

# Configurez ISE 2.1 et contrôle de la posture USB d'AnyConnect 4.3

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[ASA](#)

[ISE](#)

[Étape 1. Périphérique de configure network](#)

[Étape 2. Configurez les états et les stratégies de posture](#)

[Étape 3. Configurez les ressources et la stratégie en ravitaillement de client](#)

[Étape 4. Configurez les règles d'autorisation](#)

[Vérifier](#)

[Avant établissement de session VPN](#)

[Établissement de session VPN](#)

[Ravitaillement de client](#)

[Contrôle de posture et CoA](#)

[Dépanner](#)

[Références](#)

## Introduction

Ce document décrit comment configurer le Logiciel Cisco Identity Services Engine (ISE) pour fournir l'accès complet au réseau seulement quand des mémoires de masse USB sont déconnectées.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de configuration CLI de l'appliance de sécurité adaptable (ASA) et de configuration du VPN de Protocole SSL (Secure Socket Layer)
- Connaissance de base de configuration du VPN d'Accès à distance sur l'ASA
- Connaissance de base des services ISE et de posture

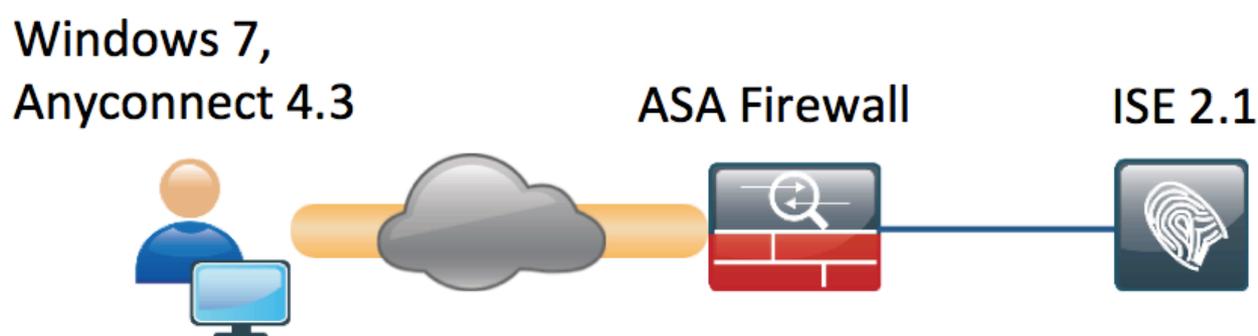
[Composants utilisés](#)

Version 2.1 du Logiciel Cisco Identity Services Engine (ISE) avec le contrôle et la correction sécurisés de mémoire de masse USB de supports du client 4.3 de mobilité d'AnyConnect. Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Versions de logiciel de Cisco ASA 9.2(4) et plus tard
- Version 7 de Microsoft Windows avec la version 4.3 et ultérieures de Client à mobilité sécurisé Cisco AnyConnect
- Cisco ISE, version 2.1 et ultérieures

## Configurer

### [Diagramme du réseau](#)



L'écoulement est le suivant :

- L'utilisateur n'est pas connecté au VPN encore, la mémoire de masse privée USB est branchée et satisfait est disponible pour l'utilisateur
- La session VPN initiée par le client d'AnyConnect est authentifiée par l'intermédiaire d'ISE. Le statut de posture du point final n'est pas connu, la règle « Posture\_Unknown » est frappée et en conséquence la session sera réorientée à l'ISE
- Les contrôles USB introduit une nouvelle classe de signe la posture à C.A. ISE, du fait ils surveillent continuellement le point final tant que il demeure dans le même réseau contrôlé par ISE. La seule action logique de correction disponible est de bloquer les dispositifs USB identifiés par leur identificateur de lecteur
- La session VPN sur l'ASA est mise à jour, réorientent l'ACL est retirée et l'accès complet est accordé

La session VPN a été présentée juste comme exemple. La fonctionnalité de posture fonctionne bien également pour d'autres types de l'accès.

