

Configurez ISE 2.0 et chiffrez le cryptage de BitLocker de posture d'AnyConnect 4.2

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[ASA](#)

[BitLocker sur le Windows 7](#)

[ISE](#)

[Étape 1. Périphérique de réseau](#)

[Étape 2. État et stratégies de posture](#)

[Étape 3. Ressources et stratégie en ravitaillement de client](#)

[Étape 4. Règles d'autorisation](#)

[Vérifier](#)

[Étape 1. Établissement de session VPN](#)

[Étape 2. Ravitaillement de client](#)

[Étape 3. Contrôle de posture et CoA](#)

[Bogues](#)

[Dépanner](#)

[Informations connexes](#)

Introduction

Ce document décrit comment chiffrer la partition de disque du point final avec l'utilisation de Microsoft BitLocker et comment configurer le Logiciel Cisco Identity Services Engine (ISE) afin de fournir l'accès complet au réseau, seulement quand le cryptage correct est configuré. La version 2.0 de Cisco ISE avec le client sécurisé 4.2 de mobilité d'AnyConnect prend en charge la posture pour le chiffrement de disque.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

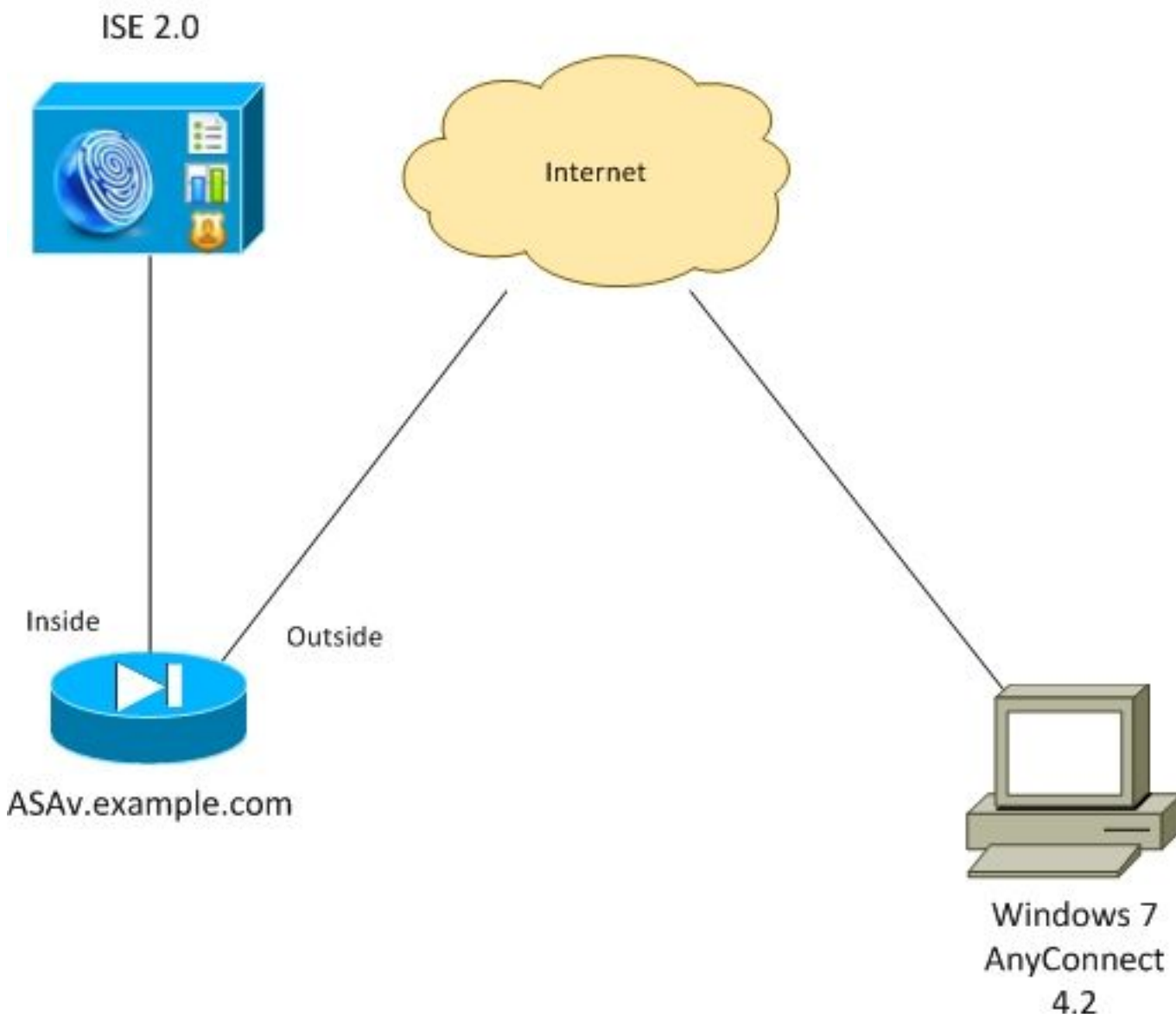
Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Versions de logiciel 9.2.1 de Cisco ASA et plus tard
- Version 7 de Microsoft Windows avec la version 4.2 et ultérieures de Client à mobilité sécurisé Cisco AnyConnect
- Cisco ISE, version 2.0 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 en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



L'écoulement est comme suit :

- 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, l'**inconnu de la règle ASA VPN** est frappé et en conséquence la session est réorientée à l'ISE pour le ravitaillement
- L'utilisateur ouvre le navigateur Web, le trafic http est réorienté par ASA à ISE. ISE pousse la plus nouvelle version d'AnyConnect avec le module de posture et de conformité au point final
- Une fois que le module de posture est exécuté, il vérifie si la partition **E** : est entièrement chiffré par BitLocker. Si oui, l'état est envoyé à ISE qui ne déclenche la modification de Radius de l'autorisation (CoA) sans aucun ACL (l'accès complet)
- La session VPN sur l'ASA est mise à jour, réorientent l'ACL est retirée et la session a l'accès complet

La session VPN est présentée comme exemple. La fonctionnalité de posture fonctionne bien trop pour d'autres types de l'accès.

ASA

Il est configuré de l'accès distant de VPN SSL avec l'utilisation d'ISE comme serveur d'Authentification, autorisation et comptabilité (AAA). Le CoA de Radius avec RÉORIENTENT les besoins d'ACL d'être configuré :

```

aaa-server ISE20 protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE20 (inside) host 10.48.17.235
  key cisco

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
  address-pool POOL
authentication-server-group ISE20
accounting-server-group ISE20
  default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
  group-alias TAC enable

group-policy AllProtocols internal
group-policy AllProtocols attributes
  vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable

access-list REDIRECT extended deny udp any any eq domain
access-list REDIRECT extended deny ip any host 10.48.17.235
access-list REDIRECT extended deny icmp any any
access-list REDIRECT extended permit tcp any any eq www

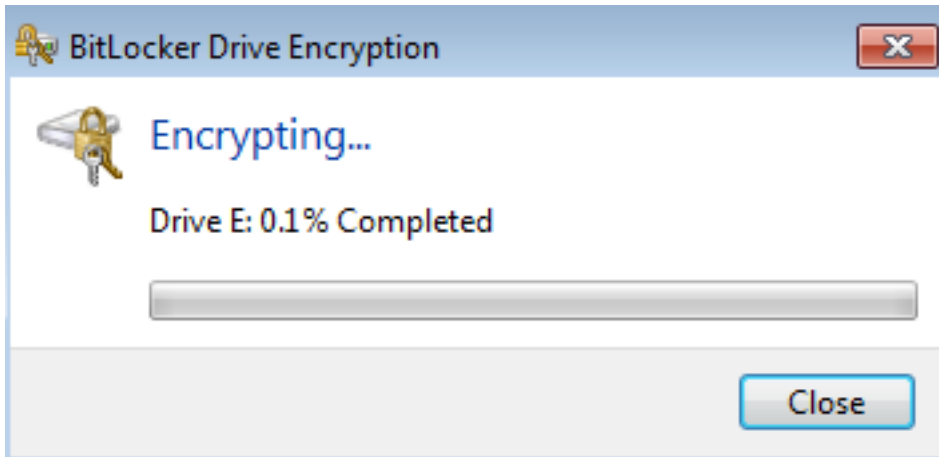
ip local pool POOL 172.16.31.10-172.16.31.20 mask 255.255.255.0

