

ISE 2.0 configureren en AnyConnect 4.2 versleutelen met bittere kluis

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[ASA](#)

[BitPoint op Windows 7](#)

[ISE](#)

[Stap 1. Netwerkapparaat](#)

[Stap 2. Postvoorwaarden en beleid](#)

[Stap 3. Resources voor clientprovisioning en -beleid](#)

[Stap 4. Vergunningsregels](#)

[Verifiëren](#)

[Stap 1. VPN-sessieinstelling](#)

[Stap 2. Clientprovisioning](#)

[Stap 3. Postcontrole en CoA](#)

[Bugs](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe de diskdeling van het eindpunt met het gebruik van Microsoft BitPluk moet worden versleuteld en hoe u Cisco Identity Services Engine (ISE) moet configureren om volledige toegang tot het netwerk te bieden, alleen wanneer de juiste encryptie is geconfigureerd. Cisco ISE versie 2.0 ondersteunt, samen met AnyConnect Secure Mobility Client 4.2, de positie voor diskencryptie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van adaptieve security applicatie (ASA) CLI en Secure Socket Layer (SSL) VPN
- VPN-configuratie voor externe toegang op ASA
- ISE- en posterijen

Gebruikte componenten

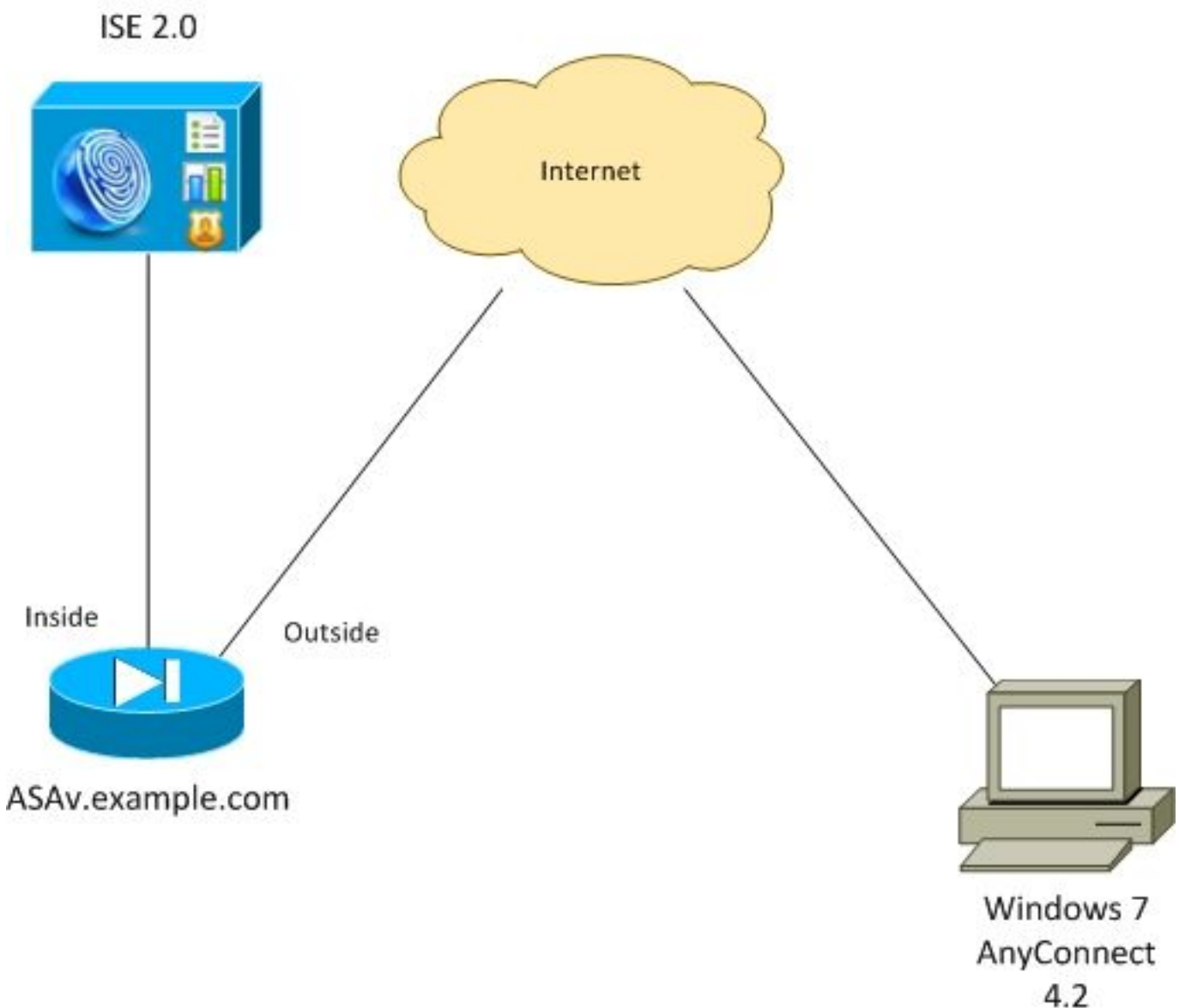
De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco ASA-software-releases 9.2.1 en hoger
- Microsoft Windows versie 7 met Cisco AnyConnect Secure Mobility Client versie 4.2 en hoger
- Cisco ISE, release 2.0 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Netwerkdigram



De stroom is als volgt:

- VPN-sessie gestart door AnyConnect-client is authentiek via ISE. De status van het eindpunt

is niet bekend, regel **ASA VPN onbekend** wordt geraakt en als resultaat hiervan wordt de sessie voor provisioning naar ISE omgeleid

- Gebruiker opent webbrowser, HTTP-verkeer wordt door ASA naar ISE omgeleid. ISE duwt de nieuwste versie van AnyConnect samen met de opstelling en module voor overeenstemming naar het eindpunt
- Zodra de posteringsmodule is uitgevoerd, controleert het of de verdeling **E**: volledig versleuteld met BitPluk. Zo ja, dan wordt het rapport naar ISE gestuurd, dat Radius Change of Authorisation (CoA) zonder enige ACL (volledige toegang) in werking stelt
- VPN-sessie over ASA wordt bijgewerkt, ACL-omleiding wordt verwijderd en volledige toegang voor de sessie

De zitting van VPN wordt als voorbeeld gepresenteerd. De postfunctie werkt ook goed voor andere typen toegang.