## ASA

L'ASA est configurée pour l'accès distant de VPN SSL utilisant ISE comme serveur d'AAA. Le

CoA de Radius avec réorientent les besoins d'ACL d'être configuré :

```
aaa-server ISE21 protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE21 (outside) host 10.48.23.88
  key cisco
```

```
tunnel-group RA type remote-access
tunnel-group RA general-attributes
  address-pool POOL
  authentication-server-group ISE21
  accounting-server-group ISE21
  default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
  group-alias RA enable
```

```
webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-4.3.00520-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable
  group-policy GP-SSL internal
  group-policy GP-SSL attributes
  dns-server value 10.62.145.72
  vpn-tunnel-protocol ssl-client
```

```
access-list ACL_WEBAUTH_REDIRECT extended deny udp any any eq domain
access-list ACL_WEBAUTH_REDIRECT extended deny ip any host 10.48.23.88
access-list ACL_WEBAUTH_REDIRECT extended deny icmp any any
access-list ACL_WEBAUTH_REDIRECT extended permit tcp any any
```

Pour plus de détails veuillez se rapportent :

[Intégration d'AnyConnect 4.0 avec l'exemple de configuration de version 1.3 ISE](#)

## ISE

### Étape 1. Périphérique de configure network

De la gestion > des ressources de réseau > des périphériques de réseau > ajoutez l'ASA.

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Network Devices List > BSNS-ASA5515-11

### Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

Location

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

CoA Port

## Étape 2. Configurez les états et les stratégies de posture

Assurez-vous que des états de posture sont mise à jour : **La gestion > le système > les configurations > la posture > met à jour > option de mise à jour maintenant.**

ISE 2.1 est livré avec un état préconfiguré USB, qui vérifie si une mémoire de masse USB est connectée.

**De la stratégie > des éléments de stratégie > conditionne > posture > état USB** vérifient l'état existant :

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

- Anti-Malware Condition
- Anti-Spyware Condition
- Anti-Virus Condition
- Application Condition
- Compound Condition
- Disk Encryption Condition
- File Condition
- Patch Management Condition
- Registry Condition
- Service Condition
- USB Condition

Dictionary Simple Condition

Dictionary Compound Condition

Guest

Common

Name USB\_Check

Description Cisco Predefined Check: Checks if USB mass storage device is connected.

Operating System Windows All

Compliance Module 4.x or later ⓘ

De la stratégie > des éléments de stratégie > résulte > la posture > les conditions requises, vérifient la condition requise préconfigurée qui utilise cette condition.

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Remediation Actions

Requirements

Client Provisioning

Requirements

Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
USB_Block	for Windows All	using 4.x or later	met if USB_Check	then USB_Block

De la stratégie > de la posture, ajoutez une condition pour tout le Windows pour utiliser cette condition requise :

Identity Services Engine Home > Context Directory > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

### Posture Policy

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

Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Other Conditions	Requirements
✓	Windows 7 USB check	If Any	and Windows 7 (All)	and 4.x or later	and	then USB_Block

De la stratégie > des éléments de stratégie > résultat > les actions de posture > de correction > les corrections USB vérifient l'action préconfigurée de correction de bloquer des périphériques de stockage USB :

Identity Services Engine Home > Context Directory > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys > Conditions > Results

### USB Remediations

Edit + Add Duplicate Delete

Name	Description	Type
<input type="checkbox"/> USB_Block	Cisco Predefined Remediation: ...	Automatic

- Authentication
- Authorization
- Profiling
- Posture
  - Remediation Actions
    - Anti-Malware Remediations
    - Anti-Spyware Remediations
    - Anti-Virus Remediations
    - File Remediations
    - Launch Program Remediations
    - Link Remediations
    - Patch Management Remediations
    - USB Remediations
    - Windows Server Update Services Remediations
    - Windows Update Remediations
    - Requirements
- Client Provisioning

### Étape 3. Configurez les ressources et la stratégie en ravitaillement de client

De la stratégie > des éléments de stratégie > du ravitaillement > des ressources de client téléchargez le module de conformité de Cisco.com et téléchargez manuellement le module d'AnyConnect 4.3 :

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Directory', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is expanded to show 'Policy Elements'. On the left, there is a sidebar with 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning' sections. The main area displays a table of resources under the 'Resources' heading.