```

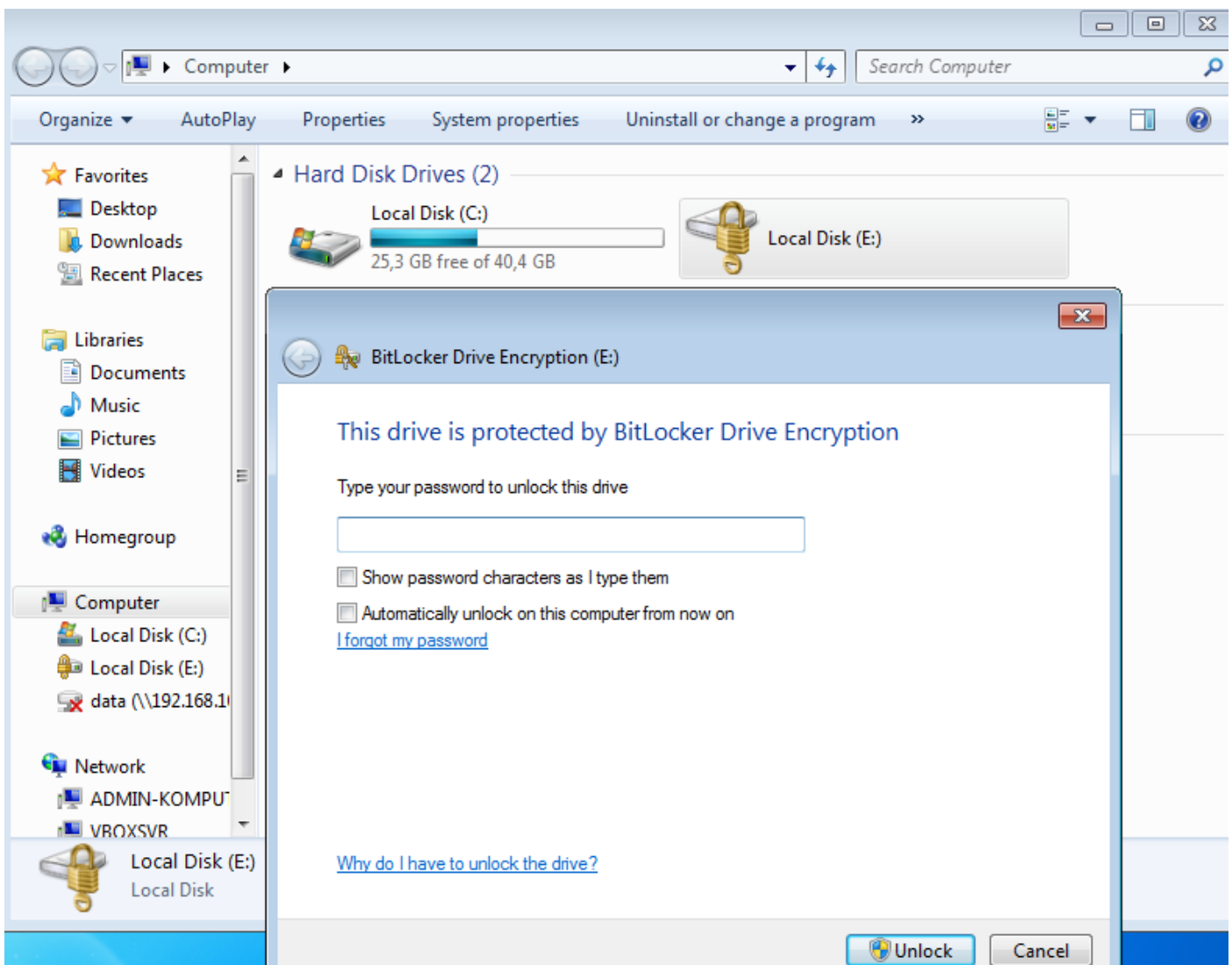
Pour plus de détails référez-vous :

BitLocker sur le Windows 7

Naviguez vers le **panneau de configuration > le système et la Sécurité > le cryptage d'entraînement de BitLocker**, l'enable **E** : cryptage de partition. Protégez-le par le mot de passe (PIN) suivant les indications de l'image.



Une fois qu'il est chiffré, montez-le (avec la fourniture du mot de passe) et assurez-vous qu'il est accessible suivant les indications de l'image.



Pour plus de détails, suivez la documentation Microsoft :

[Guide de pas à pas de cryptage d'entraînement de Windows BitLocker](#)

ISE

Étape 1. Périphérique de réseau

Naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau**, ajoutez l'ASA avec le type de périphérique = l'ASA. Ceci est utilisé car une condition dans les règles mais elle d'autorisation n'est pas obligatoire (d'autres types de conditions peuvent être utilisés).

Si approprié, le groupe de périphériques réseau n'existe pas. Afin de créer, naviguez vers la **gestion > les ressources de réseau > les groupes de périphériques réseau**.

Étape 2. État et stratégies de posture

Assurez que des états de posture sont mise à jour : Naviguez vers la **gestion > le système > les configurations > la posture > les mises à jour > la mise à jour maintenant**.

Naviguez vers la **stratégie > les éléments de stratégie > les conditions > la posture > l'état de cryptage de disque**, ajoutez un nouvel état suivant les indications de l'image.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a "Disk Encryption Condition". The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements > Dictionaries > Conditions > Results.

The main configuration area is titled "Disk Encryption Condition" and includes the following fields:

- * Name: bitlocker
- Description: (empty)
- * Operating System: Windows All
- * Vendor Name: Microsoft Corp.

Below these fields is a table titled "Products for Selected Vendor":

	Product Name	Version	Encryption State Check	Minimum Compliant Module Supp...
<input type="checkbox"/>	BitLocker Drive Encryption	10.x	YES	3.6.10146.2
<input checked="" type="checkbox"/>	BitLocker Drive Encryption	6.x	YES	3.6.10146.2

At the bottom, there is a checkbox for "Encryption State" which is checked. Below this is a configuration for the encryption state:

Location: [Specific Locatio] E: [] is Fully Encrypted OR [] Pending Encryption OR [] Partially Encrypted

Contrôles de cette condition si BitLocker pour le Windows 7 est installé et si E : la partition est

entièrement chiffrée.

Note: BitLocker est cryptage de niveau de disque et il ne prend en charge pas l'emplacement spécifique avec l'argument de chemin, seulement lettre de disque.

Naviguez vers la **stratégie > les éléments > les résultats > la posture > les conditions requises de stratégie** afin de créer une nouvelle condition requise qui utilise la condition suivant les indications de l'image.

