win-4.0.00048-k9.pkg :

Authentication Authorization . Dictionaries Conditions Results	🖌 Profiling 🛛 🕅 Posture	🗒 Client Provisioning 👔	TrustSec	Policy Elements		
Results	Agent Resources From Loca Agent Resources Fr Category	al Disk > Agent Resources From rom Local Disk [Cisco Provided Packages [/mnt/crypt/home/mga	• Local Disk • @ rcarz/Dov	vnloads/anyconn	ect-Brow	/\$0,
Posture     Cilent Provisioning		+ AnyConnect Uploaded Res	ources			
E Resources		Name	▲ Type	2	Version	Description
	Submit Cancel	AnyConnectDesktopWindown	84 Angv	ConnectDesktopWin	4.0.48.0	AnyConnect Secure Mobility

4. Répétez l'étape 4 pour le module de conformité.

#### Étape 5. Installez le profil VPN/NAM

- 1. Naviguez vers la **stratégie > les résultats > le ravitaillement > les ressources de client**, et ajoutez les ressources en agent à partir du disque local.
- 2. Choisissez les modules et le **profil d'AnyConnect** créés par client de type. Sélectionnez le profil précédemment créé NAM (fichier XML) :

Authentication Dictionaries Co	<ul> <li>Authorization</li> <li>nditions</li> <li>Results</li> </ul>	Rrofiling	💽 Posture	👸 Client Provisioning	🚞 TrustSec	Policy Elements	)
Results	Ę	Agent Re Agent 1	sources From Loc Resources Fi	al Disk > Agent Resources I rom Local Disk	From Local Disk		
Authentication		2-	Category	Customer Created Packag	ges 🔻 🕖		
Authorization     Profiling     Desture			Type * Name	AnyConnect Profile	•		
Client Provisionin     Elesources     TrustSec	g		Description				
				/mnt/crypt/tmp/NA	.M.xml		Browse
		Submi	t Cancel				

3. Étapes semblables de répétition pour le profil VPN :

🔝 Authentication 🛛 🧕	Authorization	🔀 Profiling	🧑 Posture	👸 Client Provisioning	📄 TrustSec	🐴 Policy Elements	
Dictionaries Condition	s Results						
Results	<b>م</b> ٢	Agent Re Agent	sources From Loco Resources Fr Category Type * Name Description	al Disk > Agent Resources rom Local Disk Customer Created Packa AnyConnect Profile VPN-Profile /mnt/crypt/tmp/VP	From Local Disk ges • ① • • ?N.xml		Browse
		Subm	it Cancel				

#### Étape 6. Configurez la posture

Des profils NAM et VPN doivent être configurés extérieurement avec l'éditeur de profil d'AnyConnect et être importés dans ISE. Mais la posture est saturée sur ISE.

Naviguez vers la **stratégie > les conditions > la posture > le fichier Condition.You** peut voir qu'un état simple pour l'existence de fichier a été créé. Vous devez avoir ce fichier afin d'être conforme avec la stratégie vérifiée par le module de posture :

cisco Identity Services Engine	🏠 Home	Operations   🔻	Policy   🔻	Guest Access   🔻	Administration   🔻
Authentication O Authorization Profile Dictionaries Conditions Results	ng 🧑 Posture	🙀 Client Provi	sioning	📑 TrustSec 🧧	n Policy Elements
Posture  Posture  File  File File	Conditions List > file- e Condition Des * F * F * File C * Operating tve Reset	* Name file-cond cription	dition JTE_PATH tence s All $\diamondsuit$	¥ [C:\test.txt ¥	

Cette condition est utilisée pour une condition requise :

cisco Identity Services Engine	🏠 Home Operatio	ns 💌 Policy 💌 Guest Access	s 💌 Administration 💌	
🛓 Authentication 🛛 👩 Authorization 🦂	Profiling 📴 Posture 🔂 Clie	ent Provisioning 📑 TrustSec	Policy Elements	
Dictionaries Conditions Results				
Results	Requirements			
٩	Name	Operating Systems	Conditions	Remediation Actions
🗇 🕈 🖽 🕈 🛛 💮 🗸				
Aathentication	FileRequirement	for Windows All	met if file-condition	else Message Text Only
Authorization   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#/DefRemediation/MI In
E Requirements  Client Provisioning	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 AnyASDefRemediation/Ni n
	Any_AV_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	eise AnyASDerRemediationMa c