Name	Type	Version	Last Update	Description
<input checked="" type="checkbox"/> AnyConnectDesktopWindows 4.3.520.0	AnyConnectDesktopWindows	4.3.520.0	2016/03/11 11:10:47	AnyConnect Secure Mobility Clie...
<input checked="" type="checkbox"/> AnyConnectComplianceModuleWind...	AnyConnectComplianceMo...	4.2.330.0	2016/03/11 11:11:16	AnyConnect Windows Complian...
<input type="checkbox"/> WinSPWizard 2.1.0.50	WinSPWizard	2.1.0.50	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
<input type="checkbox"/> AnyConnect Configuration	AnyConnectConfig	Not Applicable	2016/03/11 11:12:42	
<input type="checkbox"/> MacOsXSPWizard 2.1.0.39	MacOsXSPWizard	2.1.0.39	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
<input type="checkbox"/> Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
<input type="checkbox"/> Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
<input type="checkbox"/> Anyconnect_Posture_Profile	AnyConnectProfile	Not Applicable	2016/03/11 14:39:03	

Utilisant **ajoutez > agent NAC** ou le **profil de posture d'AnyConnect** crée un profil de posture d'AnyConnect (nom : *Anyconnect\_Posture\_Profile*) avec des valeurs par défaut.

Utilisant **ajoutez > configuration d'AnyConnect** ajoutent une configuration d'AnyConnect (nom : Configuration d'AnyConnect) :

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for 'AnyConnect Configuration'. The top navigation bar is the same as in the previous screenshot. The left sidebar is also the same. The main area shows the configuration form for 'AnyConnect Configuration'.

**AnyConnect Configuration > AnyConnect Configuration**

\* Select AnyConnect Package: AnyConnectDesktopWindows 4.3.520.0

\* Configuration Name: AnyConnect Configuration

Description: [Text Area]

**DescriptionValue**

\* Compliance Module: AnyConnectComplianceModuleWindows 4.2.330.0

**Notes**

**AnyConnect Module Selection**

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Start Before Logon
- Dagnostic and Reporting Tool

**Profile Selection**

- \* ISE Posture: Anyconnect\_Posture\_Profile
- VPN: [Dropdown]
- Network Access Manager: [Dropdown]
- Web Security: [Dropdown]
- AMP Enabler: [Dropdown]
- Network Visibility: [Dropdown]
- Customer Feedback: [Dropdown]

De la **stratégie > du ravitaillement de client** créez une nouvelle stratégie (Windows\_Posture) pour Windows pour utiliser la configuration d'AnyConnect :

### Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:  
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then WinSPWizard 2.1.0.50 And Cisco-ISE-NSP
Windows_Posture	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration
MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOsXSPWizard 2.1.0.39 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

## Étape 4. Configurez les règles d'autorisation

De la stratégie > des éléments de stratégie > résultat > l'autorisation ajoutent un profil d'autorisation (nom : Posture\_Redirect) ce redirect to un portail par défaut de ravitaillement de client :

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authorization Profiles > Posture\_Redirect

### Authorization Profile

\* Name: Posture\_Redirect

Description: [Empty]

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

---

**Common Tasks**

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: ACL\_WEBAUTH\_REDIRECT Value: Client Provisioning Portal (defa

Remarque: L'ACL ACL\_WEBAUTH\_REDIRECT est défini sur l'ASA.

De la stratégie > de l'autorisation créez une règle d'autorisation pour la redirection. Une règle d'autorisation pour les périphériques conformes est préconfigurée sur ISE :