The screenshot shows the Cisco ISE interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The sub-navigation is: Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements. The 'Results' section is active, showing a list of requirements:

Name	Operating Systems	Conditions	Remediation Actions
Bitlocker	for Windows All	met if bitlocker	else Message Text Only
Any_AV_Definition_Mac	for Mac OSX	met if ANY_av_mac_def	else AnyAVDefRemediationMac
Any_AS_Definition_Win_copy	for Windows All	met if ANY_as_win_def	else AnyASDefRemediationWin
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

Naviguez vers la **stratégie > la posture**, ajoutez une condition pour tout le Windows afin d'utiliser la condition requise suivant les indications de l'image.

The screenshot shows the 'Posture Policy' configuration screen in Cisco ISE. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The sub-navigation is: Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements. The page title is 'Posture Policy' and it says '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"/>	Bitlocker	if Any	and Windows All		then Bitlocker

Étape 3. Ressources et stratégie en ravitaillement de client

Naviguez vers la **stratégie > les éléments de stratégie > le ravitaillement > les ressources de client**, téléchargez le **module de conformité de Cisco.com** et téléchargez manuellement le **module d'AnyConnect 4.2** suivant les indications de l'image.

Resources

The screenshot shows the 'Resources' table in Cisco ISE. At the top, there are action buttons: Edit, Add, Duplicate, and Delete. The table has the following columns: Name, Type, Version, Last Update, and Description. Two rows are checked:

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.36	MacOsXSPWizard	1.0.0.36	2015/10/08 09:24:15	ISE 2.0 Supplicant Provisioning ...
<input type="checkbox"/>	WinSPWizard 1.0.0.43	WinSPWizard	1.0.0.43	2015/10/29 17:15:02	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	ComplianceModule 3.6.10231.2	ComplianceModule	3.6.10231.2	2015/11/06 17:49:36	NACAgent ComplianceModule ...
<input checked="" type="checkbox"/>	AnyConnectDesktopWindows 4.2.96.0	AnyConnectDesktopWindows	4.2.96.0	2015/11/14 12:24:47	AnyConnect Secure Mobility Cli...
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.10231.2	AnyConnectComplianceMo...	3.6.10231.2	2015/11/06 17:50:14	AnyConnect Windows Complian...
<input type="checkbox"/>	AnyConnectPosture	AnyConnectProfile	Not Applicable	2015/11/14 12:26:16	
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2015/10/29 22:10:20	Pre-configured Native Supplica...
<input type="checkbox"/>	AnyConnect Configuration	AnyConnectConfig	Not Applicable	2015/11/14 12:26:42	
<input type="checkbox"/>	WinSPWizard 1.0.0.46	WinSPWizard	1.0.0.46	2015/10/08 09:24:16	ISE 2.0 Supplicant Provisioning ...

Naviguez pour ajouter > agent NAC ou le profil de posture d'AnyConnect, créez le profil de posture d'AnyConnect (nom : AnyConnectPosture) avec des valeurs par défaut.

Naviguez pour ajouter > configuration d'AnyConnect, ajoutez le profil d'AnyConnect (nom : Configuration d'AnyConnect) suivant les indications de l'image.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb trail is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements > Results. The left sidebar shows a navigation menu with 'Client Provisioning' selected. The main content area is titled 'AnyConnect Configuration > AnyConnect Configuration'. It contains several configuration fields:

- * Select AnyConnect Package: AnyConnectDesktopWindows 4.2.96.0
- * Configuration Name: AnyConnect Configuration
- Description: (empty text box)
- DescriptionValue
- * Compliance Module: AnyConnectComplianceModuleWindows 3.6.1

 Below these fields is the 'AnyConnect Module Selection' section with a list of checkboxes:

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

 The 'Profile Selection' section contains a list of dropdown menus:

- * ISE Posture: AnyConnectPosture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- Network Visibility
- Customer Feedback

Naviguez vers la stratégie > le ravitaillement de client et modifiez la stratégie par défaut pour Windows afin d'utiliser le profil configuré d'AnyConnect suivant les indications de l'image.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for the Client Provisioning Policy. The breadcrumb trail is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements. The page title is 'Client Provisioning Policy'. Below the title is a brief description: '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.' Below this is a table of rules:

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Windows	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration
<input checked="" type="checkbox"/> MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOsXSPWizard 1.0.0.36 And Cisco-ISE-NSP

Étape 4. Règles d'autorisation

Naviguez vers la **stratégie > les éléments > les résultats > l'autorisation de stratégie**, ajoutez le profil d'autorisation (nom : **RedirectForPosture**) quels redirect to un portail par défaut de ravitaillement de client suivant les indications de l'image.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. Under Policy Elements, there are sub-menus for Dictionaries, Conditions, and Results. The left sidebar shows a tree view with Authentication, Authorization (selected), Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > RedirectForPosture' and 'Authorization Profile'. The configuration fields are:

- * Name: RedirectForPosture
- Description: (empty)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template: (checkbox unchecked)
- Track Movement: (checkbox unchecked)

 The 'Common Tasks' section is expanded, showing:

- Web Redirection (CWA, MDM, NSP, CPP)
 - Client Provisioning (Posture): (dropdown)
 - ACL: REDIRECT
 - Value: Client Provisioning Portal
- Static IP/Host name/FQDN

RÉORIENTEZ L'ACL est défini sur l'ASA.

Naviguez vers la **stratégie > l'autorisation**, créez 3 règles d'autorisation suivant les indications de l'image.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for the Authorization Policy. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes Authentication, Authorization (selected), Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with Authentication, Authorization (selected), Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Policy'. Below the title, there is a description: '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'. There is a dropdown menu for 'First Matched Rule Applies' set to 'First Matched Rule Applies'. Below this, there is a section for 'Exceptions (0)' with a sub-section for 'Standard'. A table lists three rules:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	ASA VPN compliant	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Compliant)	then PermitAccess
<input checked="" type="checkbox"/>	ASA VPN unknown	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Unknown)	then RedirectForPosture
<input checked="" type="checkbox"/>	ASA VPN non compliant	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS NonCompliant)	then RedirectForPosture

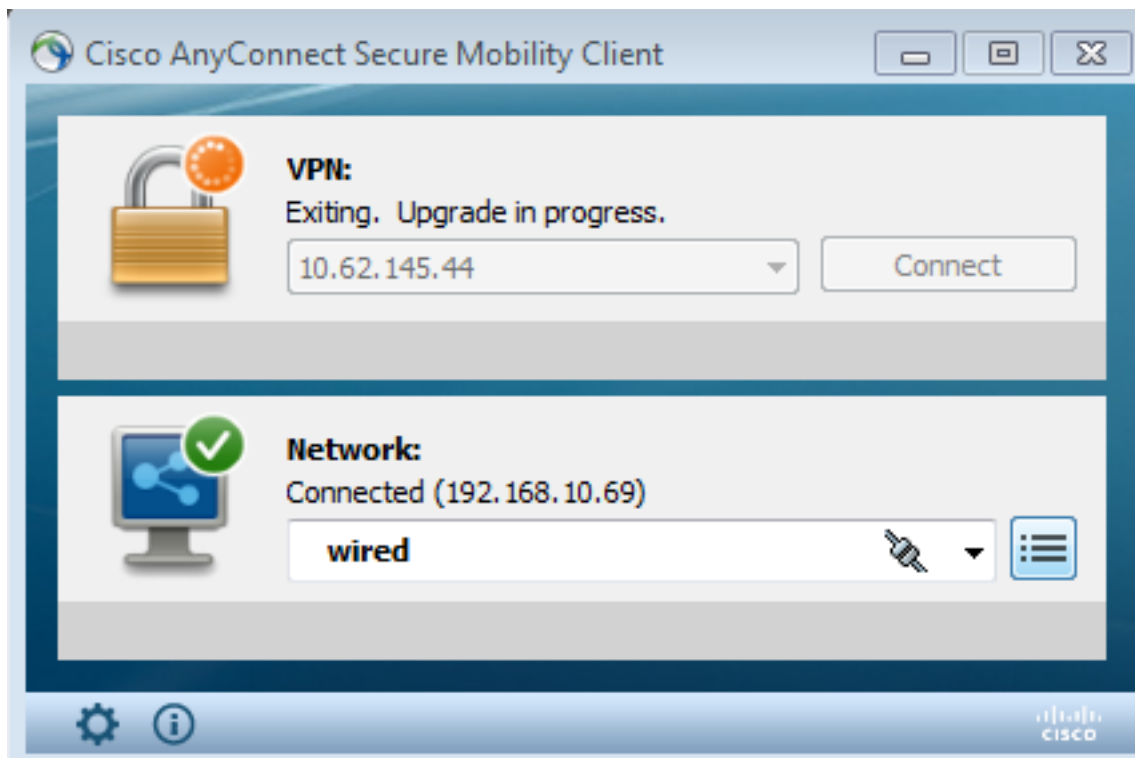
Si le point final est conforme, l'accès complet est fourni. Si l'état est inconnu ou non conforme, la redirection pour le ravitaillement de client est retournée.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Établissement de session VPN