Et la condition requise est utilisée dans la stratégie de posture pour des systèmes de Microsoft Windows :

cisco Identity Ser	vices Engine		🟠 Home	Operations   •	Policy   🔻	Guest Access	Administration	,	
🛓 Authentication	Authorization	🛃 Profiling 📒	🐼 Posture	🗟 Client Provis	sioning	🚞 TrustSec	🐴 Policy Elements		
Posture Policy Define the Posture Policy b	y configuring rules bas	ed on operating syste	m and/or other (	conditions.					
÷									
Status Rule Na	me	Identi	ty Groups	Operating S	ystems	Other Condi	tions		Requirements
🖌 File		II Any		and Windows Al	1			then	FileRequirement

Pour plus d'informations sur la configuration de posture, référez-vous aux <u>services de posture sur</u> le guide de configuration de Cisco ISE.

Une fois que la stratégie de posture est prête, il est temps d'ajouter la configuration d'agent intermédiaire.

- Naviguez vers la stratégie > les résultats > le ravitaillement > les ressources de client et ajoutez le profil de posture d'agent de Contrôle d'admission au réseau (NAC) ou d'agent d'AnyConnect.
- 2. AnyConnect choisi (un nouveau module de posture de version 1.3 ISE a été utilisé au lieu du vieil agent NAC) :

ዿ Authentication	👩 Auth	orization	3	Profiling	💽 Posture	凤 Clier	t Provisioning
Dictionaries	Conditions	Results					
Results				ISE Posture	Agent Profile S	ettings > Ne	w Profile
		<b>م</b> ن	)	Posture Ag	ent Profile Settin	ngs	
Authentication	n	10.00		* Name:	ISEPosture		
Authorization				Description	:		
<ul> <li>Profiling</li> <li>Posture</li> </ul>							
🔻 🚞 Client Provisi	ioning			Agent Beha	avior		
E Resources							

3. De la section Protocole de posture, n'oubliez pas d'ajouter \* afin de permettre à l'agent pour se connecter à tous les serveurs.

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. Si le champ de règles de nom du serveur est parti vide, ISE ne sauvegarde pas des configurations et signale cette erreur :

Server name rules: valid value is required

#### Étape 7. Configurez AnyConnect

Àce stade, toutes les applications (AnyConnect) et la configuration de profil pour tous les modules (VPN, NAM, et posture) ont été configurées. Il est temps de le lier ensemble.

- 1. Naviguez vers la **stratégie > les résultats > le ravitaillement > les ressources de client**, et ajoutez la configuration d'AnyConnect.
- 2. Configurez le nom et sélectionnez le module de conformité et tous modules requis d'AnyConnect (VPN, NAM, et posture).
- 3. Dans la sélection de profil, choisissez le profil configuré plus tôt pour chaque module.

🛃 Authentication 🛛 👩 Authorization	Rofiling 🐼 Posture 🔂 Client Provisi	oning 📄 TrustSec 👘 Policy Elements
Dictionaries Conditions Results		
Results	AnyConnect Configuration > AnyConnect Co	nfiguration
Authentication	<ul> <li>* Select AnyConnect Package:</li> </ul>	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	
	Customer Feedback	· · · · · · · · · · · · · · · · · · ·

4. Il est obligatoire pour que tous autres modules fonctionnent le module VPN corrrectly. Même si le module VPN n'est pas sélectionné pour l'installation, il sera poussé et installé sur le client. Si vous ne voulez pas utiliser le VPN, il y a une possibilité pour configurer un profil spécial pour le VPN qui masque l'interface utilisateur pour le module VPN. Ces lignes devraient être ajoutées au **fichier VPN.xml**:

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

5. Ce genre de profil est également installé quand vous utilisez Setup.exe du module ISO (anyconnect-win-3.1.06073-pre-deploy-k9.iso). Puis, le profil VPNDisable\_ServiceProfile.xml pour le VPN est installé avec la configuration, qui désactive l'interface utilisateur pour le module VPN.

#### Étape 8. Règles de ravitaillement de client

La configuration d'AnyConnect créée dans l'étape 7 devrait être mise en référence dans les règles de ravitaillement de client :