### 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

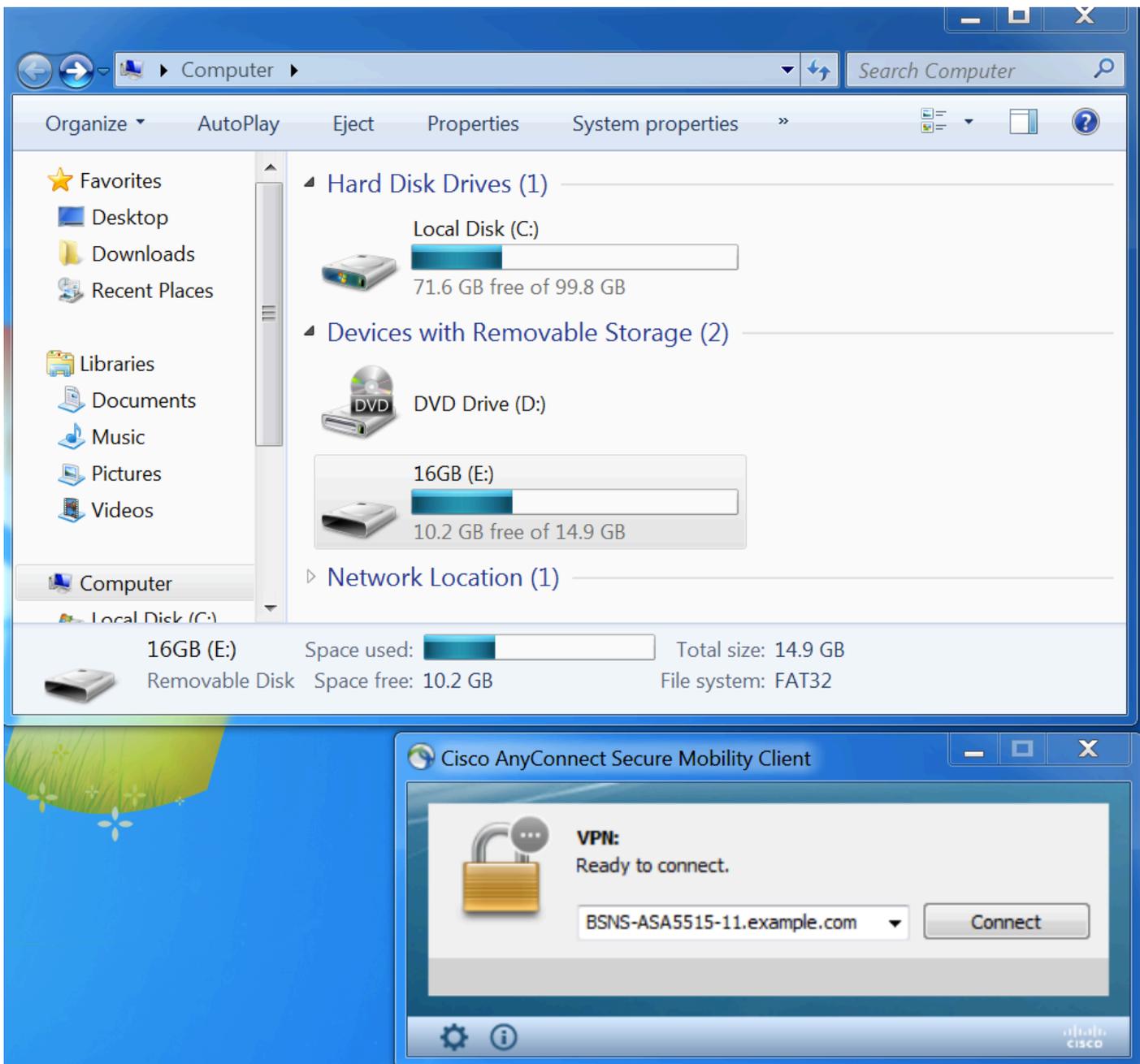
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices )	then PermitAccess
✔	Posture_Unknown	if Session:PostureStatus NOT_EQUALS Compliant	then Posture_Redirect

Si le point final est conforme, l'accès complet est fourni. Si l'état est inconnu ou nonconformant, la redirection pour le ravitaillement de client est retournée.

## Vérifiez

### Avant établissement de session VPN

Le périphérique USB branché, et son contenu est disponible pour l'utilisateur.



## Établissement de session VPN

Pendant l'authentification, ISE renverra le redirect access-list et réorientera l'URL en tant qu'élément du profil d'autorisation de Posture\_Redirect

Cisco Identity Services Engine											
Operations > Policy > Administration > Work Centers											
RADIUS TC-NAC Live Logs > TACACS Legacy Dashboard > Reports > Troubleshoot > Adaptive Network Control											
Live Logs Live Sessions											
Misconfigured Supplicants		Misconfigured Network Devices		RADIUS Drops		Client Stopped Responding		Repeat Counter			
0		0		6		0		0			
Refresh Every 1 minute Show Latest 20 records Within Last 5 minutes											
Time	Sta...	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Pr...	IP Address	Network De...	Posture Status	Server
Mar 11, 2016 03:57:40.126 PM			cisco	00:0C:29:C9:...	Default >> Default >> Default	Default >> Posture_Un...	Posture_Redirect	10.10.10...		Pending	ISE21-1
Mar 11, 2016 03:57:39.598 PM			cisco	00:0C:29:C9:...	Default >> Default >> Default	Default >> Posture_Un...	Posture_Redirect		BSNS-ASA55...	Pending	ISE21-1

Une fois que la session VPN est établie, le trafic ASA du client obtiendra réorienté selon le redirect