ASA

Het wordt ingesteld vanaf een externe SSL VPN-toegang met behulp van ISE als AAA-server (Verificatie, autorisatie en accounting). Radius CoA moet samen met REDIRECT ACL worden geconfigureerd:

```
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

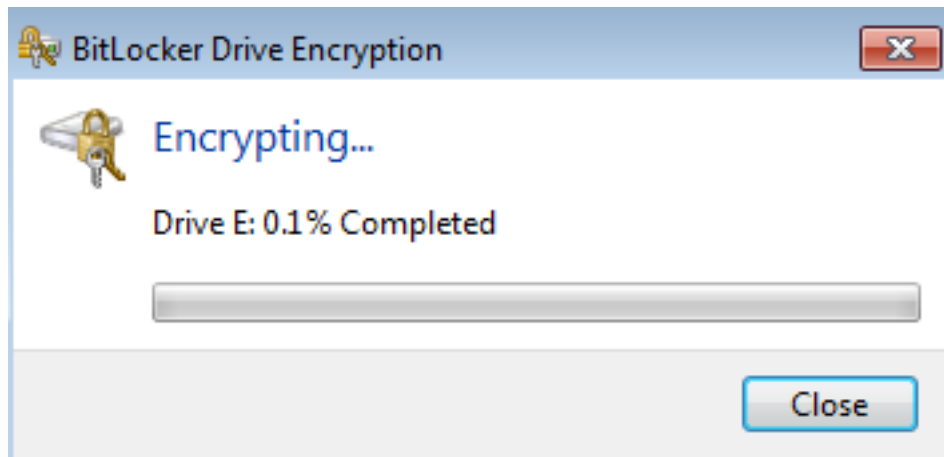
access-list REDIRECT extended deny udp any any eq domain
access-list REDIRECT extended deny ip any host 10.48.17.235
access-list REDIRECT extended deny icmp any any
access-list REDIRECT extended permit tcp any any eq www

ip local pool POOL 172.16.31.10-172.16.31.20 mask 255.255.255.0
```

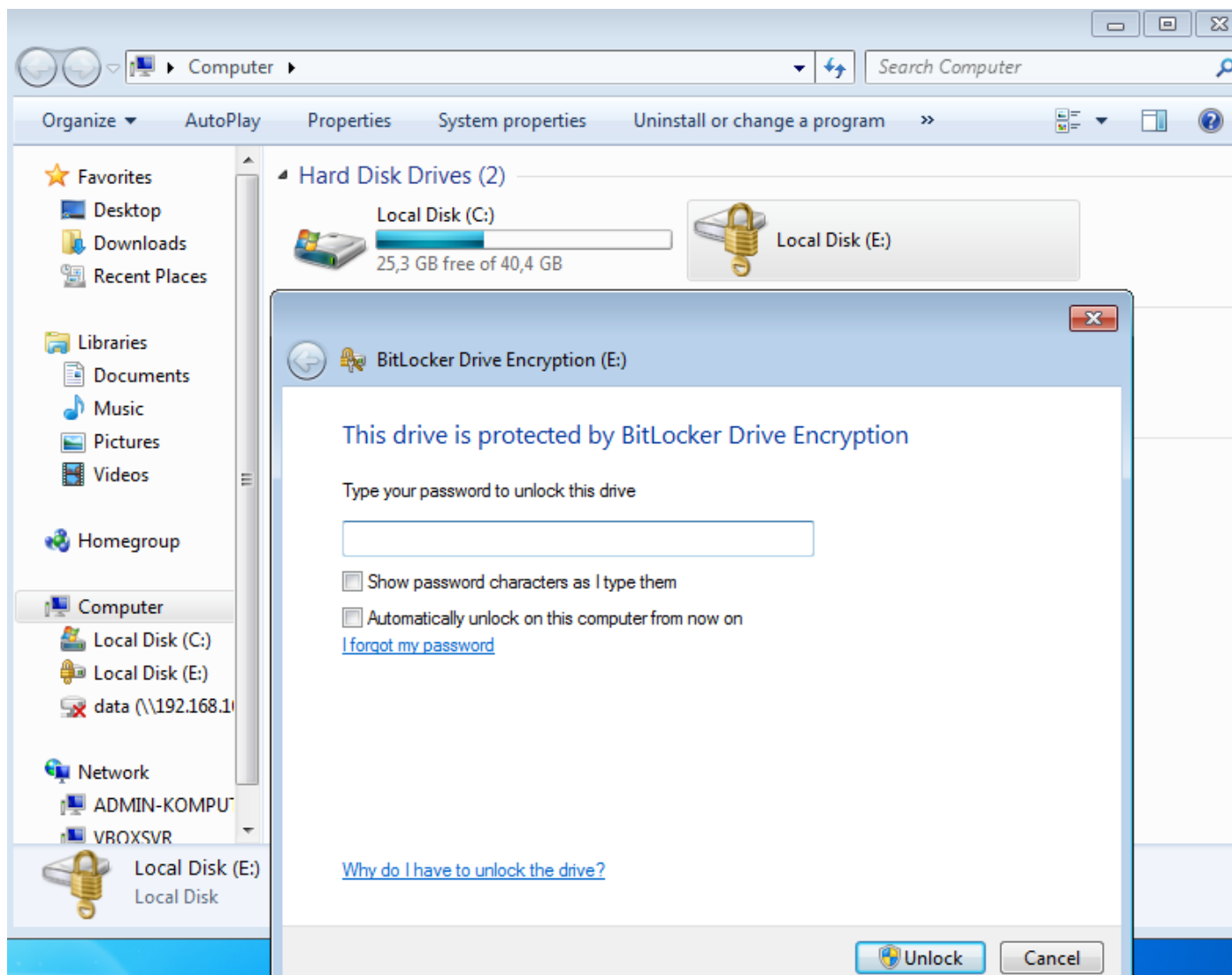
Zie voor meer informatie:

BitPoint op Windows 7

Navigatie naar **Control Panel > System and Security > BitPoint Drive-encryptie**, schakelt **E** in: partitieencryptie. Bescherm het met een wachtwoord (PIN), zoals in de afbeelding weergegeven.