Une fois que la session VPN est établie, l'ASA pourrait vouloir exécuter une mise à jour des modules d'AnyConnect suivant les indications de l'image.



Sur ISE la dernière règle est frappée, en conséquence des autorisations de **RedirectForPosture** sont renvoyées suivant les indications de l'image.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-11-14 14:59:06...	✓				10.229.20.45		PermitAccess	ASA	Dynamic Authorization succeeded
2015-11-14 14:59:04...	ⓘ		0	cisco	08:00:27:81:50:86	Default >> ASA VP...	RedirectForPosture	ASA	Session State is Postured
2015-11-14 14:58:22...	✓			cisco	08:00:27:81:50:86	Default >> ASA VP...	RedirectForPosture	ASA	Authentication succeeded

Une fois que l'ASA finit d'établir la session VPN, elle signale que la redirection doit se produire :

```
ASAv# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : cisco                Index          : 32
Assigned IP   : 172.16.31.10         Public IP      : 10.61.90.226
```

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 53201 Bytes Rx : 122712
Pkts Tx : 134 Pkts Rx : 557
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : AllProtocols Tunnel Group : TAC
Login Time : 21:29:50 UTC Sat Nov 14 2015
Duration : 0h:56m:53s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a80101000200005647a7ce
Security Grp : none

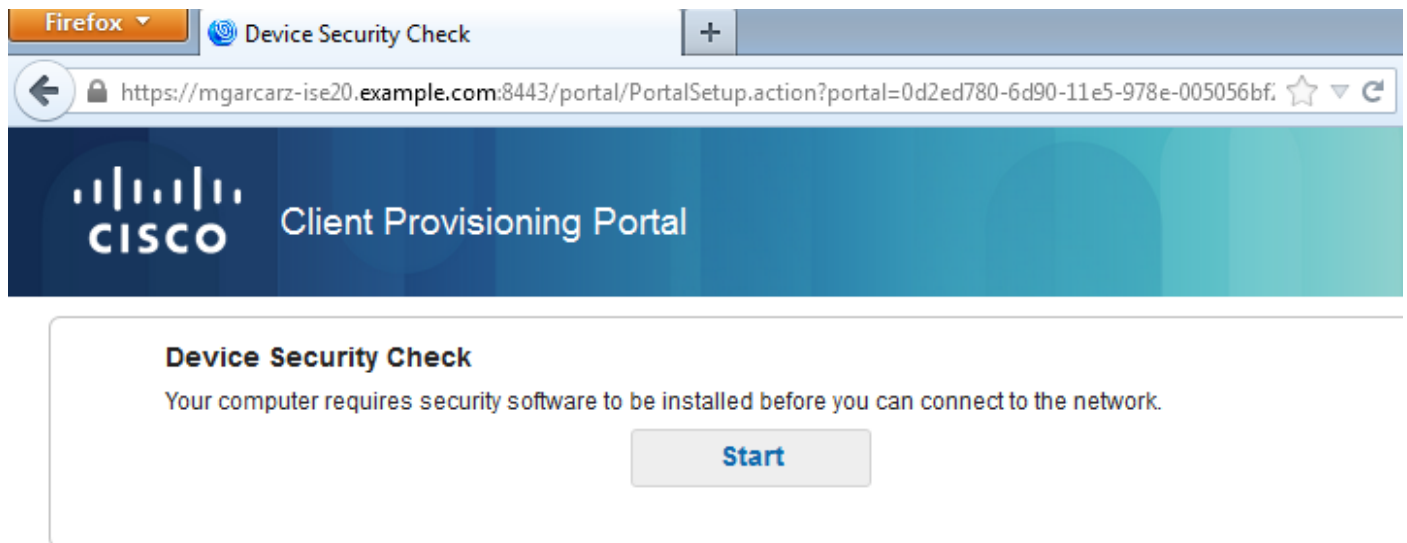
<some output omitted for clarity>

ISE Posture:

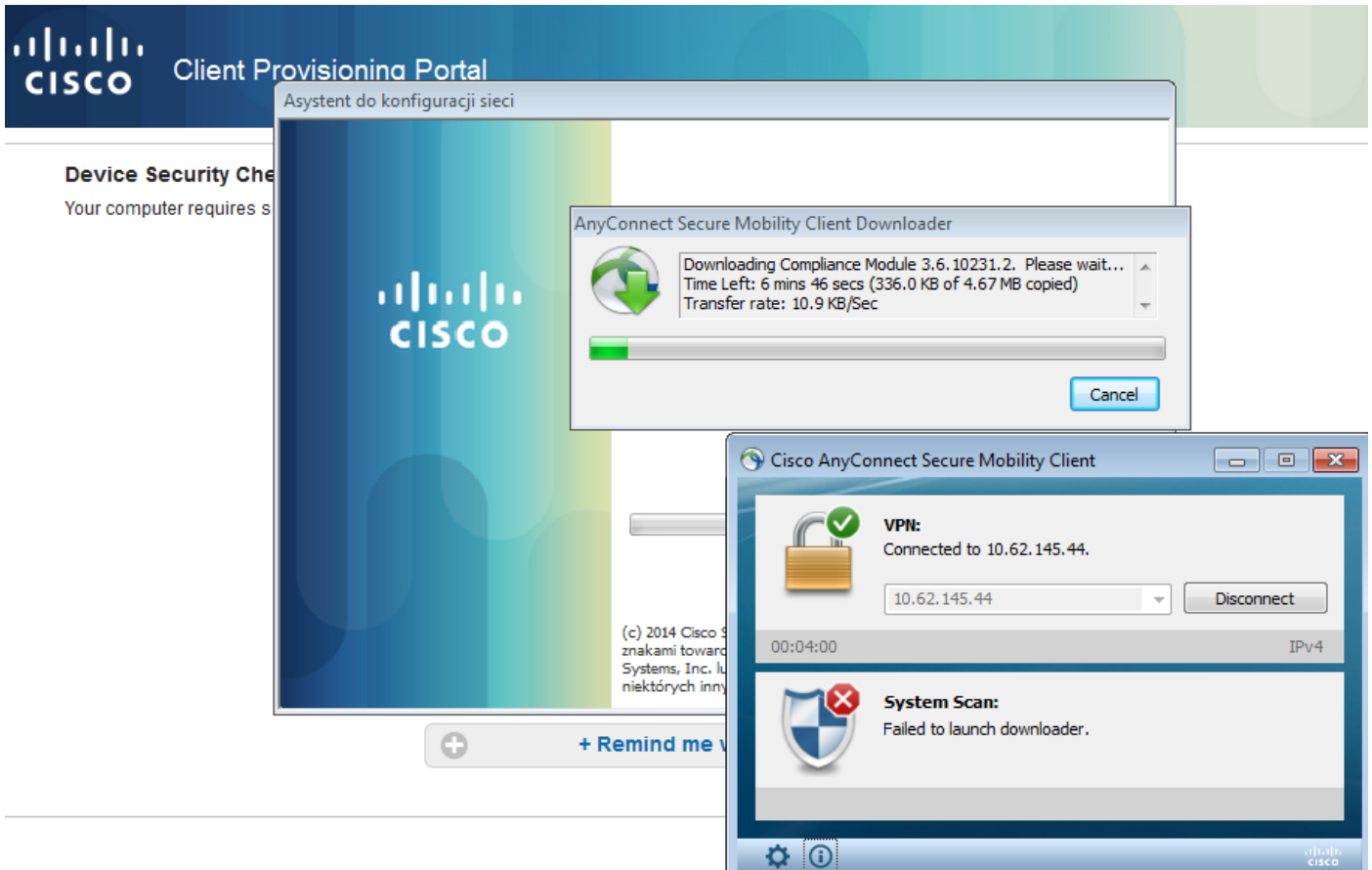
Redirect URL : <https://mgarcarz-ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-00505...>
Redirect ACL : REDIRECT