## access-list :

BSNS-ASA5515-11# **sh vpn-sessiondb detail anyconnect**

Session Type: AnyConnect Detailed

Username : cisco Index : 29  
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Premium  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES128  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 14696 Bytes Rx : 18408  
Pkts Tx : 20 Pkts Rx : 132  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : GP-SSL Tunnel Group : RA  
Login Time : 15:57:39 CET Fri Mar 11 2016  
Duration : 0h:07m:22s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0a3042ca0001d00056e2dce3  
Security Grp : none

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 29.1  
Public IP : 10.229.16.34  
Encryption : none Hashing : none  
TCP Src Port : 61956 TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes  
Client OS : win  
Client OS Ver: 6.1.7601 Service Pack 1  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520  
Bytes Tx : 6701 Bytes Rx : 774  
Pkts Tx : 5 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 29.2  
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34  
Encryption : AES128 Hashing : SHA1  
Encapsulation: TLSv1.0 TCP Src Port : 61957  
TCP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520  
Bytes Tx : 6701 Bytes Rx : 1245  
Pkts Tx : 5 Pkts Rx : 5  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 29.3  
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34  
Encryption : AES128 Hashing : SHA1  
Encapsulation: DTLSv1.0 UDP Src Port : 55708  
UDP Dst Port : 443 Auth Mode : userPassword

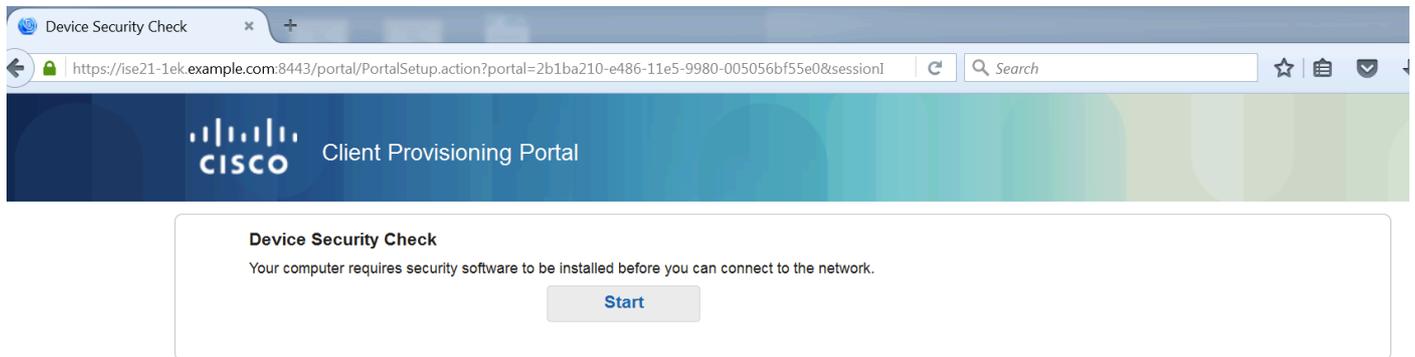
Idle Time Out: 30 Minutes                      Idle TO Left : 26 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520  
Bytes Tx : 1294                                      Bytes Rx : 16389  
Pkts Tx : 10    Pkts Rx : 126  
Pkts Tx Drop : 0                                      Pkts Rx Drop : 0

**ISE Posture:**

Redirect URL : <https://ISE21-1ek.example.com:8443/portal/gateway?sessionId=0a3042ca0001d00056e2dce3&portal=2b1ba210-e...>  
Redirect ACL : ACL\_WEBAUTH\_REDIRECT