lu Identity Co	mileos Engino					_		
o Identity Se	rvices Engine		🟠 Home	Operations   •	Policy 🔻	Guest Access	Administration	
Authentication	Authorization	🔀 Profiling	💽 Posture	🕞 Client Pro	visioning	🚊 TrustSec	🐥 Policy Elements	
t Provisionin	g Policy							
he Client Provision	ning Policy to determine	what users will r	eceive upon login :	and user session in	itiation:			
nt Configuration: v ive Supplicant Cor	ersion of agent, agent profile figuration: wizard profile	e and/or wizard. D	pliance module, ar rag and drop rules	d/or agent customiz to change the order	tation package. T			
Rule N	ame	Identity Gro	ups Op	erating Systems	Othe	er Conditions		Results
-				da		(Wa - 7-)		1
Anyconne	civan	IT Any	and var	dows All	and Con	ation(s)	then	Configuration
	Identity Se     Withentication     t Provisionin     the Client Provision     mt Configuration: v     ive Supplicant Cor     Rule N     Rule N     Anyconne	Identity Services Engine     Withentication     O Authorization     Provisioning Policy     the Client Provisioning Policy to determine     nf Configuration: version of agent, agent p     we Supplicant Configuration: wizard profile     Rule Name     AnyconnectWin	Identity Services Engine     withentication     Authorization     Authorization     Profiling     t Provisioning Policy     he Client Provisioning Policy to determine what users will r nt Configuration: version of agent, agent profile, agent com     result Configuration: wizard profile and/or wizard. D     Rule Name     Identity Gro     AnyconnectWin     If Any	Identity Services Engine       Image: Description of Authorization         Authorization       Authorization         Provisioning Policy         the Client Provisioning Policy to determine what users will receive upon login and Configuration: version of agent, agent profile, agent compliance module, and we Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules         Rule Name       Identity Groups       Ope         AnyconnectWin       If Any       and Win	Identity Services Engine       Image: Authorization       Image: Home       Operations       Image: Client Provisioning Policy         In Configuration: Version of agent, agent profile, agent compliance module, and/or agent customic ive Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order         Rule Name       Identity Groups       Operating Systems         Image: AnyconnectWin       If       Any       and Windows All	Identity Services Engine       Image: None Operations in Policy in the operation of the operation opera	Identity Services Engine       Image: Notice Provision in the provision of agent, agent profile, agent compliance module, and/or agent customization package, we supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.       Other Conditions         Rule Name       Identity Groups       Operating Systems       Other Conditions         Image: AnyconnectWin       If Any and Windows All and Condition(s)	Identity Services Engine       Image: Nome       Operations       Policy       Guest Access       Administration         withentication       Image: Authorization       Image: Profiling       Posture       Image: Client Provisioning       TrustSec       Policy Elements         t Provisioning Policy       Home       Operations       Image: Client Provisioning       Image: TrustSec       Policy Elements         t Provisioning Policy       Home       Operating and user session initiation: Inf Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. Ive Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.         Rule Name       Identity Groups       Operating Systems       Other Conditions         Rule Name       Identity Groups       Operating Systems       Other Conditions         and Condition(s)       If Any       and Windows All       and Condition(s)       then

Les règles de ravitaillement de client décident quelle application sera poussée au client. Seulement une règle est nécessaire ici avec le résultat qui indique la configuration créée dans l'étape 7. De cette façon, tous les points finaux de Microsoft Windows qui sont réorientés pour le ravitaillement de client utilisera la configuration d'AnyConnect avec tous les modules et profils.

#### Étape 9. Profils d'autorisation

Le profil d'autorisation pour le ravitaillement de client doit être créé. Le portail par défaut de ravitaillement de client est utilisé :

cisco Identity Services Engine	🏠 Home	Operations    Policy	Guest Access   🔻	Administration   •
🛃 Authentication 🛛 🧔 Authorization	Profiling 🔯 Posture	Client Provisioning	📑 TrustSec 🛛 🔤	Policy Elements
Dictionaries Conditions Results				
Results	Authorization Profiles > Gu Authorization Profile *Name Guestf Description *Access Type ACCESS Service Template	estProvisioning Provisioning S_ACCEPT  *		
Social Formulary	Common Tasks     Web Redirection (CWA.)	MDM, NSP, CPP)		
PermitAccess     Downloadable ACLs     Downloadable ACLs	Client Provisioning (Po	sture) 🔻 ACL GuestRedi	rect	Value Client Provisioning Portal +

Ce profil force les utilisateurs à réorienter pour le ravitaillement au portail par défaut de ravitaillement de client. Ce portail évalue la stratégie de Provisiong de client (règles créées dans étape 8). Les profils d'autorisation sont les résultats des règles d'autorisation configurées dans l'étape 10.

La liste de contrôle d'accès de GuestRedirect (ACL) est le nom de l'ACL défini sur le WLC. Cet ACL décide ce que le trafic devrait être réorienté à ISE. Le pour en savoir plus, se rapportent à l'authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine.

