

Configurar ISE 2.0 e cifre a criptografia de BitLocker da postura de AnyConnect 4.2

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[ASA](#)

[BitLocker em Windows 7](#)

[ISE](#)

[Etapa 1. Dispositivo de rede](#)

[Etapa 2. Condição e políticas da postura](#)

[Etapa 3. Recursos e política do abastecimento do cliente](#)

[Etapa 4. Regras da autorização](#)

[Verificar](#)

[Etapa 1. Estabelecimento da sessão de VPN](#)

[Etapa 2. Abastecimento do cliente](#)

[Etapa 3. Verificação da postura e CoA](#)

[Erros](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este original descreve como cifrar o partição de disco do valor-limite com o uso de Microsoft BitLocker e como configurar o Cisco Identity Services Engine (ISE) a fim fornecer o acesso direto à rede, simplesmente quando a criptografia correta é configurada. A versão 2.0 de Cisco ISE junto com o cliente seguro 4.2 da mobilidade de AnyConnect suporta a postura para a criptografia do disco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de CLI da ferramenta de segurança (ASA) e configuração de VPN adaptáveis do Secure Socket Layer (SSL)
- Configuração do acesso remoto VPN no ASA
- ISE e serviços da postura

Componentes Utilizados

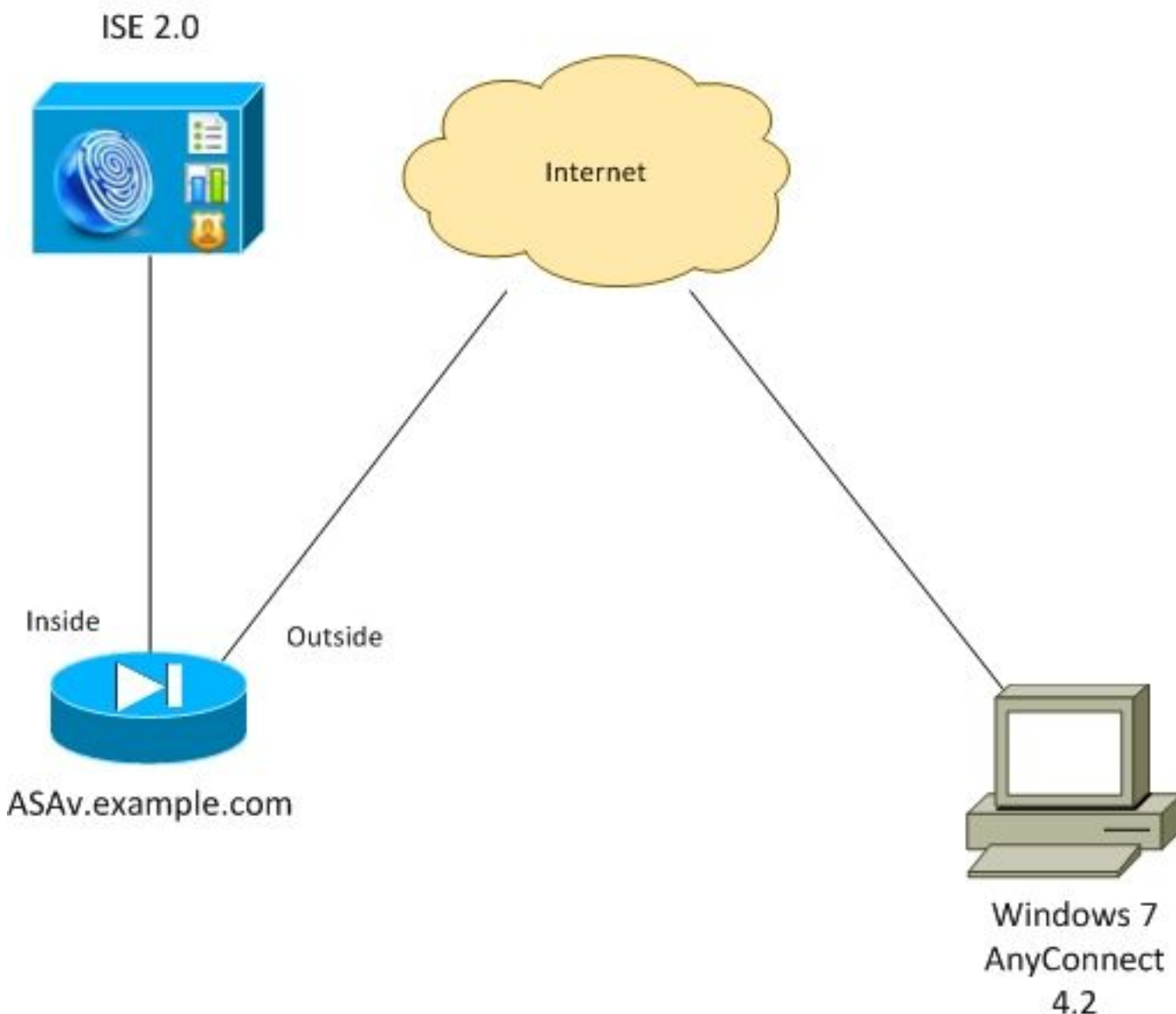
As informações neste documento são baseadas nestas versões de software:

- Versões de software 9.2.1 de Cisco ASA e mais atrasado
- Versão 7 de Microsoft Windows com versão 4.2 e mais recente do Cliente de mobilidade Cisco AnyConnect Secure
- Cisco ISE, libera 2.0 e mais atrasado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



O fluxo é como segue:

- A sessão de VPN iniciada pelo cliente de AnyConnect é autenticada através do ISE. O estado da postura do valor-limite não é sabido, o **desconhecido da regra ASA VPN** é batido e em consequência a sessão é reorientada ao ISE para o abastecimento
- O usuário abre o web browser, tráfego de HTTP é reorientado pelo ASA ao ISE. O ISE empurra a versão a mais nova de AnyConnect junto com o módulo da postura e da conformidade para o valor-limite
- Uma vez que o módulo da postura é executado, verifica se a separação **E**: é cifrado inteiramente por BitLocker. Se sim, o relatório é enviado ao ISE que provoca a mudança do raio da autorização (CoA) sem nenhum ACL (o acesso direto)
- A sessão de VPN no ASA é atualizada, reorienta o ACL é removida e a sessão tem o acesso direto

A sessão de VPN é apresentada como um exemplo. A funcionalidade da postura trabalha muito bem demasiado para outros tipos do acesso.