Nadat het is versleuteld kunt u het wachtwoord monteren (met het wachtwoord) en ervoor zorgen dat het toegankelijk is zoals in de afbeelding.



Raadpleeg de documentatie bij Microsoft voor meer informatie:

[Stap 1000-encryptie voor Windows-bit-luis](#)

ISE

Stap 1. Netwerkapparaat

Navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**, voeg **ASA** toe met **apparaattype = ASA**. Dit wordt gebruikt als voorwaarde in de vergunningsregels, maar is niet verplicht (er kunnen andere soorten voorwaarden worden gebruikt).

Indien van toepassing, bestaat de Netwerkapparaatgroep niet. Om te creëren, navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaatgroepen**.

Stap 2. Postvoorwaarden en beleid

Zorg ervoor dat de posteringsomstandigheden worden bijgewerkt: Navigeer naar **Administratie > Systeem > Instellingen > Posture > Update nu**.

Navigeer naar **beleid > Beleidselementen > Voorwaarden > Posture > Disc Encryption Condition**, voeg een nieuwe voorwaarde toe zoals in de afbeelding.

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. The left sidebar shows the navigation menu with "Posture" expanded and "Disk Encryption Condition" selected. The main content 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 that, a "Location" dropdown is set to "Specific Locatio" and a text field "E:" is empty. The status is "is Fully Encrypted OR" followed by "Pending Encryption OR" and "Partially Encrypted".

Deze conditie controleert of Bitmelding voor Windows 7 is geïnstalleerd en of **E:** de scheiding is

volledig versleuteld .

Opmerking: BitHub is een encryptie van het diskniveau en het steunt geen Specifieke Plaats met het argument, slechts de schijfbrief.

Navigeer naar **Beleids-elementen > Resultaten > Posture > Vereisten** om een nieuw vereiste te creëren dat de conditie zoals in de afbeelding gebruikt.

The screenshot shows the Cisco ISE interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. Under 'Posture', there is a 'Remediation Actions' section with a 'Requirements' link. The 'Requirements' table is displayed with the following data:

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

Navigeren in **Policy > Posture**, voeg een voorwaarde voor alle Windows toe om het vereiste te gebruiken zoals in de afbeelding wordt weergegeven.

The screenshot shows the 'Posture Policy' configuration page in Cisco ISE. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. Under 'Posture', there is a 'Policy Elements' section. The 'Posture Policy' page has a sub-header 'Define the Posture Policy by configuring rules based on operating system and/or other conditions.' Below this is a table with the following data:

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Bitlocker	If Any	and Windows All		then Bitlocker

Stap 3. Resources voor clientprovisioning en -beleid

Navigeer naar **Policy > Policy Elementen > Client Provisioning > Resources**, download van Cisco.com en handmatig uploaden van **AnyConnect 4.2-pakket** zoals in de afbeelding getoond.

Resources

The screenshot shows the 'Resources' table in Cisco ISE. The table has columns for Name, Type, Version, Last Update, and Description. The following resources are listed:

Name	Type	Version	Last Update	Description
MacOsXSPWizard 1.0.0.36	MacOsXSPWizard	1.0.0.36	2015/10/08 09:24:15	ISE 2.0 Supplicant Provisioning ...
WinSPWizard 1.0.0.43	WinSPWizard	1.0.0.43	2015/10/29 17:15:02	Supplicant Provisioning Wizard f...
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 ...

Navigeren in **Add > NAC Agent of AnyConnect Posture Profile**, maakt AnyConnect Posture-profiel (naam: **AnyConnectPosture**) met standaardinstellingen.

Navigeren in op **Add > AnyConnect Configuration**, voegt AnyConnect-profiel toe (naam: **AnyConnect Configuration**) zoals in de afbeelding weergegeven.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements > Results > Conditions > Results. The main configuration area is titled "AnyConnect Configuration > AnyConnect Configuration".

Configuration fields include:

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

AnyConnect Module Selection

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

Profile Selection

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

Navigeer in op **Policy > Client Provisioning** en wijzig standaardbeleid voor Windows om geconfigureerd AnyConnect-profiel te gebruiken zoals in de afbeelding.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for Client Provisioning Policy. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements. The main configuration area is titled "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
<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

Stap 4. Vergunningsregels

Navigeren in **Policy > Policy Elementen > Resultaten > Vergunningsprofiel toevoegen** (naam:

RedirectForPosture) dat naar een standaard-clientprovisioningportal wordt doorgestuurd zoals in de afbeelding.

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. 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: (disabled)
- Track Movement: (disabled)

 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

REDIRECT ACL wordt gedefinieerd op ASA.

Navigeren in Policy > Authorization, maak 3 autorisatieregels zoals in de afbeelding getoond.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for the 'Authorization Policy' page. 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' with the value '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