## Ravitaillement de client

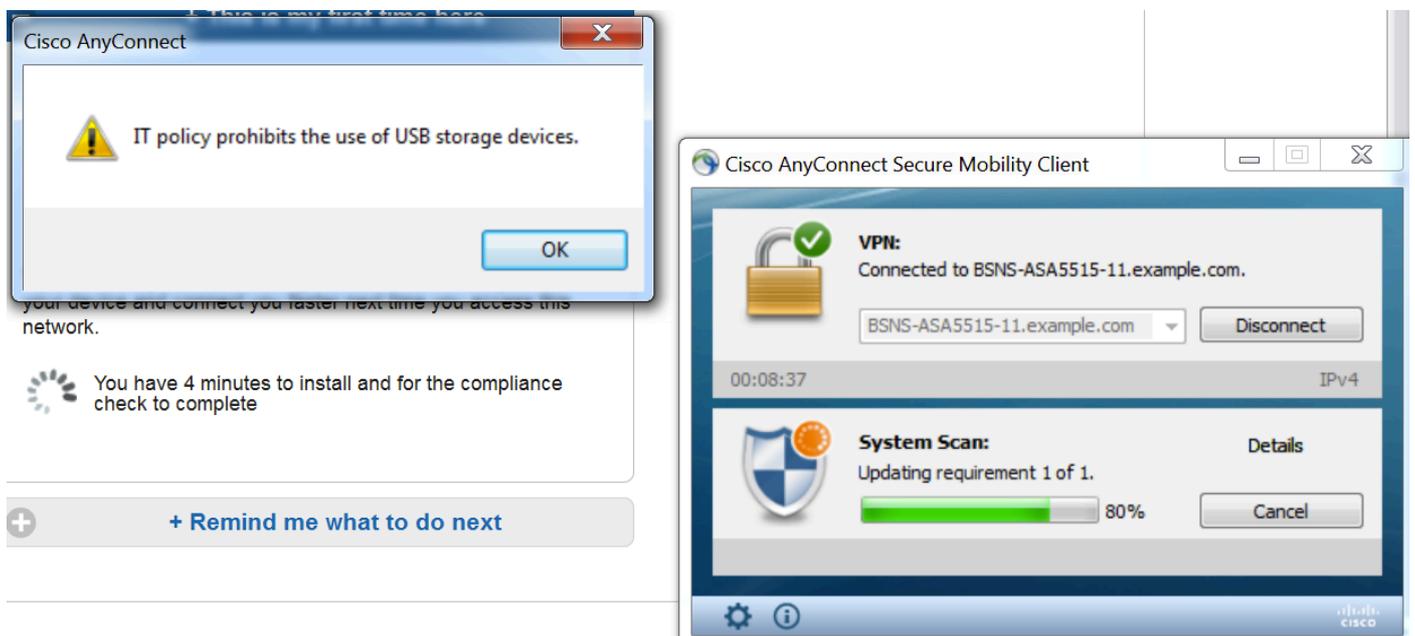
À cette étape, le trafic de navigateur Web de point final est réorienté à ISE pour le ravitaillement de client :



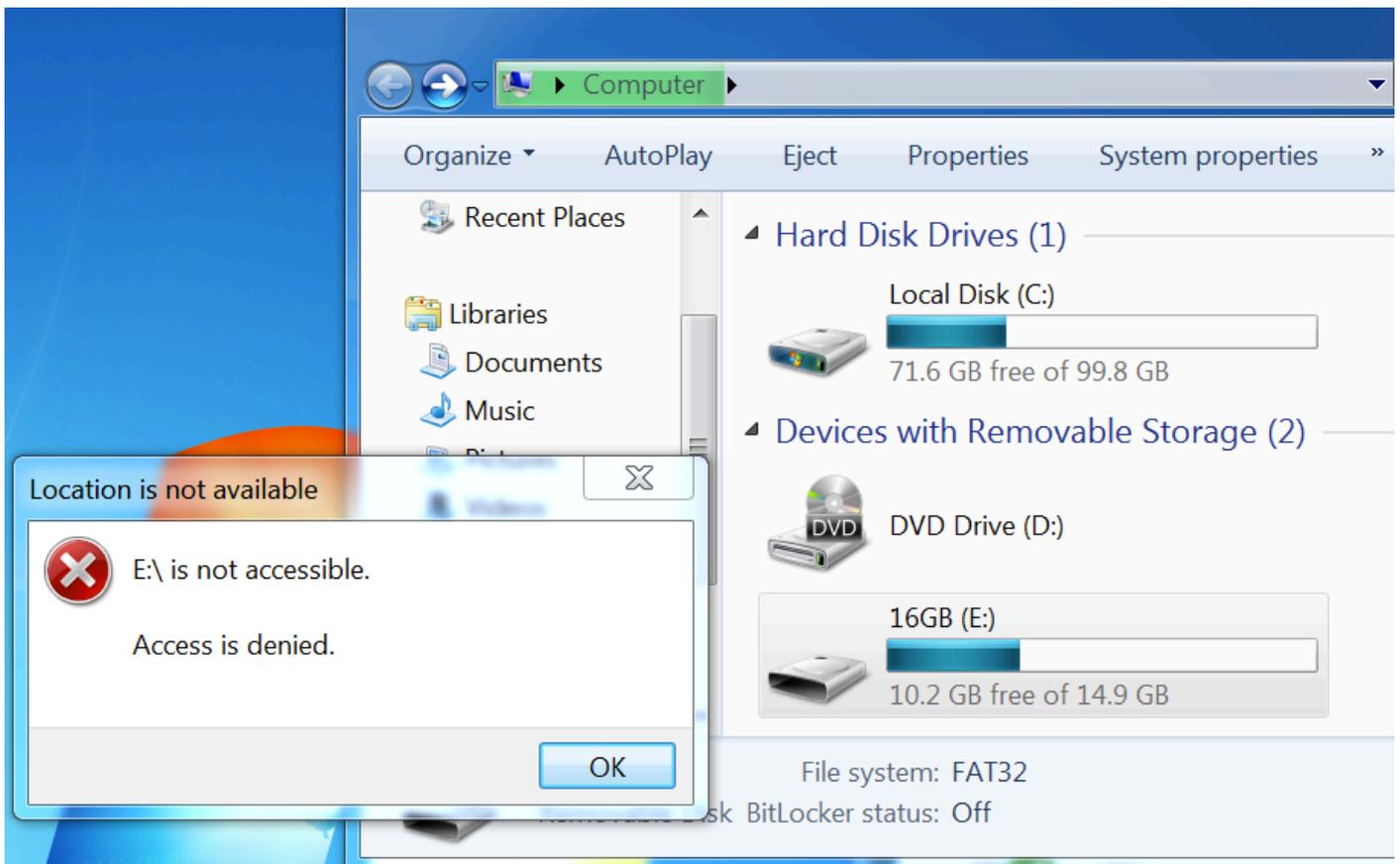
Si nécessaire, AnyConnect avec le module de posture et de conformité est mis à jour.