ASA

É configurado do acesso remoto SSL VPN com o uso do ISE como o server do Authentication, Authorization, and Accounting (AAA). O CoA do raio junto com REORIENTA O ACL precisa de ser configurado:

```

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

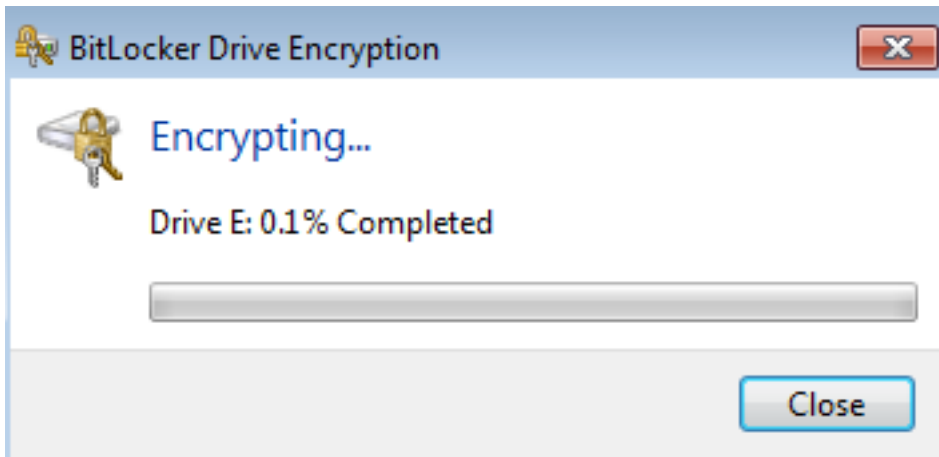
```

Consulte para mais detalhes:

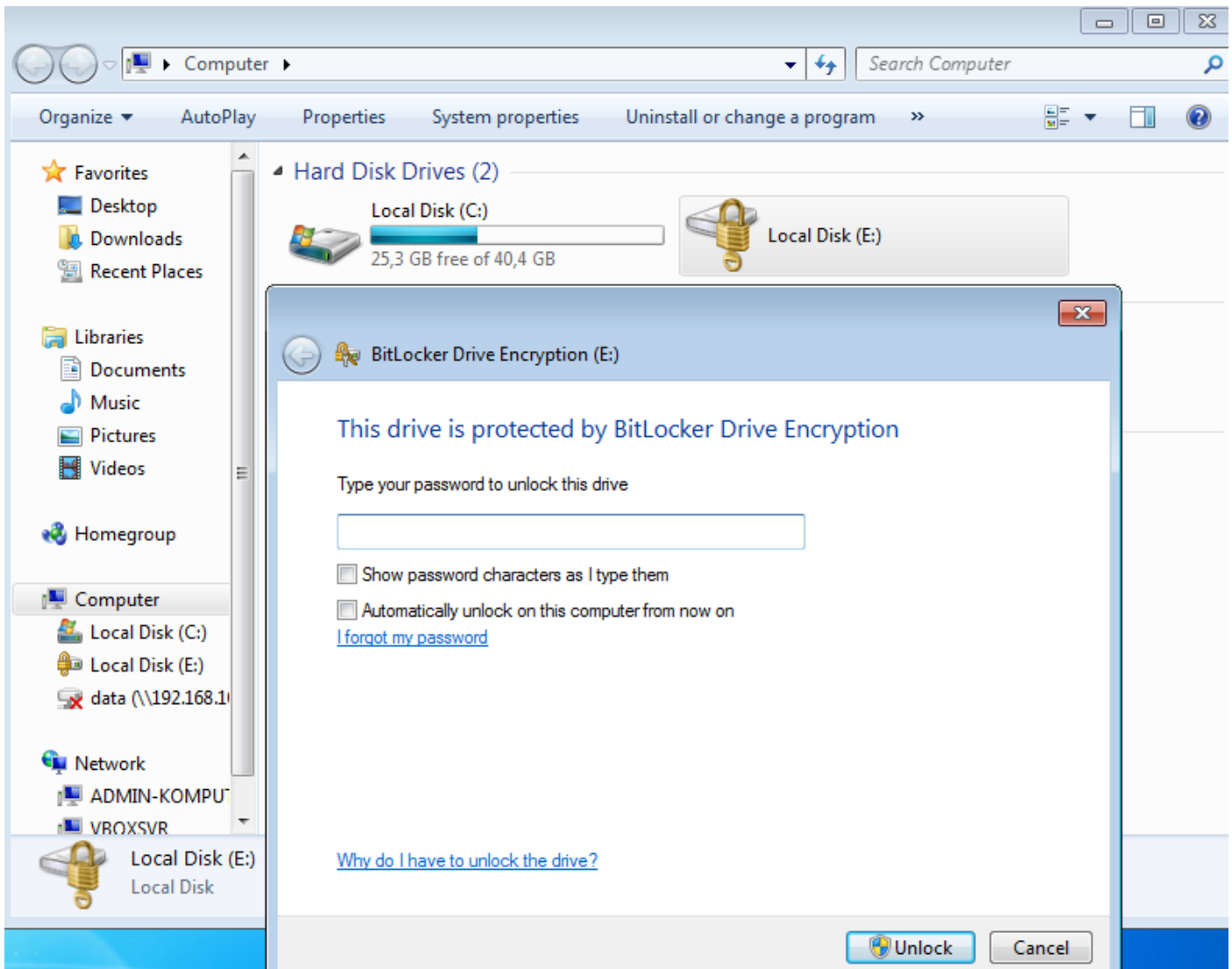
[Integração de AnyConnect 4.0 com exemplo de configuração da versão 1.3 ISE](#)

BitLocker em Windows 7

Navegue ao **Control Panel > ao sistema e a Segurança > a criptografia da movimentação de BitLocker**, permitem **E:** criptografia da separação. Proteja-a pela senha (PIN) segundo as indicações da imagem.



Uma vez que é cifrado, monte-o (com a disposição da senha) e assegure-se de que seja acessível segundo as indicações da imagem.