Étape 2. Ravitaillement de client

À cette étape, le trafic de navigateur Web de point final est réorienté à ISE pour le ravitaillement de client suivant les indications de l'image.

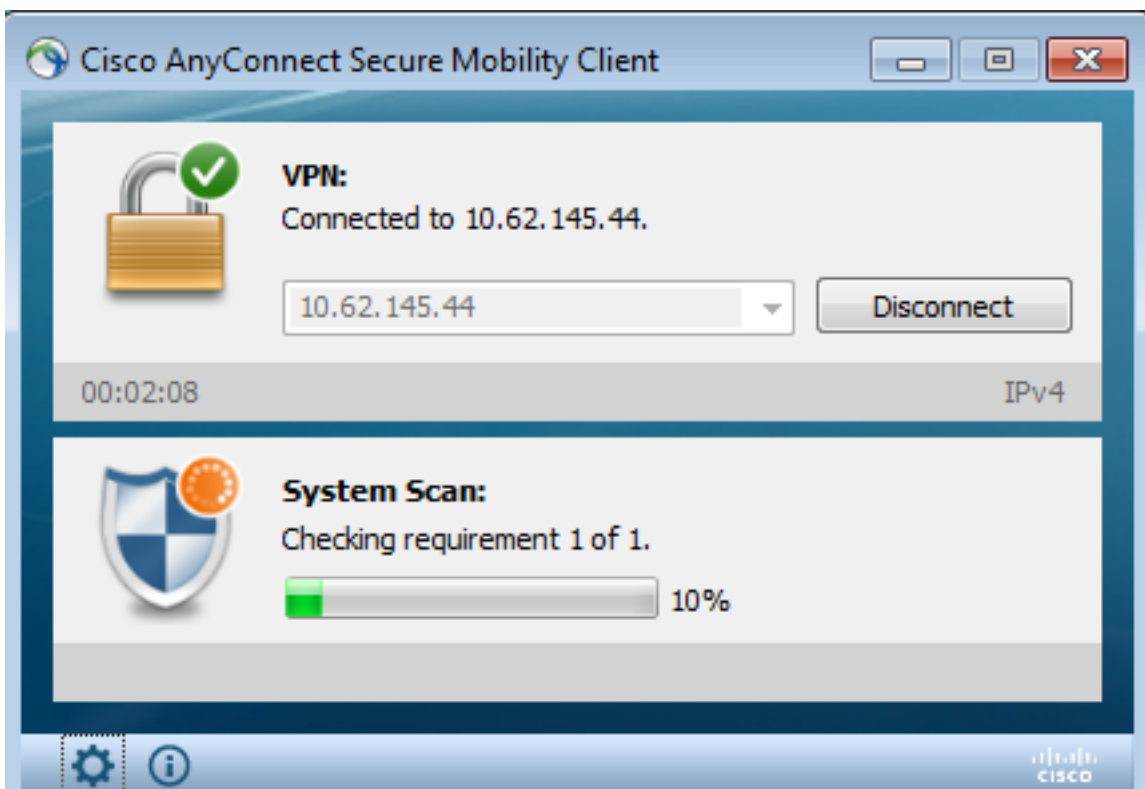


Si nécessaire, AnyConnect avec la posture et le module de conformité est mis à jour suivant les indications de l'image.