Il y a également un autre profil d'autorisation qui fournit l'accès au réseau limité (DACL) pour les utilisateurs non-conformes (appelés LimitedAccess).

#### Étape 10. Règles d'autorisation

Tout ceux sont combinés dans quatre règles d'autorisation :

abab	6					_			
cisco	o Identity	Services Engine		🟠 Home	Operations   •	Policy   🔻	Guest Access	▼ Ad	Iministration   🔻
🔔 Au	uthentication	Authorization	🛃 Profiling	💽 Posture	👩 Client Provi	sioning	💼 TrustSec	🐥 Pol	licy Elements
Autho	rization P	olicy							
Define th For Polic	e Authorizatio y Export go to	n Policy by configuring rules Administration > System	based on identif > Backup & I	y groups and/or othe Restore > Policy E	r conditions. Drag : xport Page	and drop rule	es to change the ord	er.	
First M	fatched Rule	Applies +							
► Exce	eptions (0)								
Stand	dard								
5	Status Rule	e Name	C	onditions (identity gr	oups and other cor	nditions)			Permissions
	Com	pliant	ir <mark>(</mark> R Se	adius:Called-Station ssion:PostureStatus	-ID CONTAINS sec EQUALS Complia	ure_access int)	AND	then	PermitAccess
	Non	Compliant	if <mark>(</mark> R Se	adius:Called-Station ssion:PostureStatus	-ID CONTAINS sec EQUALS NonCon	ure_access npliant)	AND	then	LimitedAccess
	<ul> <li>Unkr</li> </ul>	nown	if <mark>(</mark> R Se	adius:Called-Station ssion:PostureStatus	-ID CONTAINS sec EQUALS Unknow	ure_access n)	AND	then	GuestProvisioning
1	Prov	isioning	if <mark>(</mark> R Se	adius:Called-Station ssion:PostureStatus	-ID CONTAINS pro EQUALS Unknow	visioning AN n )	D	then	GuestProvisioning

D'abord vous vous connectez au ravitaillement SSID et êtes réorienté pour le ravitaillement à un portail par défaut de ravitaillement de client (règle Provisioning Désigné). Une fois que vous vous connectez au **Secure\_access** SSID, il réoriente toujours pour le ravitaillement si aucun état du module de posture n'est reçu par ISE (règle Unknown Désigné). Une fois que le point final est entièrement conforme, on accorde l'accès complet (nom de règle conforme). Si le point final est signalé comme non-conforme, il a limité l'accès au réseau (règle NonCompliant Désigné).

## Vérifiez

Vous vous associez avec le ravitaillement SSID, essayez d'accéder à n'importe quelle page Web, et êtes réorienté au portail de ravitaillement de client :



Puisqu'AnyConnect n'est pas détecté, vous êtes invité à l'installer :

#### **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								
<ol> <li>You must install AnyConnect to check your device before accessing the network. <u>Click here to download and install</u> <u>AnyConnect</u></li> <li>After installation, AnyConnect will automatically scan your device before allowing you access to the network.</li> <li>You have 4 minutes to install and for the system scan to complete.</li> </ol>								
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								

Un petit application a appelé l'assistant de configuration réseau, qui est responsable du processus d'installation entier, est téléchargé. Notez qu'il est différent que l'assistant de configuration réseau dans la version 1.2.



Tous les modules (VPN, NAM, et posture) sont installés et configurés. Vous devez redémarrer votre PC :



Après que la réinitialisation, AnyConnect soit automatiquement exécutée et essai NAM pour s'associer avec les secure\_access SSID (selon le profil configuré). Notez que le profil VPN est correctement installé (entrée asav2 pour le VPN) :

Cisco AnyConne	ct   secure_access	🔊 Cisco AnyCo	nnect Secure Mobility Client 🛛 🙂 🖾
Please enter	r your username and password for the network: secure_access	C	VPN: Verify your network connection.
Password:		_	asav2   Connect
	Show Password	No Network C	Connectivity
	OK Cancel	<b>E</b>	Network: Authenticating secure_access
		٢	System Scan: Limited or no connectivity.
		<b>\$</b> ()	ajaaja. Cisco

Après authentification, AnyConnect télécharge des mises à jour et pose également les règles pour lesquelles la vérification est exécutée :

🕥 Cisco AnyCo	nnect Secure Mobility Client	
	VPN: Ready to connect. asav2	▼ Connect
	Network: Connected (10.221.0.250) secure_access	- 11.
	System Scan: Checking requirement 1 of 1.	
<b>\$</b> (i)		aljajn cisco