## Contrôle de posture et CoA

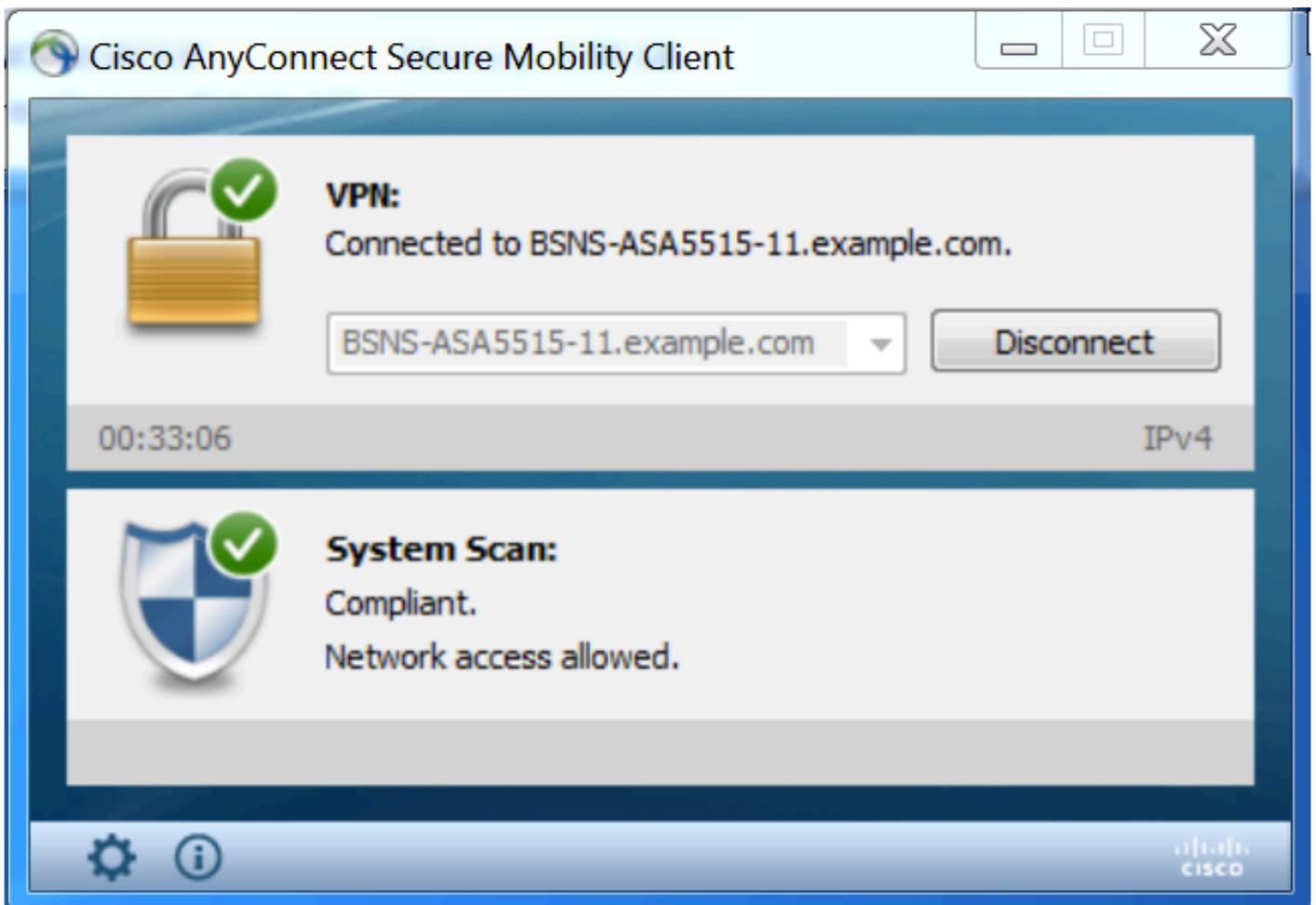
Le module de posture est exécuté, découvre ISE (il pourrait exiger pour avoir l'enregistrement des DN A pour qu'enroll.cisco.com réussisse), télécharge et vérifie des états de posture, nouvelle action de périphérique USB de bloc OPSWAT v4. Le message configuré sera affiché pour l'utilisateur :