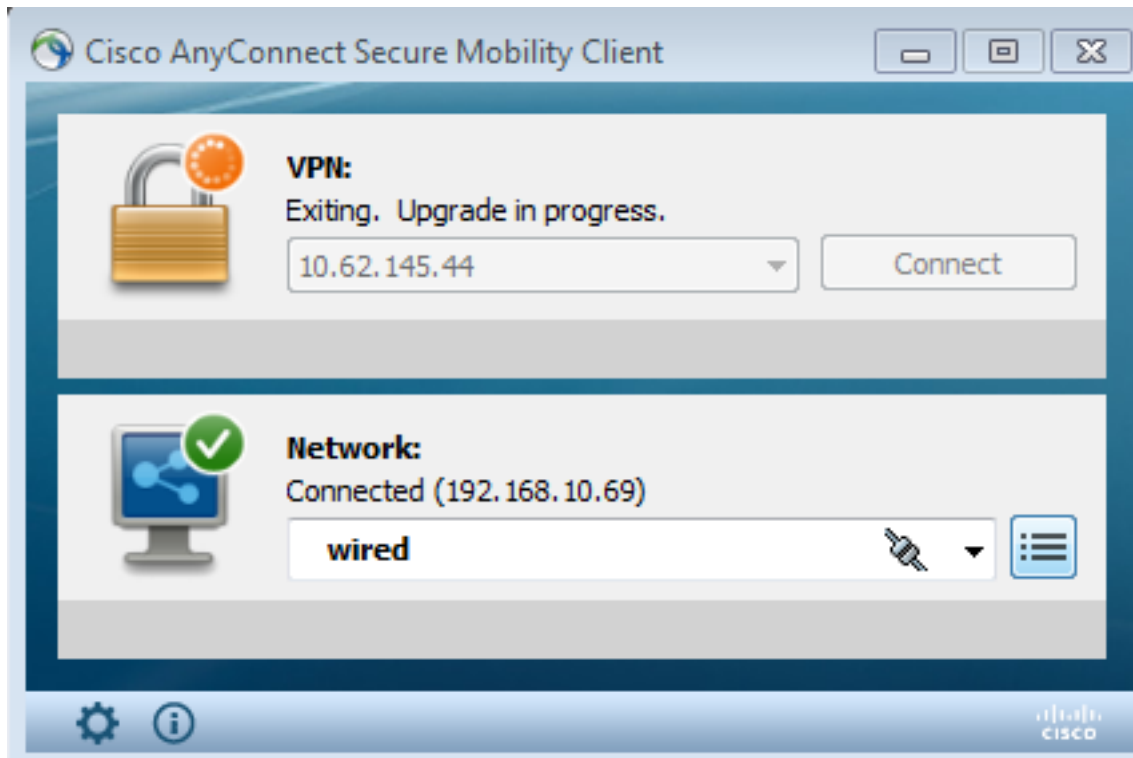
Als het eindpunt compatibel is, wordt volledige toegang verleend. Als de status onbekend of niet-conform is, wordt de omleiding voor Clientprovisioning teruggegeven.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Stap 1. VPN-sessieinstelling

Nadat de VPN-sessie is ingesteld, kan ASA een upgrade willen uitvoeren van AnyConnect-modules zoals in de afbeelding.



Op ISE wordt de laatste regel ingedrukt, zodat de toestemming **RedirectForPosture** wordt teruggegeven zoals in de afbeelding wordt getoond.

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		Session State is Postured
2015-11-14 14:58:22...	✓			cisco	08:00:27:81:50:86	Default >> ASA VP...	RedirectForPosture	ASA	Authentication succeeded

Nadat ASA klaar is met het bouwen van de VPN-sessie, meldt het dat omleiding moet plaatsvinden:

```
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
```

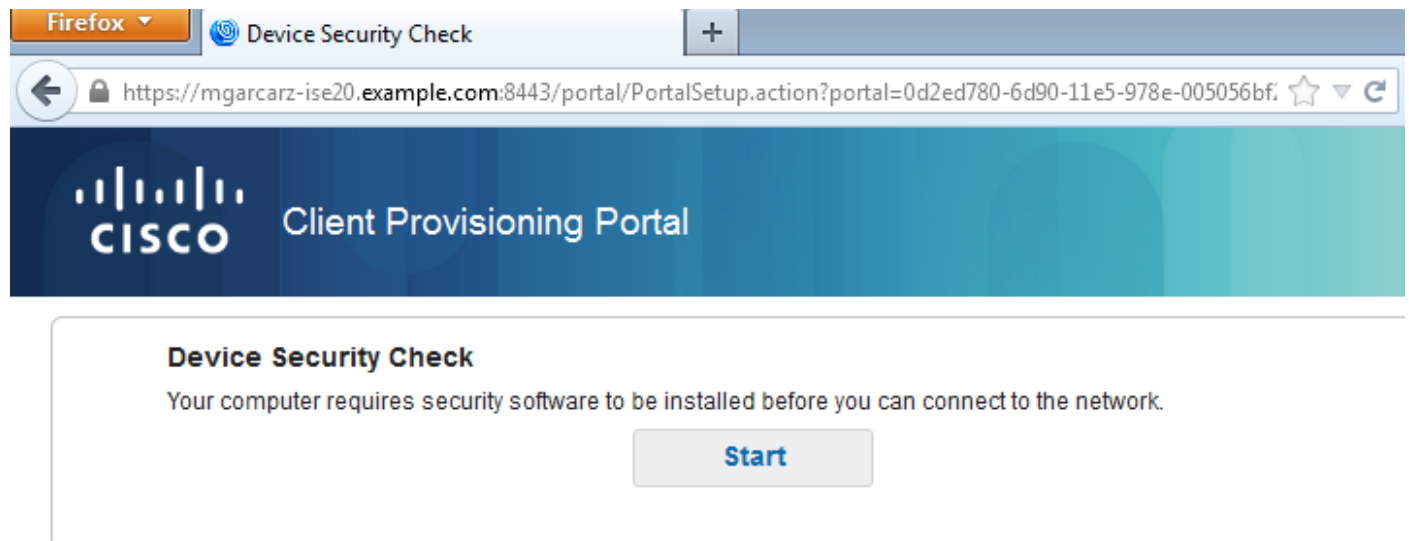
<some output omitted for clarity>

ISE Posture:

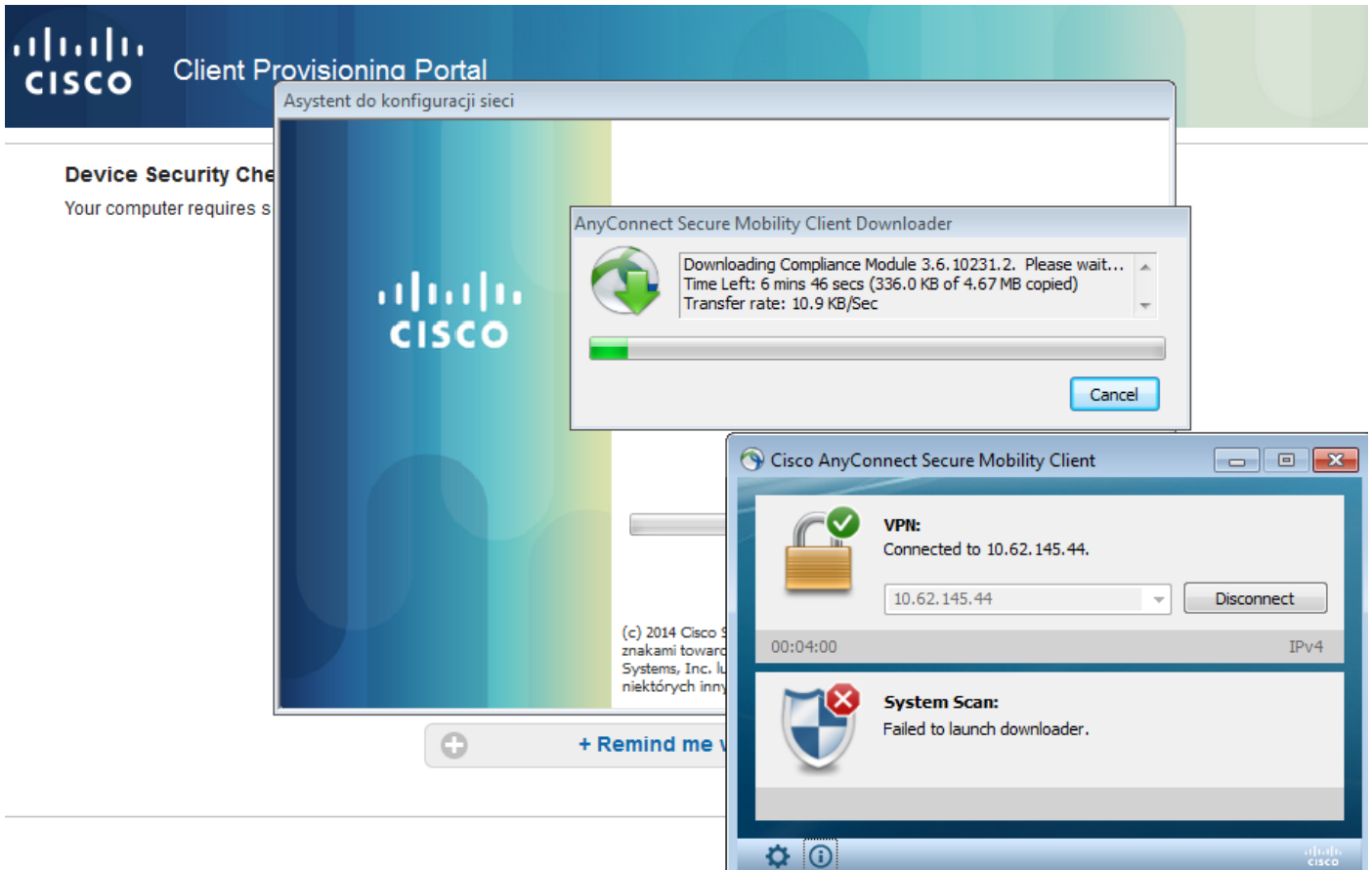
Redirect URL : <https://mgarcarz-ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-005056bf...>
Redirect ACL : REDIRECT

Stap 2. Clientprovisioning

In dat stadium wordt het internetverkeer van endpoints opnieuw naar ISE gericht voor clientprovisioning zoals in de afbeelding.

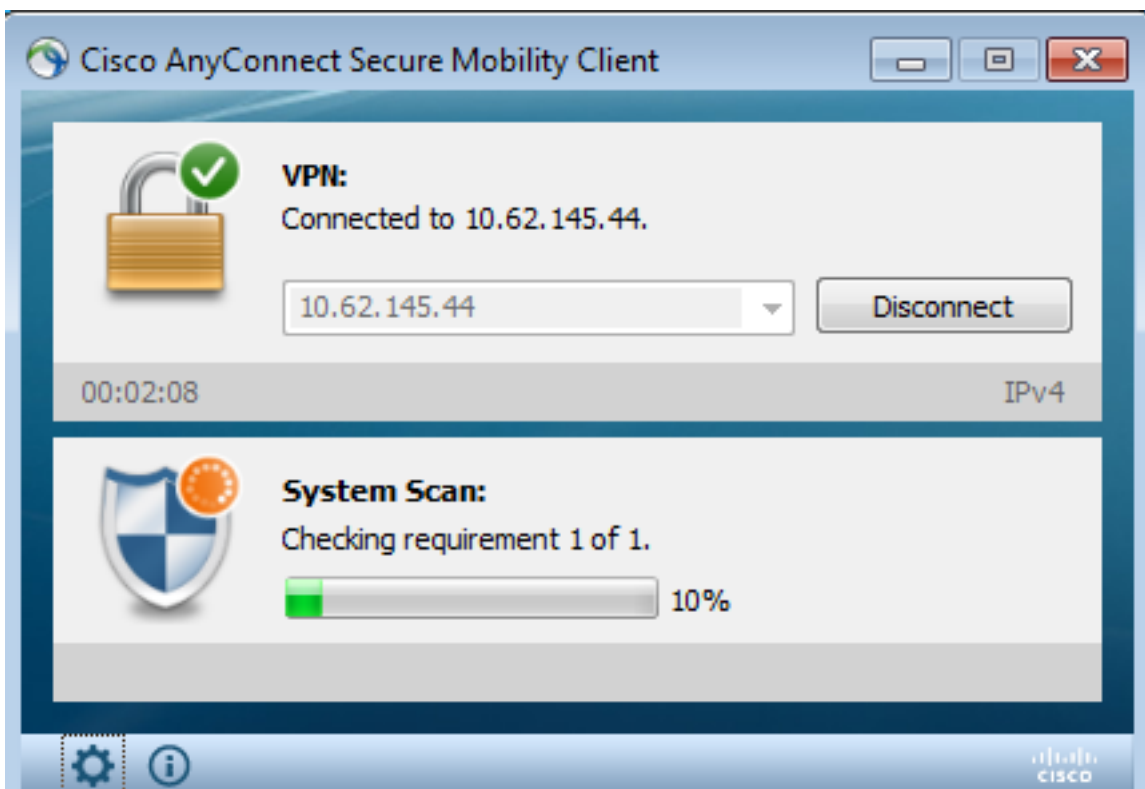


Indien nodig wordt AnyConnect met Posture en de nalevingsmodule bijgewerkt zoals in de afbeelding wordt getoond.