Para mais detalhes, siga a documentação Microsoft:

[Guia passo a passo da criptografia da movimentação de Windows BitLocker](#)

ISE

Etapa 1. Dispositivo de rede

Navegue à **administração > aos recursos de rede > aos dispositivos de rede**, adicionar o **ASA** com **tipo de dispositivo = ASA**. Isto é usado porque uma condição nas regras mas nela da autorização não é imperativa (outros tipos de condições podem ser usados).

Se apropriado, o grupo de dispositivo de rede não existe. A fim criar, navegue à **administração > aos recursos de rede > aos grupos de dispositivo de rede**.

Etapa 2. Condição e políticas da postura

Assegure-se de que condições da postura esteja atualizada: Navegue à **administração > ao sistema > aos ajustes > à postura > às atualizações > à atualização agora**.

Navegue à **política > aos elementos da política > às circunstâncias > à postura > à condição da criptografia do disco**, adicionar uma condição nova segundo as indicações da imagem.

The screenshot shows the Cisco ISE configuration interface for a "Disk Encryption Condition" named "bitlocker". The breadcrumb trail is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements > Conditions > Results.

Disk Encryption Condition Configuration:

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

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

Encryption State: Encryption State (i)

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

Verificações desta circunstância se BitLocker para Windows 7 é instalado e se E: a separação é cifrada inteiramente.

Nota: BitLocker é criptografia nivelada do disco e não suporta o lugar específico com argumento do trajeto, somente letra do disco.

Navegue à política > aos elementos > aos resultados > à postura > às exigências da política a fim criar uma exigência nova que use a circunstância segundo as indicações da imagem.

The screenshot shows the Cisco ISE configuration interface for "Requirements". The breadcrumb trail is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements > Results > Requirements.

Requirements Table:

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

Navegue à política > à postura, adicionar uma condição para todo o Windows a fim usar a exigência segundo as indicações da imagem.

Posture Policy

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

Etapa 3. Recursos e política do abastecimento do cliente

Navegue à política > aos elementos da política > ao abastecimento > aos recursos do cliente, transfira o módulo da conformidade do cisco.com e transfira arquivos pela rede manualmente o pacote de AnyConnect 4.2 segundo as indicações da imagem.

Resources

Edit + Add Duplicate Delete

<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 ...

Navegue para adicionar > agente NAC ou o perfil da postura de AnyConnect, cria o perfil da postura de AnyConnect (nome: AnyConnectPosture) com configurações padrão.

Navegue para adicionar > configuração de AnyConnect, adicionar o perfil de AnyConnect (nome: Configuração de AnyConnect) segundo as indicações da imagem.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.96.0

* Configuration Name: AnyConnect Configuration

Description:

DescriptionValue

* 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
- Network Access Manager
- Web Security
- AMP Enabler
- Network Visibility
- Customer Feedback

Navegue à política > ao abastecimento do cliente e altere a política padrão para Windows a fim usar o perfil configurado de AnyConnect segundo as indicações da imagem.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