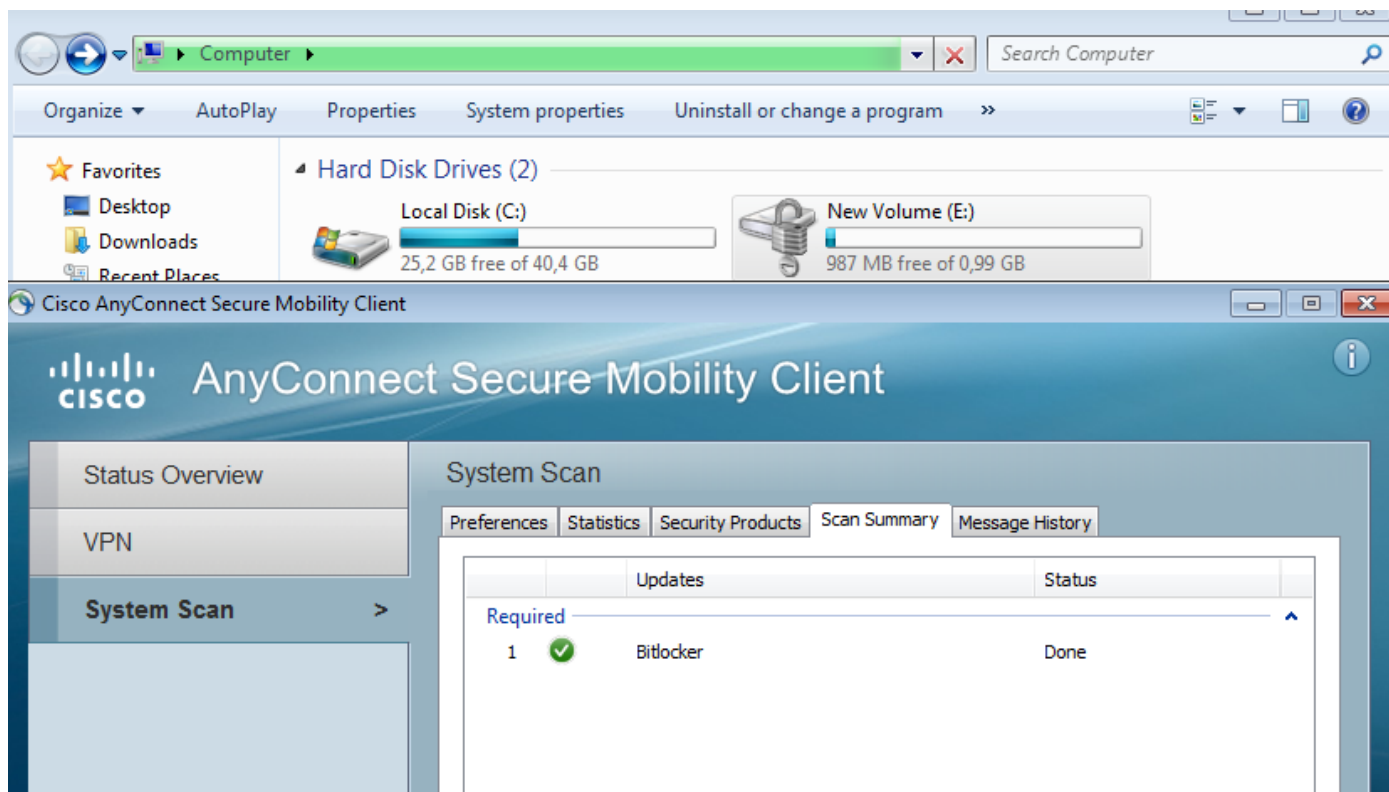
Étape 3. Contrôle de posture et CoA

Le module de posture est exécuté, découvre ISE (il pourrait exiger d'avoir l'enregistrement des DN A pour enroll.cisco.com afin de réussir), télécharge et vérifie des états de posture suivant les indications de l'image.

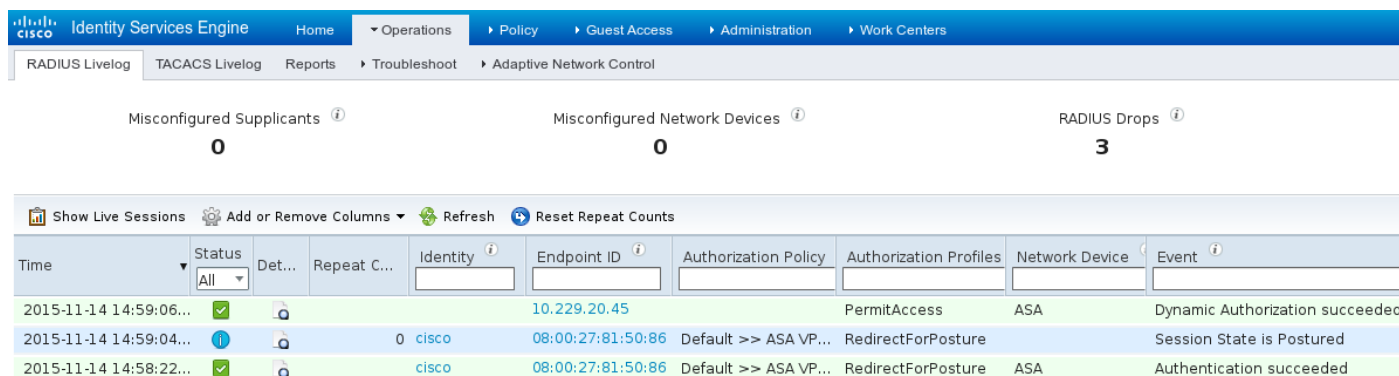


Une fois qu'on le confirme qu'E : la partition est entièrement chiffrée par BitLocker, l'état correct

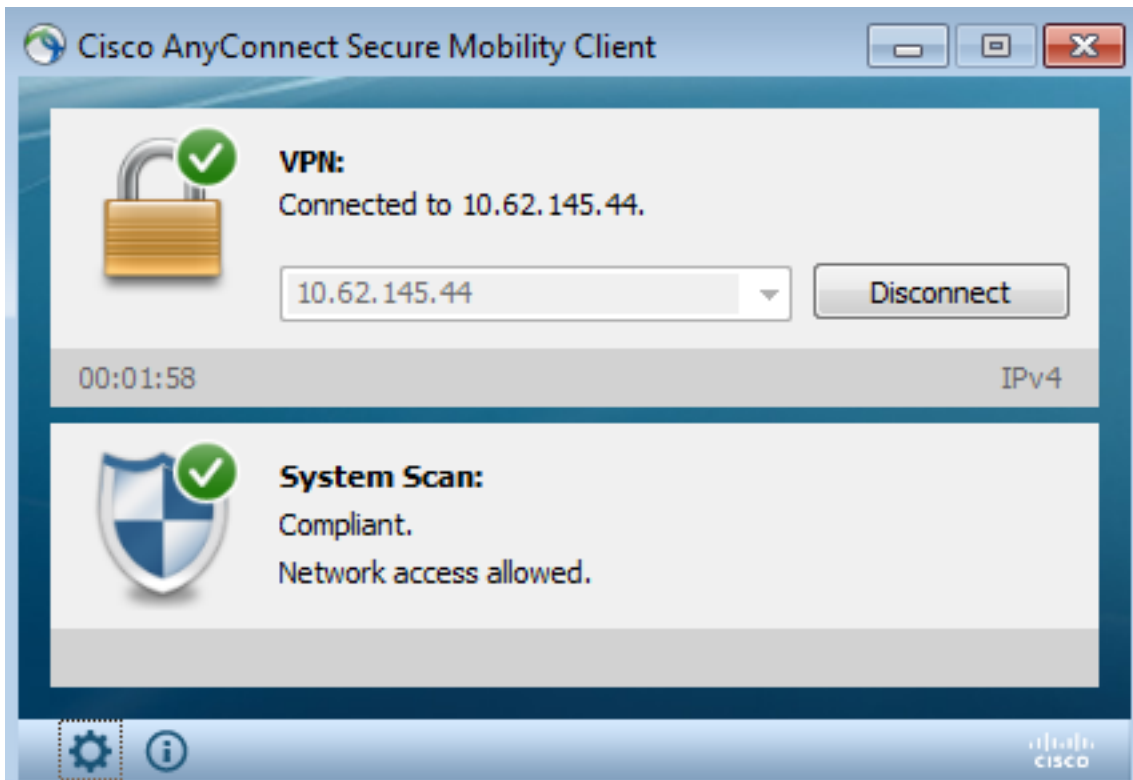
est envoyée à ISE suivant les indications de l'image.



Ceci déclenche le CoA pour reauthorize la session VPN, suivant les indications de l'image.



L'ASA retire l'ACL de redirection qui fournit l'accès complet. AnyConnect signale la conformité suivant les indications de l'image.



En outre, les rapports détaillés sur ISE peuvent confirmer que les deux conditions sont satisfaites (l'estimation de posture par condition est le nouvel état ISE 2.0 qui affiche chaque condition). Le premier état (`hd_inst_BitLockerDriveEncryption_6_x`) vérifie l'installation/processus, second les contrôles (`hd_loc_bitlocker_specific_1`) si l'emplacement spécifique (E :) est entièrement chiffré suivant les indications de l'image.

Report Selector	Posture Assessment by Condition									
Report Selector Favorites ISE Reports Audit (10 reports) Device Administration (4 reports) Diagnostics (10 reports) Endpoints and Users Authentication Summary Client Provisioning Current Active Sessions External Mobile Device Management Identity Mapping Manual Certificate Provisioning Posture Assessment by Condition (Filters) * Time Range: Today Run Posture Assessment by Endpoint	From 11/14/2015 12:00:00 AM to 11/14/2015 02:59:15 PM									
	Logged At	Postur	Identity	Endpoint ID	IP Address	Endpoint OS	Policy	Enforcement	Condition Status	Condition name
	2015-11-14 14:59:04.8	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_loc_bitlocker_specific_1
	2015-11-14 14:59:04.8	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:42:25.7	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:42:25.7	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_1
	2015-11-14 14:38:46.1	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_2
	2015-11-14 14:35:32.3	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:35:32.3	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1
	2015-11-14 14:32:07.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:32:07.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1

L'estimation de posture ISE par état de point final confirme que toutes les conditions sont satisfaites, suivant les indications de l'image.