Àce stade, il pourrait encore y avoir d'accès limité (vous rencontrez la règle inconnue d'autorisation sur ISE). Une fois que la station est conforme, cela est signalé par le module de posture :

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

Les détails peuvent être également vérifiés (le FileRequirement est satisfait) :

9	Cisco AnyConnect Secure Mobility Client						- • <b>·</b> ×
	cisco AnyConnee	ct	Sec	ure	Mobility Client		î
	Status Overview		Systen	n Scan			
	VPN		Preference	ces Stat	istics Security Products Scan Summary	Message History	
	Network		Requ	uired —	Updates	Status	-
	System Scan >		1	0	FileRequirement	Done	
Г							

L'historique de message affiche les étapes détaillées :

```
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.

L'état réussi est envoyé à ISE, qui déclenche la modification de l'autorisation. La deuxième authentification rencontre la règle conforme et le plein accès au réseau est accordé. Si l'état de posture est envoyé tandis que toujours associé au ravitaillement SSID, ces logs sont vus sur ISE :

cisco	Identity Ser	vices Engine			A Home C	perations   * Policy   *	Quest Access   • Ad	ministration   •		Lance We	uned a 1 mars 1 agent 1 codere 1	
🗰 Authent Eczions 👔 Reports 🔯 Endpoint Protection Service 🔪 Troubleshoot												
Misconfigured Supplicants (0) Misconfigured Natwork Devices (0) RADIUS Drops (0) Client Stopped Responding (0) 0 1									ed Responding (1) 1			
G She	w Live Sessions	and an i	Remove C	olumns 🕶 🤣	Refresh 👩 Reset Re	peat Counts				Refresh Ever	y1 minute * Show Latest 20 r	
Time		Status Al • De	t R	identity (	Endpoint ID	Authorization Policy (2)	Authorization Profiles	Network Device	Pesture Status	Server ®	Event ®	
2014-13	1-16 09:32:07		à (	cisco	C0:44:00:15:64:DC				Compliant	ise13	Session State is Started	
2014-11	1-16 09:32:07	. 🖬 🔡	ò	cisco	C0:44.00:15:64.DC	Default >> Compliant	PermitAccess	WLC1	Compliant	isel3	Authentication succeeded	
2014-13	1-16 09:32:07		ò		C0:44.00:15:64.DC			WLC1	Compliant	ise13	Dynamic Authorization succeeded	
2014-11	1-16 09:31:35	•	ò	admin	C0:44.00:15:64.DC			WLC1		ise13	Authentication failed	
2014-11	1-16 09:29:34.		ò	cisco	C0:44:00:15:64:DC	Default >> Provisioning	GuestProvisioning	WLC1	Pending	ise13	Authentication succeeded	

#### L'état de posture indique :

abab								Lances Marking	A 1.000 (	alaus i Logost i Poellack D
CISCO Identity Services Engine	🙊 Hor	te Ope	rations I .	Policy	Guest Acc	ess I • Administratio	1.			Seta
Authentications Reports 101	Indpoint Protection Service	<b>N</b> D	ubiration	e.						
Report Selector	Posture Detail Asses	sment								🐈 Favorite 🛛 🔒 Export
Favorites										Generated at 2014
ISE Reports	From 11/16/2014 12:00:0	0 AM 1o 11	162014	19.27:56 AM						Page of 3 to Resolution
<ul> <li>Auth Services Status</li> </ul>	Logged At	Status	Detail	PRA	identity	Endpoint ID	P Address	Endpoint OS	Agent	Message
# rapoda	2014-11-16 09-23-25.8		0	NIA	cisco	C0:44.00:15:6A.D	10.221.0.250	Windows 7 Utsmate 64-bit	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		i i	NIA	cisco	C0.44.00.15.64.D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect	Received a posture report from an endpoint
▼ Endpoints and Users	2014-11-16 09-16:59.6		i i	7405	cisco	C0:44:00:15:64:D	10.221.0.250	Windows 7 Utsmate 64-bit	AnyConnect	Received a posture report from an endpoint
Client Provisioning	2014-11-16 09:15:17.4		0	NIA	cisco	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 Hobile Device Hanagement										
Posture Detail Assessment										
Ÿ Niters →										
Time Range Teday										
- Run										

Les rapports détaillés affichent le FileRequirement qui est satisfait :

#### **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	2			
Client Operating System	m: Windows	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		

## Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

## Informations connexes

- Services de posture sur le guide de configuration de Cisco ISE
- Guide d'administrateurs de Cisco ISE 1.3
- Support et documentation techniques Cisco Systems