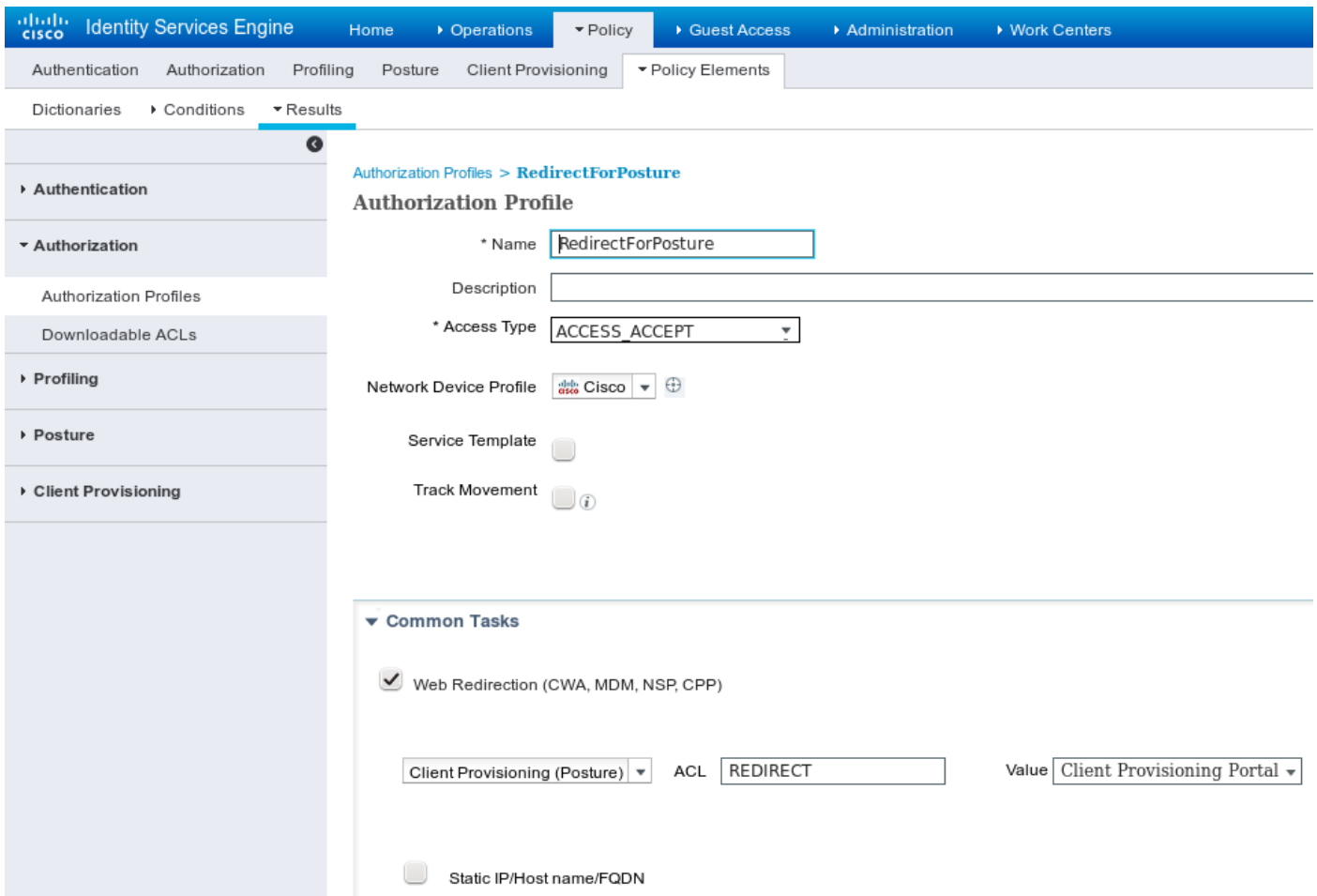
Client Provisioning Policy

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

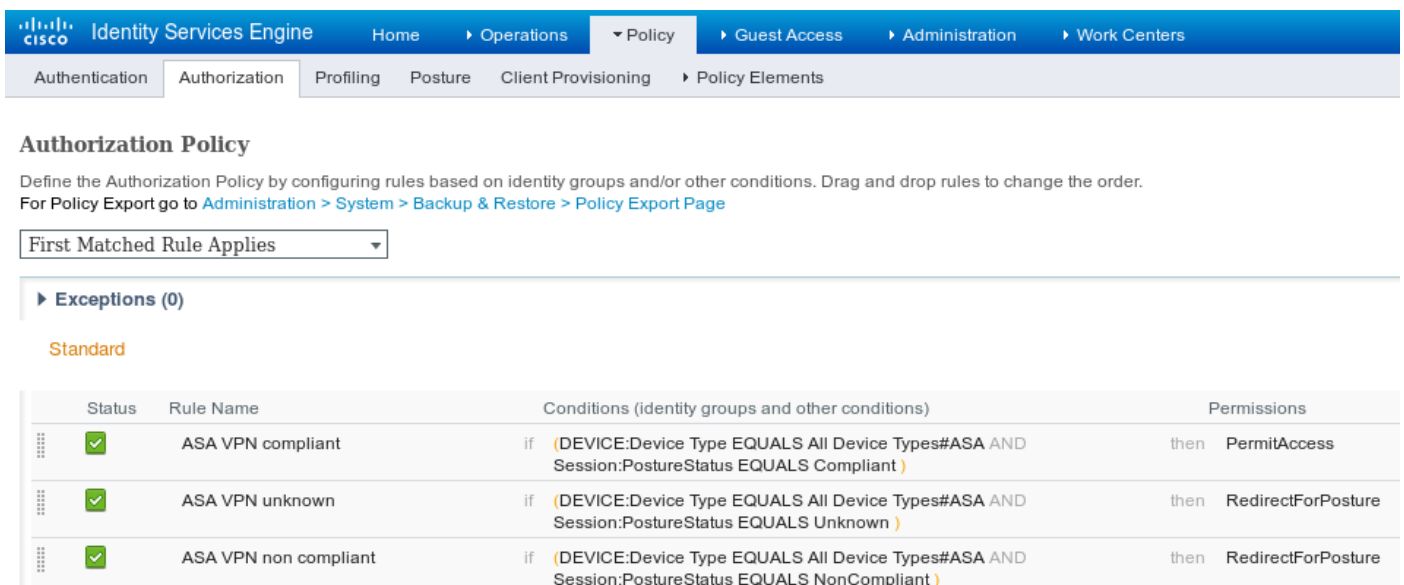
Etapa 4. Regras da autorização

Navegue à política > aos elementos > aos resultados > à autorização da política, adicionar o perfil da autorização (nome: **RedirectForPosture**) qual reorienta a um portal do abastecimento do cliente do padrão segundo as indicações da imagem.



REORIENTE O ACL é definido no ASA.

Navegue à **política > à autorização**, crie 3 regras da autorização segundo as indicações da imagem.



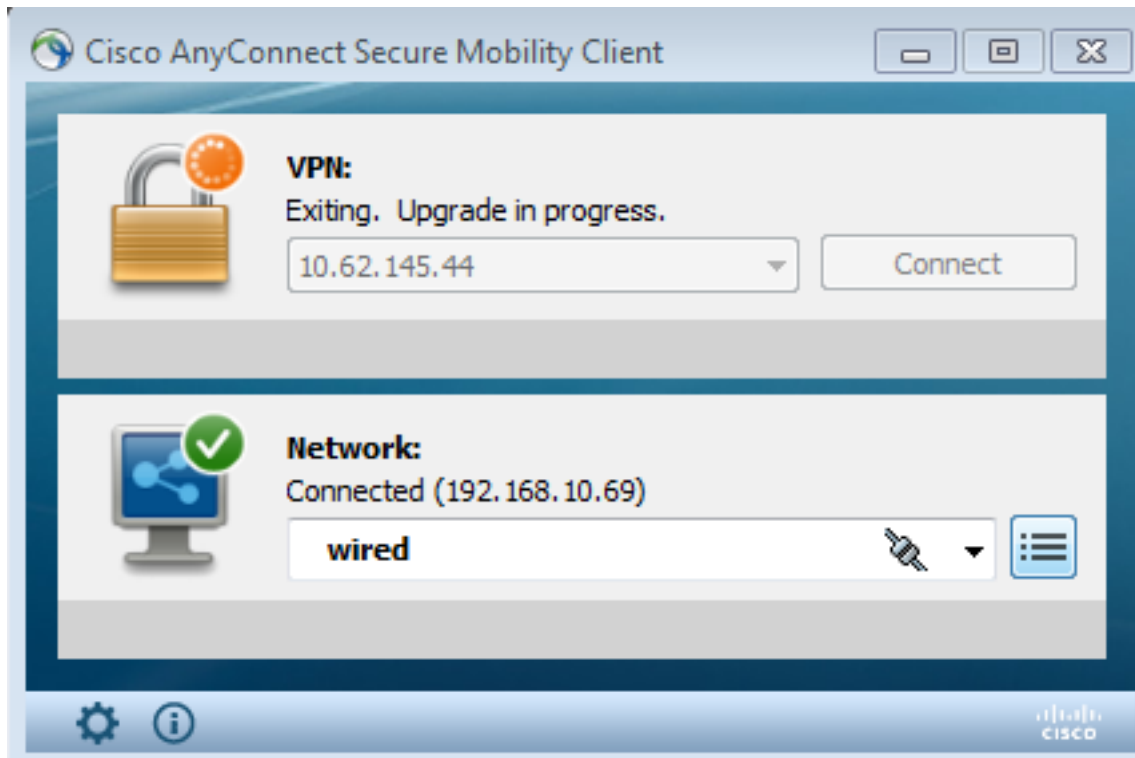
Se o valor-limite é complacente, o acesso direto está fornecido. Se o estado é desconhecido ou não complacente, a reorientação para o abastecimento do cliente está retornada.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Estabelecimento da sessão de VPN

Uma vez que a sessão de VPN é estabelecida, o ASA pôde querer executar uma elevação dos módulos de AnyConnect segundo as indicações da imagem.