Posture More Detail Assessment

Time Range: From 11/14/2015 12:00:00 AM to 11/14/2015 11:42:08 PM
Generated At: 2015-11-14 23:42:08.257

Client Details

Username:	cisco
Mac Address:	08:00:27:81:50:86
IP address:	10.62.145.44
Session ID:	c0a801010001700056473ebe
Client Operating System:	Windows 7 Ultimate 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.2.00096
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-KOMPUTER
System Domain:	n/a
System User:	admin
User Domain:	admin-Komputer
AV Installed:	
AS Installed:	Windows Defender;6.1.7600.16385;1.141.3676.0;01/11/2013;

Posture Report

Posture Status:	Compliant
Logged At:	2015-11-14 14:59:04.827

Les mêmes peuvent être confirmés d'ise-psc.log mettent au point. Posez la demande reçue par ISE et la réponse :

```
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][  
cisco.cpm.posture.runtime.PostureHandlerImpl -::c0a801010001700056473ebe::- Received posture  
request [parameters: reqtype=validate, userip=10.62.145.44, clientmac=08-00-27-81-50-86,  
os=WINDOWS, osVerison=1.2.1.6.1.1, architecture=9, provider=Device Filter, state=, ops=1,  
avpid=, avvname=Microsoft Corp.:!::!::!, avpname=Windows Defender:!::!::!,  
avpversion=6.1.7600.16385:!::!::!, avpfeature=AS:!::!::!, userAgent=Mozilla/4.0 (compatible;  
WINDOWS; 1.2.1.6.1.1; AnyConnect Posture Agent v.4.2.00096), session_id=c0a801010001700056473ebe  
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][  
cisco.cpm.posture.runtime.PostureHandlerImpl -::cisco:c0a801010001700056473ebe::- Creating a new  
session info for mac 08-00-27-81-50-86  
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][  
cisco.cpm.posture.runtime.PostureHandlerImpl -::cisco:c0a801010001700056473ebe::- Turning on  
enryption for endpoint with mac 08-00-27-81-50-86 and os WINDOWS, osVersion=1.2.1.6.1.1
```

```
2015-11-14 14:59:01,974 DEBUG [portal-http-service28][[]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco:c0a801010001700056473ebe::- Agent criteria
for rule [Name=bitlocker, Description=, Operating Systems=[Windows All],
Vendor=com.cisco.cpm.posture.edf.AVASVendor@96b084e, Check Type=Installation, Allow older def
date=0, Days Allowed=Undefined, Product Name=[com.cisco.cpm.posture.edf.AVASProduct@44870fea]] -
( ( (hd_inst_BitLockerDriveEncryption_6_x) ) & (hd_loc_bitlocker_specific_1) )
```

La réponse avec la condition requise de posture (condition + correction) est dans le format XML :

```
2015-11-14 14:59:02,052 DEBUG [portal-http-service28][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
<version>2</version>
<encryption>0</encryption>
<package>
<id>10</id>
<name>Bitlocker</name>
<version/>
<description>Bitlocker encryption not enabled on the endpoint. Station not
compliant.</description>
<type>3</type>
<optional>0</optional>
<action>3</action>
<check>
<id>hd_loc_bitlocker_specific_1</id>
<category>10</category>
<type>1002</type>
<param>180</param>
<path>E:</path>
<value>full</value>
<value_type>2</value_type>
</check>
<check>
<id>hd_inst_BitLockerDriveEncryption_6_x</id>
<category>10</category>
<type>1001</type>
<param>180</param>
<operation>regex match</operation>
<value>^6\..+$|^6$</value>
<value_type>3</value_type>
</check>
<criteria>( ( (hd_inst_BitLockerDriveEncryption_6_x) ) &
(hd_loc_bitlocker_specific_1) )</criteria>
</package>
</cleanmachines>
```

Après état chiffré est reçu par ISE :

```
2015-11-14 14:59:04,816 DEBUG [portal-http-service28][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypting
report
2015-11-14 14:59:04,817 DEBUG [portal-http-service28][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypted
report []
<report><version>1000</version><encryption>0</encryption><key></key><os_type>WINDOWS</os_type><os
sversion>1.2.1.6.1.1</osversion><build_number>7600</build_number><architecture>9</architecture><
user_name>[device-filter-AC]</user_name><agent>x.y.z.d-todo</agent><sys_name>ADMIN-
KOMPUTER</sys_name><sys_user>admin</sys_user><sys_domain>n/a</sys_domain><sys_user_domain>admin-
Komputer</sys_user_domain><av><av_vendor_name>Microsoft
Corp.</av_vendor_name><av_prod_name>Windows
```

```
Defender</av_prod_name><av_prod_version>6.1.7600.16385</av_prod_version><av_def_version>1.141.36
76.0</av_def_version><av_def_date>01/11/2013</av_def_date><av_prod_features>AS</av_prod_features
></av><package><id>10</id><status>1</status><check><chk_id>hd_loc_bitlocker_specific_1</chk_id><
chk_status>1</chk_status></check><check><chk_id>hd_inst_BitLockerDriveEncryption_6_x</chk_id><ch
k_status>1</chk_status></check></package></report> ]]
```

La station est marquée en tant que conforme et ISE envoie le CoA :

```
2015-11-14 14:59:04,823 INFO [portal-http-service28][[]
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a801010001700056473ebe::- Posture state is
compliant for endpoint with mac 08-00-27-81-50-86
2015-11-14 14:59:06,825 DEBUG [pool-5399-thread-1][[] cisco.cpm.posture.runtime.PostureCoA -
:cisco:c0a801010000f0005647358b::- Posture CoA is triggered for endpoint [08-00-27-81-50-86]
with session [c0a801010001700056473ebe
```

En outre, la configuration finale est envoyée par ISE :

```
2015-11-14 14:59:04,823 INFO [portal-http-service28][[]
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a801010001700056473ebe::- Posture state is
compliant for endpoint with mac 08-00-27-81-50-86
2015-11-14 14:59:06,825 DEBUG [pool-5399-thread-1][[] cisco.cpm.posture.runtime.PostureCoA -
:cisco:c0a801010000f0005647358b::- Posture CoA is triggered for endpoint [08-00-27-81-50-86]
with session [c0a801010001700056473ebe
```

Ces étapes peuvent être également confirmées du côté client (DART d'AnyConnect) :

```
Date       : 11/14/2015
Time       : 14:58:41
Type      : Warning
Source    : acvpnu
```

```
Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344
No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[Scanning system ... ]
```

```
Date       : 11/14/2015
Time       : 14:58:43
Type      : Warning
Source    : acvpnu
```

```
Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344
No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[Checking requirement 1 of 1. ]
```

```
Date       : 11/14/2015
Time       : 14:58:46
Type      : Warning
Source    : acvpnu
```

```
Description : Function: CNAcApiShim::PostureNotification
File: .\NacShim.cpp
Line: 461
Clearing Posture List.
```


Pour la session réussie, **rapports de historique de balayage/message de système d'AnyConnect UI** :

```
14:41:59    Searching for policy server.
14:42:03    Checking for product updates...
14:42:03    The AnyConnect Downloader is performing update checks...
14:42:04    Checking for profile updates...
14:42:04    Checking for product updates...
14:42:04    Checking for customization updates...
14:42:04    Performing any required updates...
14:42:04    The AnyConnect Downloader updates have been completed.
14:42:03    Update complete.
14:42:03    Scanning system ...
14:42:05    Checking requirement 1 of 1.
14:42:05    Updating network settings.
14:42:10    Compliant.
```