Une fois que le message est confirmé, le périphérique USB n'est plus disponible pour l'utilisateur :



L'ASA retire l'ACL de redirection fournissant l'accès complet. AnyConnect signale la conformité :



Également les rapports détaillés sur ISE peuvent confirmer que des conditions exigées sont passées.

### Estimation de posture par condition :

Report Selector

ISE Reports

Posture Assessment by Condition

From 03/11/2016 12:00:00.000 AM to 03/11/2016 04:37:13.253 PM

Logged At	Posture	Identity	Endpoint ID	IP Address	Location	Endpoint OS	Policy	Enforcement Type	Condition Status	Condition name
2016-03-11 16:06:24.974	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:31:53.456	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:26:57.007	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:16:33.483	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check

### Estimation de posture par point final :

Report Selector

ISE Reports

Posture Assessment by Endpoint

From 03/11/2016 12:00:00.000 AM to 03/11/2016 04:33:39.111 PM

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2016-03-11 16:06:24.974	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint
2016-03-11 11:31:53.456	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint
2016-03-11 11:26:57.007	✓		logoff	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Posture service received a USB-check report from an endpoint
2016-03-11 11:16:33.483	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint

### Détails d'état de point final :

**Posture More Detail Assessment**

Time Range: From 03/11/2016 12:00:00 AM to 03/11/2016 04:34:03.708 PM  
Generated At: 2016-03-11 16:34:03.708

---

Username: cisco  
Mac Address: 00:0C:29:C9:D9:37  
IP address: 10.48.66.202  
Location: All Locations  
Session ID: 0a3042ca0001d00056e2dce3  
Client Operating System: Windows 7 Ultimate 64-bit  
Client NAC Agent: AnyConnect Posture Agent for Windows 4.3.00520  
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: WIN7-PC  
System Domain: n/a  
System User: Win7  
User Domain: Win7-PC  
AV Installed:  
AS Installed:  
AM Installed: Windows Defender;6.1.7600.16385;1.215.699.0;03/09/2016;

Posture Report  
Posture Status: Compliant  
Logged At: 2016-03-11 16:06:24.974

Posture Policy Details

Policy	Name	Enforcement Type	Status	Passed Conditions	Failed Conditions	Skipped Conditions
Windows 7 USB check	USB_Block	Mandatory		USB_Check		

## Dépanner

ISE peut fournir les détails sur les conditions manquantes, des actions devrait être pris en conséquence.

## Références

- [Configuration d'un serveur externe pour l'autorisation de l'utilisateur de l'appareil de sécurité](#)
- [Guide de configuration du CLI VPN de la série Cisco ASA, 9.1](#)
- [Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 2.0](#)
- [Support et documentation techniques - Cisco Systems](#)