No ISE a última regra é batida, em consequência as permissões de **RedirectForPosture** são retornadas segundo as indicações da imagem.

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

Uma vez que o ASA termina construir a sessão de VPN, relata que a reorientação deve ocorrer:

```
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

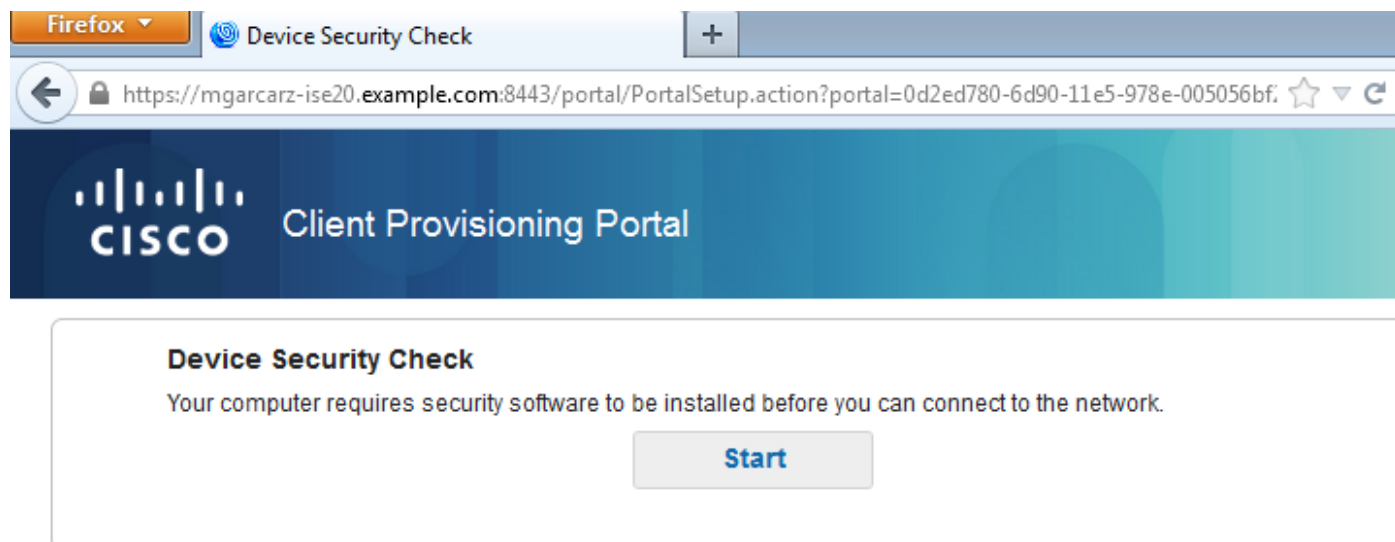
<some output omitted for clarity>

ISE Posture:

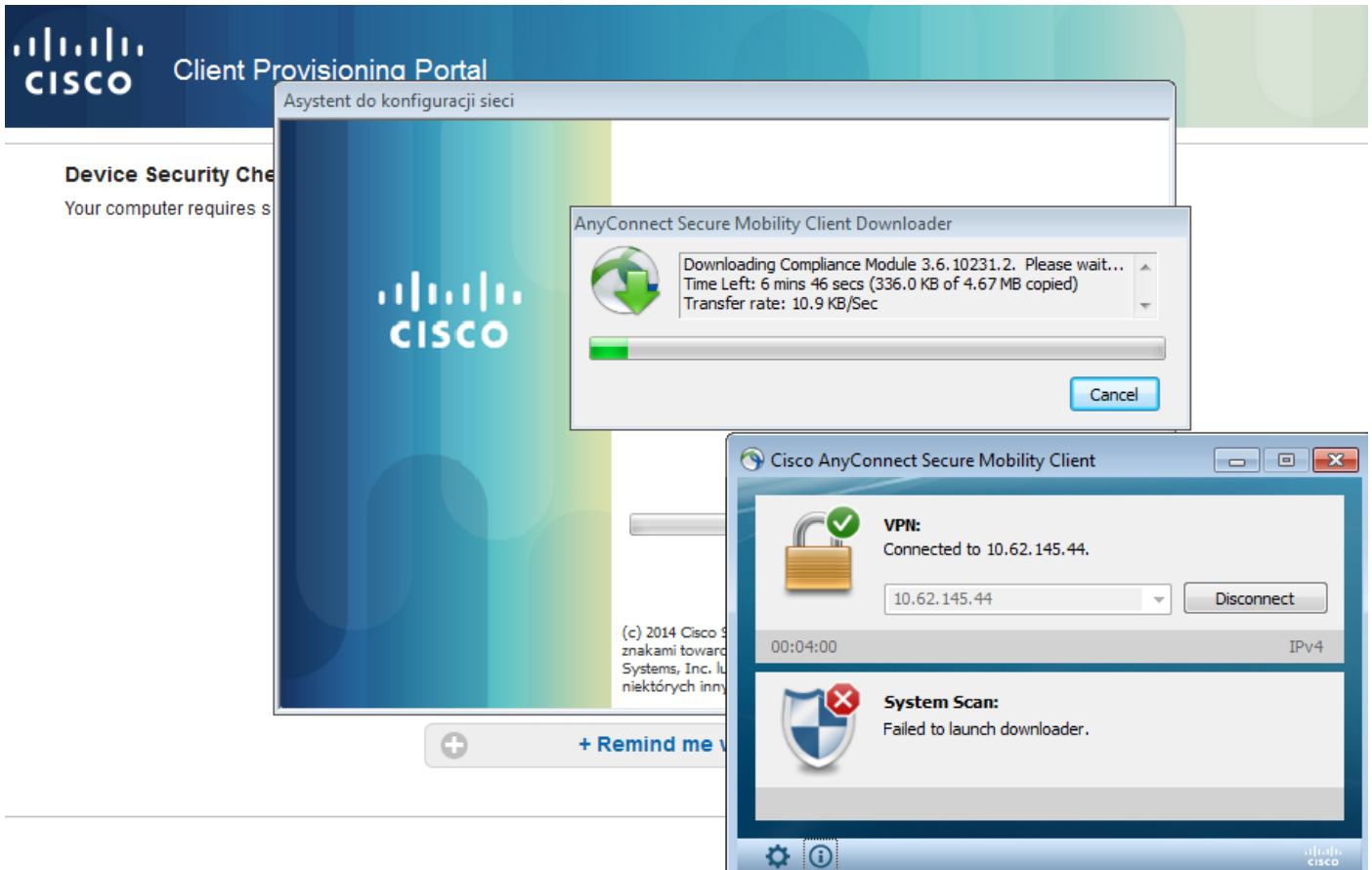
Redirect URL : <https://mgarcarz-ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-005056bf>
Redirect ACL : REDIRECT

Etapa 2. Abastecimento do cliente

Nessa fase, o tráfego do web browser do valor-limite é reorientado ao ISE para o abastecimento do cliente segundo as indicações da imagem.

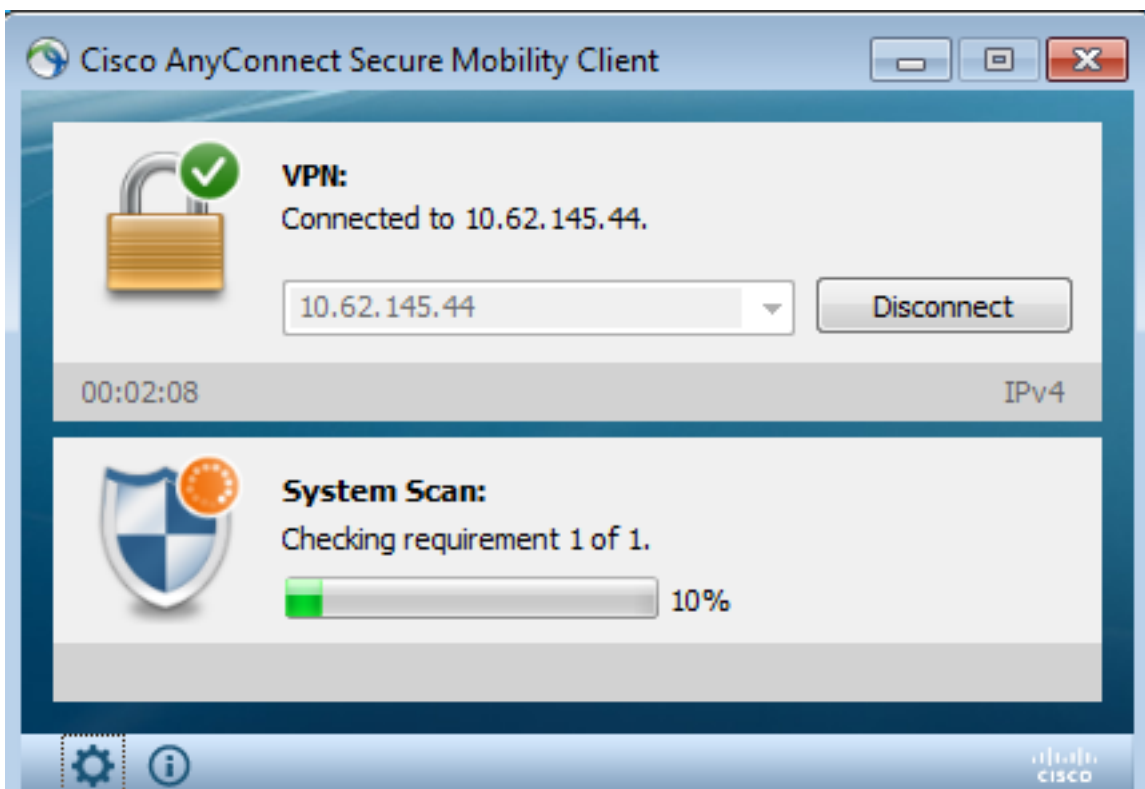