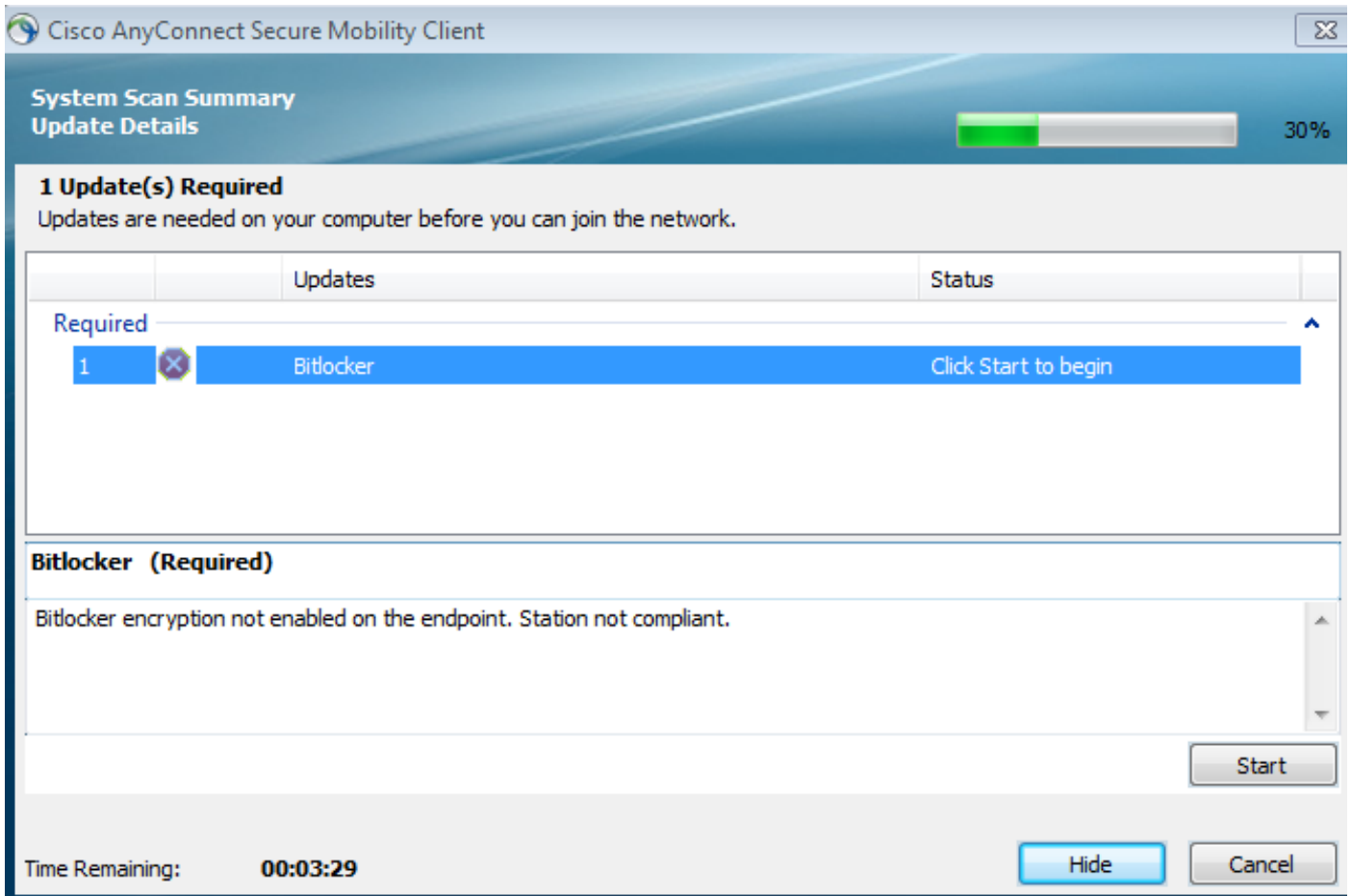
Bogues

[CSCux15941](#) - ISE 2.0 et cryptage de bitlocker de la posture AC4.2 avec manquer d'emplacement (\ de car/non pris en charge)

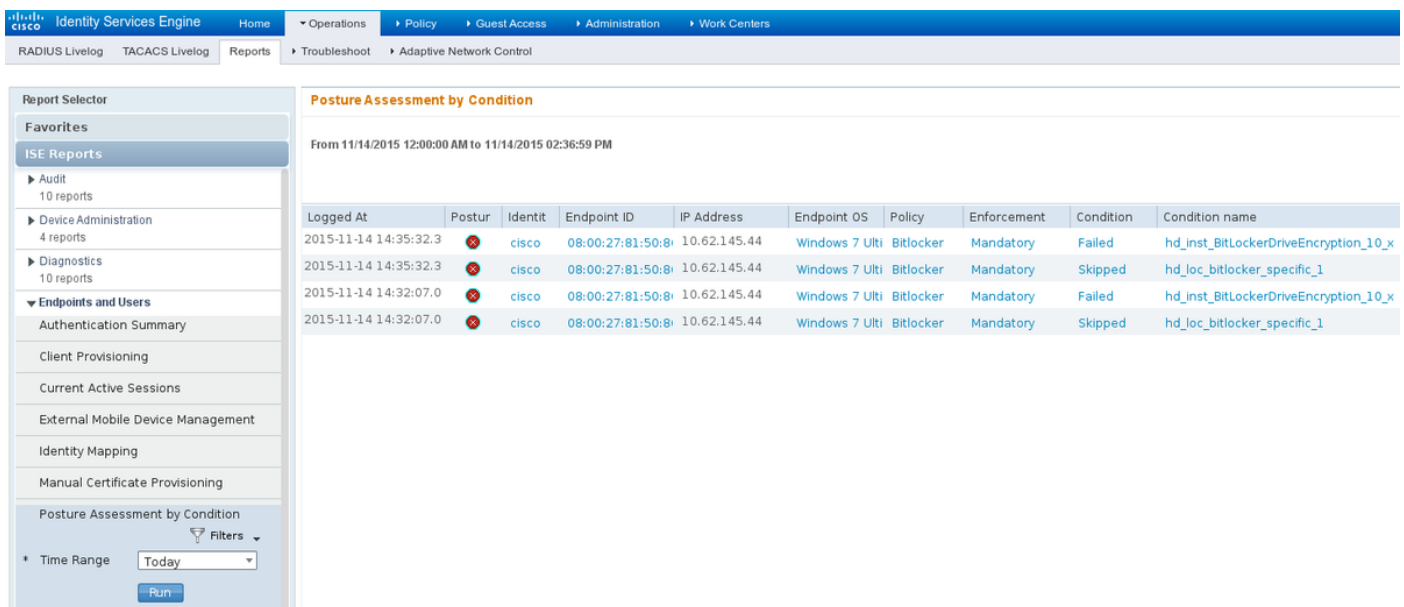
Dépanner

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si le point final est non-conforme, il est signalé par AnyConnect UI (la correction également configurée est exécutée) suivant les indications de l'image.



ISE peut fournir les détails sur les conditions manquantes, suivant les indications de l'image.



Les mêmes peuvent être vérifiés des logs CLI (les exemples de la section de logins vérifient).

Informations connexes

- [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](#)