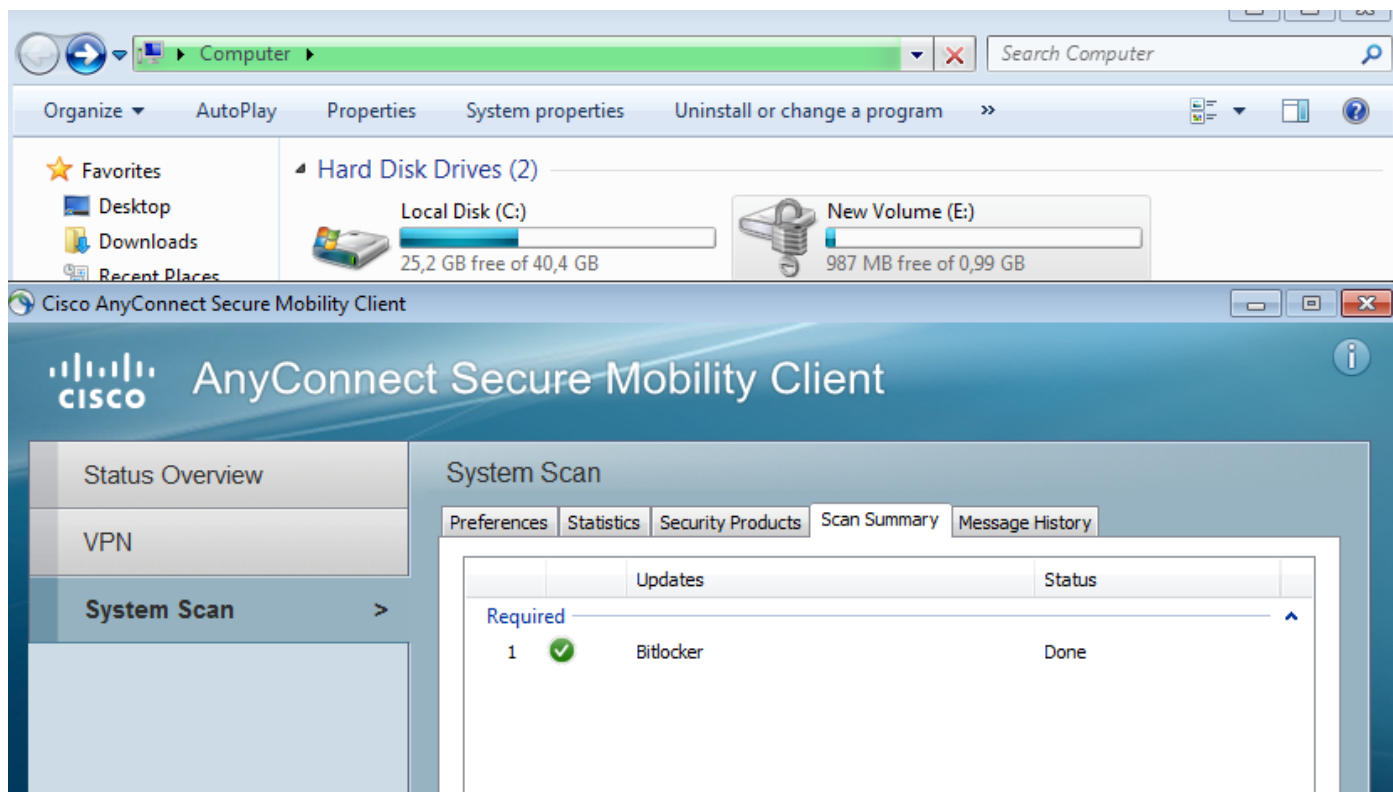
Stap 3. Postcontrole en CoA

Postmodule wordt uitgevoerd, ontdekt ISE (het kan nodig zijn om DNS A record voor enroll.cisco.com te hebben om te slagen), download en controleer postvoorwaarden zoals in de afbeelding weergegeven.

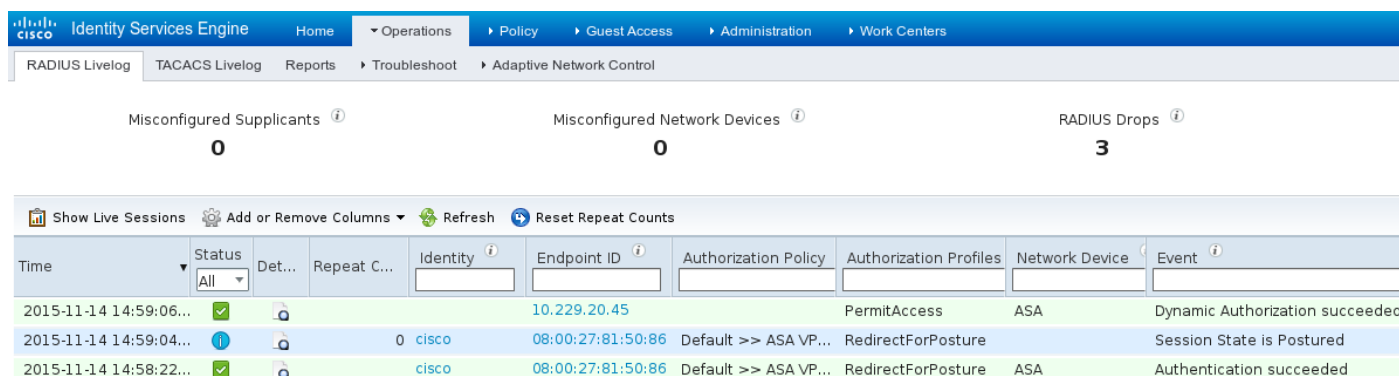


Zodra bevestigd is dat E: De verdeling wordt volledig gecodeerd door Bitmelding, het juiste rapport

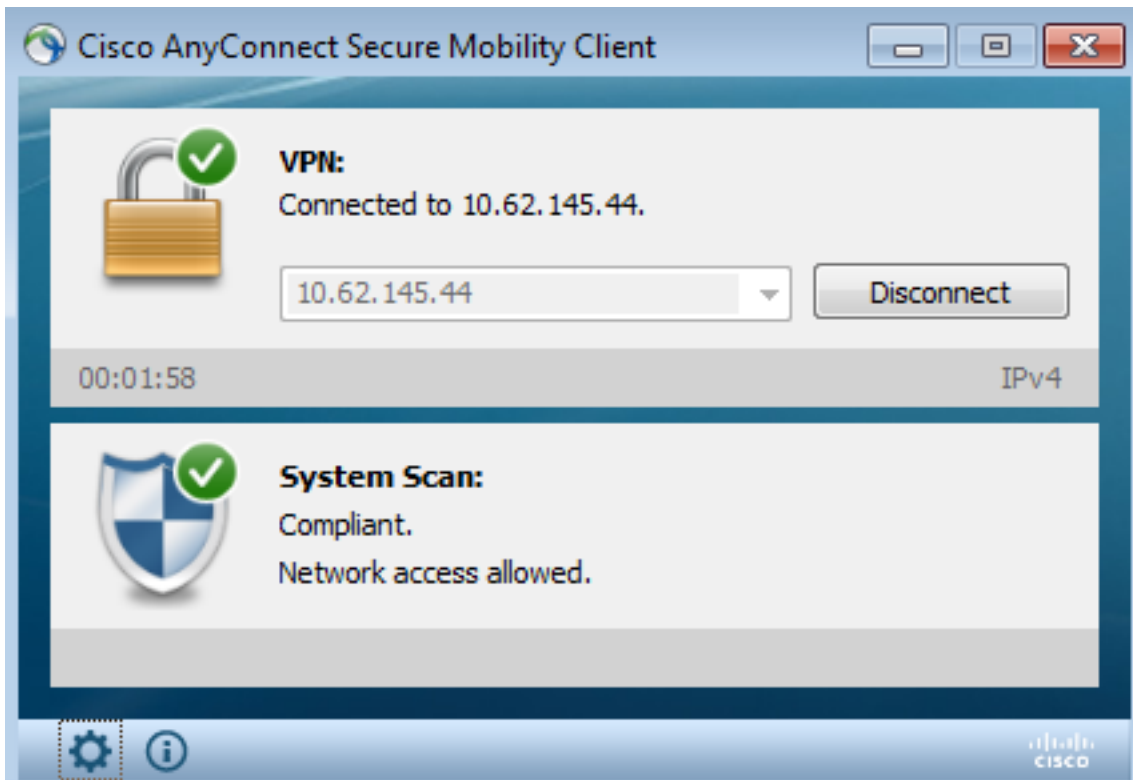
wordt naar ISE verzonden zoals in de afbeelding wordt getoond.



Hiermee wordt CoA geactiveerd om een VPN-sessie opnieuw te autoriseren, zoals in de afbeelding.



ASA verwijdert omleiding ACL die volledige toegang biedt. AnyConnect meldt overeenstemming met de afbeelding.



Bovendien kunnen gedetailleerde rapporten over ISE bevestigen dat aan beide voorwaarden is voldaan (**Posture Assessment by Condition** is het nieuwe ISE 2.0 rapport dat elke voorwaarde aantoont). De eerste conditie (**hd_Against_Bitbereidbereid**) controleert op de installatie/het proces, de tweede (**hd_loc_bitlocker_especifiek_1**) controleert of de specifieke locatie (E:) volledig versleuteld zoals in de afbeelding wordt weergegeven.

Identity Services Engine										
RADIUS Livelog TACACS Livelog Reports Troubleshoot Adaptive Network Control										
Posture Assessment by Condition										
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 14:38:46.1	✗	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 14:37:23.0	✗	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	

ISE **Posture Assessment by Endpoint** Report bevestigt dat aan alle voorwaarden is voldaan, zoals in de afbeelding te zien is.

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

Hetzelfde kan worden bevestigd bij ise-psc.log debugs. Door ISE ontvangen Postaanvraag en antwoord:

```
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  
encryption 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) )
```

De reactie op het vereiste van houding (conditie + herstel) is in XML-formaat:

```
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>
```

```
<version/>
```

```
  <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>
```

```
  <value_type>2</value_type>  
</check>  
<check>
```

```
  <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>
```

Nadat het gecodeerde rapport door ISE is ontvangen:

```
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>
```

```
</check><check><chk_id>hd_inst_BitLockerDriveEncryption_6_x</chk_id><chk_status>1</check></pack
age></report> ]]
```

Station is gemarkeerd als compatibel en ISE stuurt 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
```

De laatste configuratie wordt ook verzonden door ISE:

```
2015-11-14 14:59:04,827 DEBUG [portal-http-service28][
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Sending
response to endpoint 08-00-27-81-50-86 http response [ [ <!--X-Perfigo-DM-Error=0--><!--error=0--
><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--><!--X-Perfigo-Auto-Close-Login-
Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--><!--user role=--><!--X-Perfigo-OrigRole=--
><!--X-Perfigo-UserKey=dummykey--><!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-
Perfigo-Session=--><!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter--><!--X-
Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4--><!--X-Perfigo-DHCP-Renew-Delay=1--
><!--X-Perfigo-Client-MAC=08:00:27:81:50:86--> ]]
```

Deze stappen kunnen ook vanaf de cliëntzijde (AnyConnect DART) worden bevestigd:

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

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 : acvpnuui

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 : acvpnuui

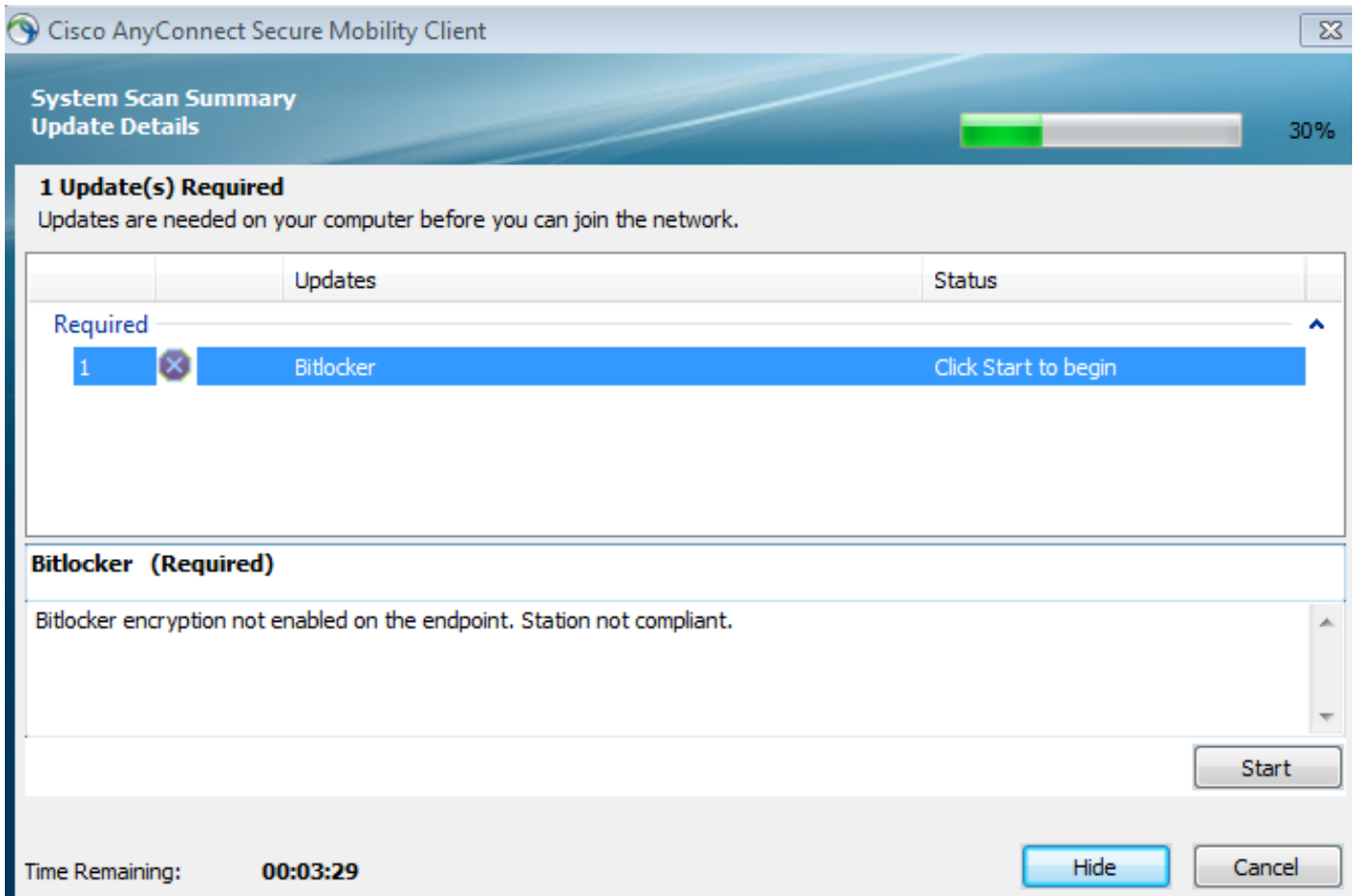
Description : Function: CMacApiShim::PostureNotification
File: .\MacShim.cpp
Line: 461

Clearing Posture List.

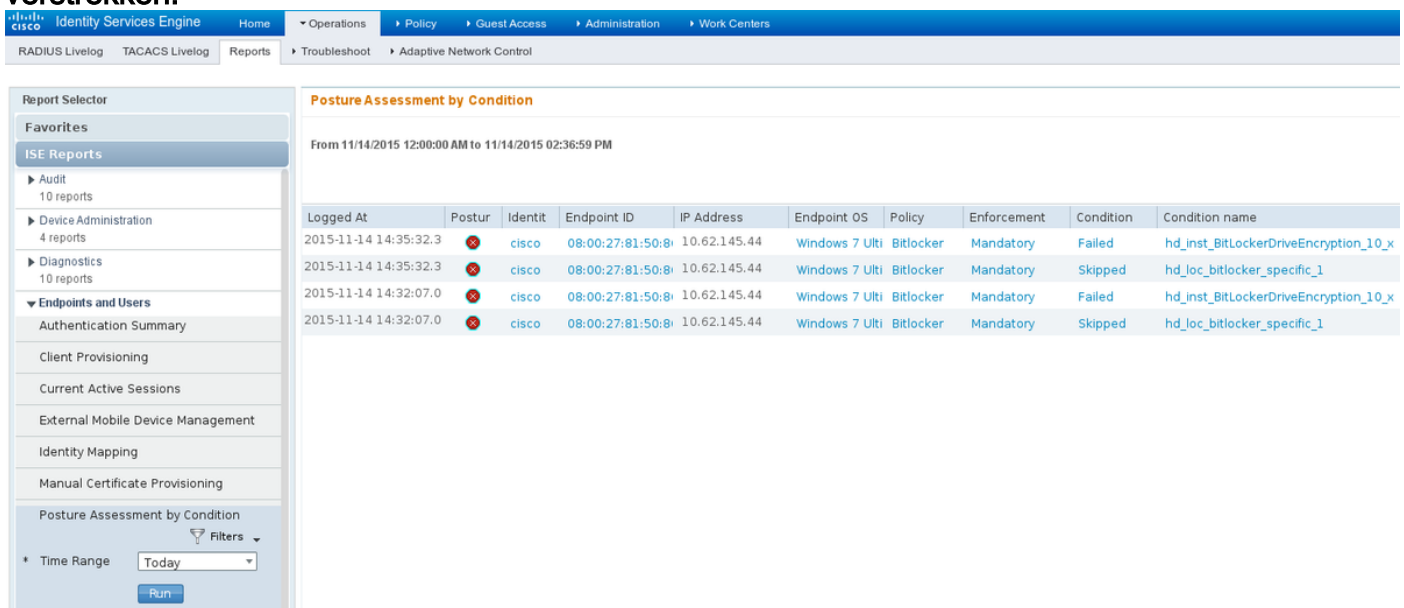
Voor een succesvolle sessie meldt AnyConnect UI-systeem Scannen/berichtengeschiedenis:

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.

Bugs[CISCOux15941](#) - ISE 2.0 en AC 4.2 posture bitlocker encryptie met locatiefalen (teken voor \ / niet ondersteund)**Problemen oplossen** Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen. Als het eindpunt niet compatibel is, wordt het gerapporteerd door AnyConnect UI (ook geconfigureerd herstel) zoals in de afbeelding.



ISE kan de gegevens over de falende omstandigheden, zoals in de afbeelding, verstrekken.



Dit kan ook worden gecontroleerd aan de hand van de CLI-logbestanden (voorbeelden van de logbestanden in sectie verify). **Gerelateerde informatie**

- [Een externe server configureren voor security applicatie, gebruikersautorisatie](#)
- [Cisco ASA Series 5000 Series VPN CLI-configuratiegids, 9.1](#)
- [Administrator-gids voor Cisco Identity Services Engine, release 2.0](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)