Se necessário, AnyConnect junto com a postura e o módulo da conformidade é atualizado segundo as indicações da imagem.



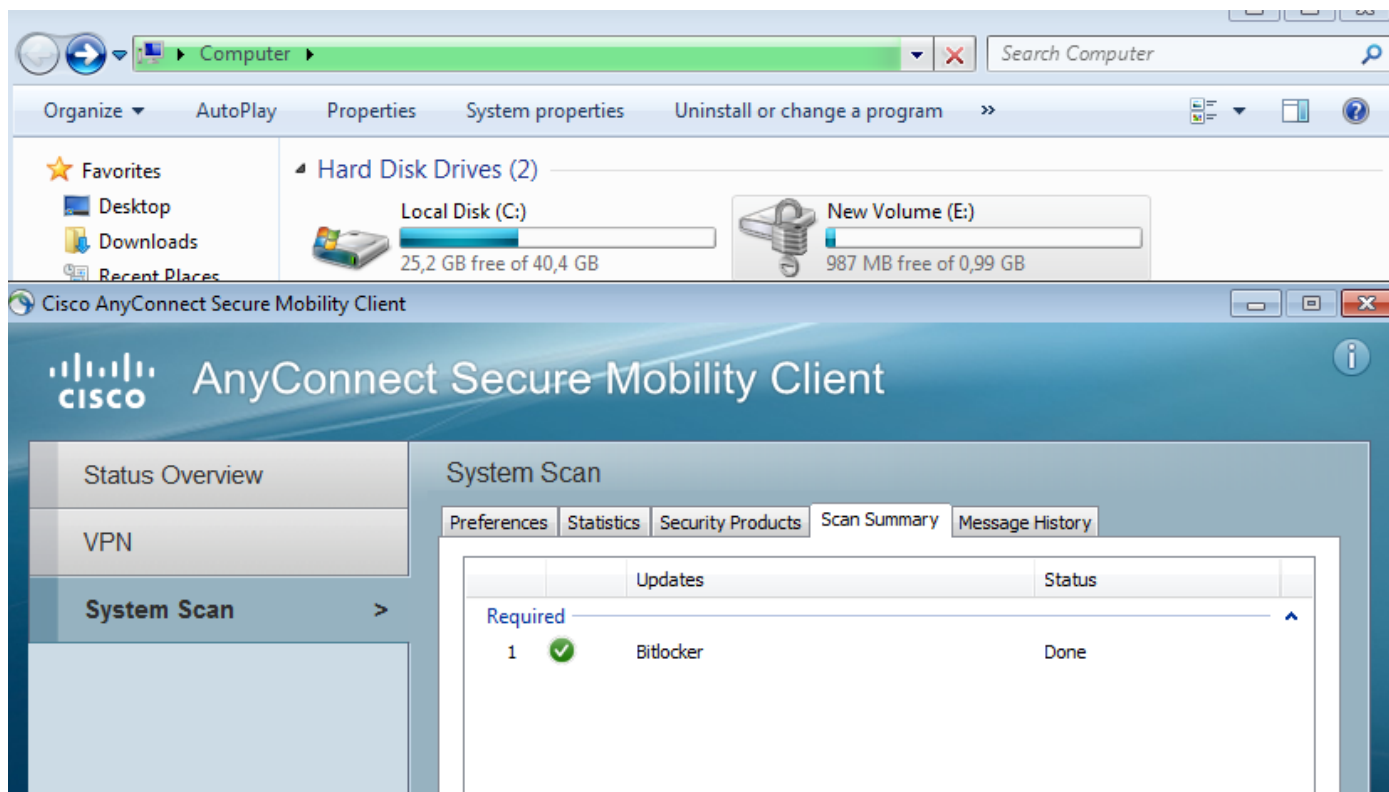
Etapa 3. Verificação da postura e CoA

O módulo da postura é executado, descobre ISE (pôde exigir para ter o registro DNS A para enroll.cisco.com a fim suceder), transfere e verifica condições da postura segundo as indicações da imagem.

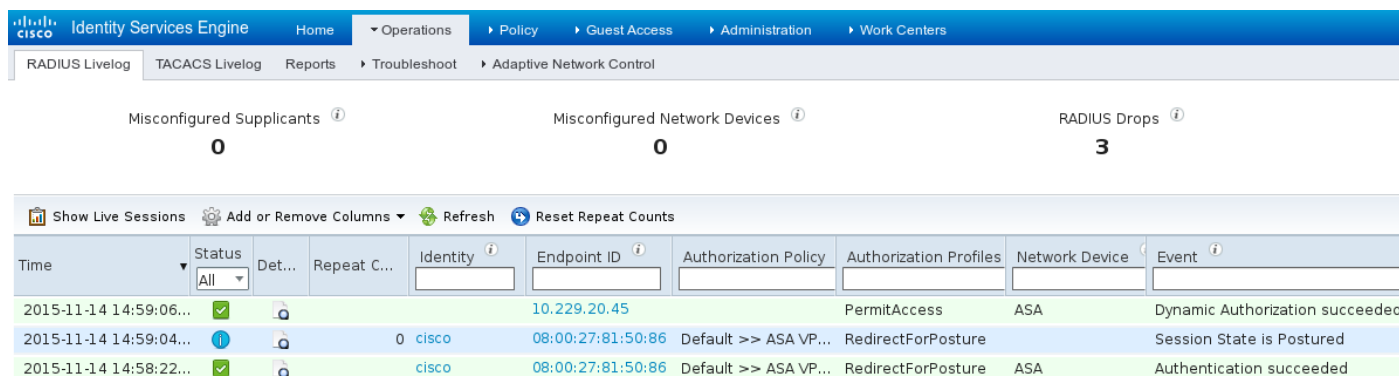


Uma vez que se confirma que E: a separação é cifrada inteiramente por BitLocker, o relatório

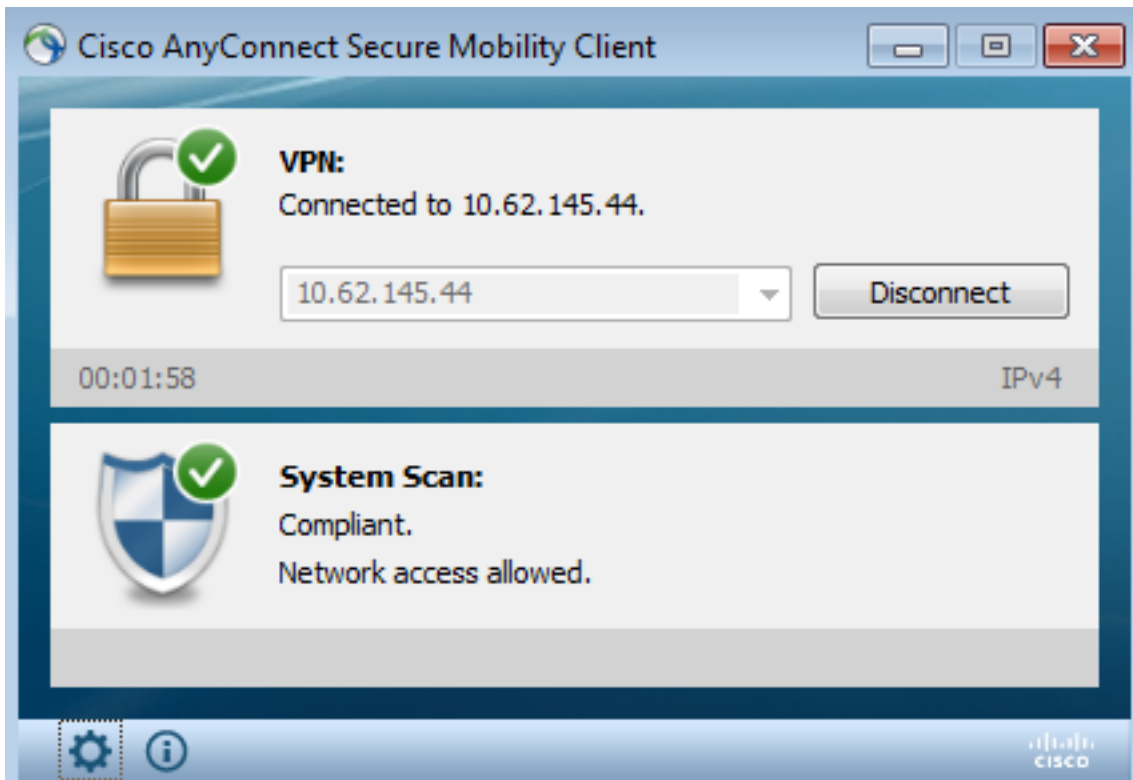
correto é enviada ao ISE segundo as indicações da imagem.



Isto provoca o CoA para reauthorize a sessão de VPN, segundo as indicações da imagem.



O ASA remove a reorientação ACL que fornece o acesso direto. AnyConnect relata a conformidade segundo as indicações da imagem.



Também, os relatórios detalhados no ISE podem confirmar que ambas as circunstâncias estão satisfeitas (a **avaliação da postura pela circunstância** é o relatório novo ISE 2.0 que mostra cada circunstância). A primeira condição (**hd_inst_BitLockerDriveEncryption_6_x**) verifica para ver se há a instalação/processo, as segundas uma verificações (**hd_loc_bitlocker_specific_1**) se o lugar específico (E:) é cifrado inteiramente segundo as indicações da imagem.

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

A **avaliação da postura ISE** pelo relatório do **valor-limite** confirma que todas as circunstâncias estão satisfeitas, segundo as indicações da imagem.

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

O mesmos podem ser confirmados de ise-psc.log debugam. Posture o pedido recebido pelo ISE e pela resposta:

```
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) )
```

A resposta com a exigência da postura (circunstância + remediação) está no formato 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>
```

Após o relatório cifrado é recebido pelo 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> ]]
```

A estação é marcada como complacente e o ISE envia o 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
```

Também, a configuração final é enviada pelo 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
```

Estas etapas podem igualmente ser confirmadas do lado do cliente (DARDO de AnyConnect):

```
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    : acvpnui
```

```
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    : acvpnui
```

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

Para a sessão bem-sucedida, a **varredura do sistema de AnyConnect UI/história da mensagem** relata:

```
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.
```

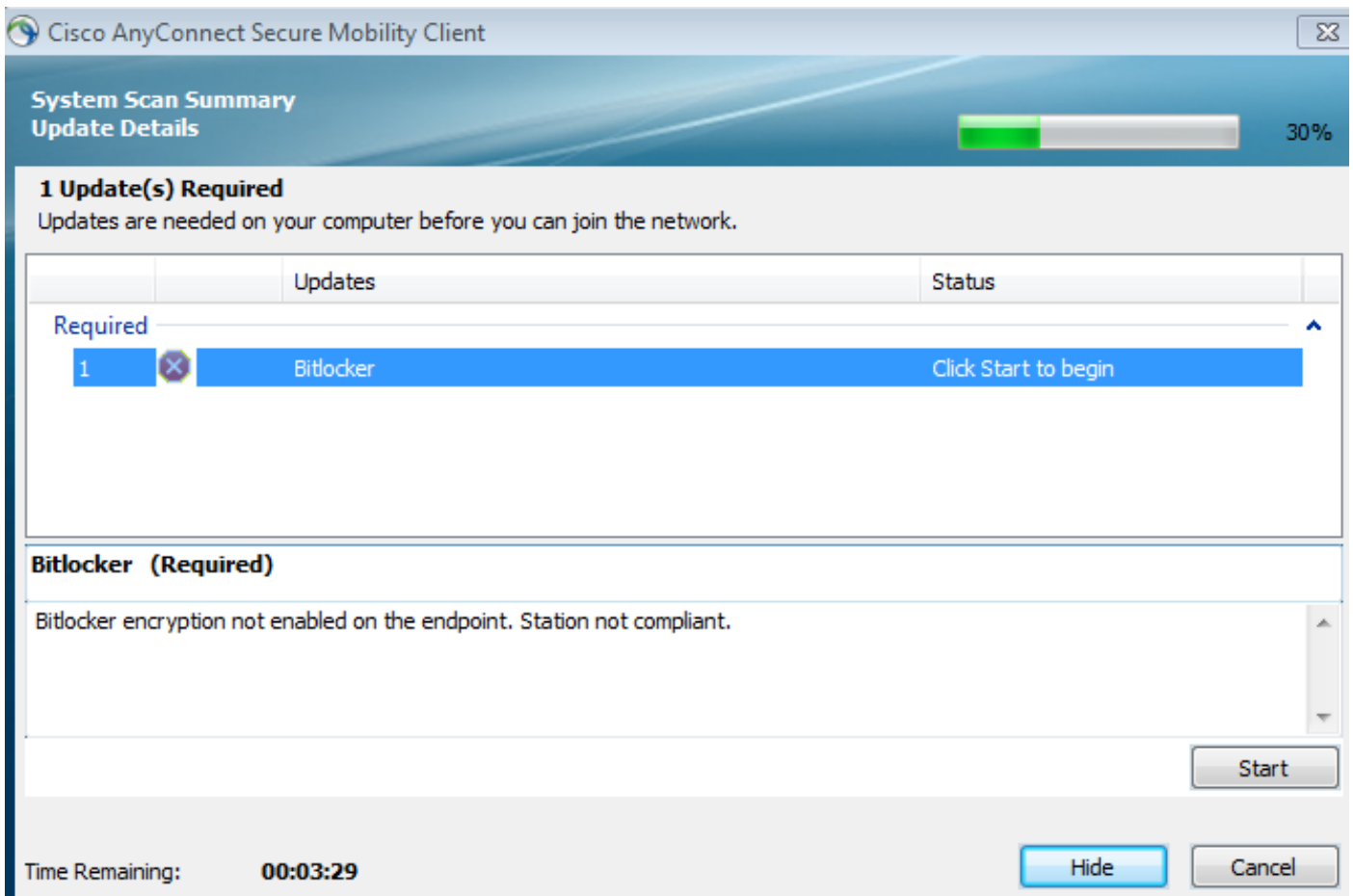
Erros

[CSCux15941](#) - ISE 2.0 e criptografia do bitlocker da postura AC4.2 com failing do lugar (\ do carvão animal/não apoiado)

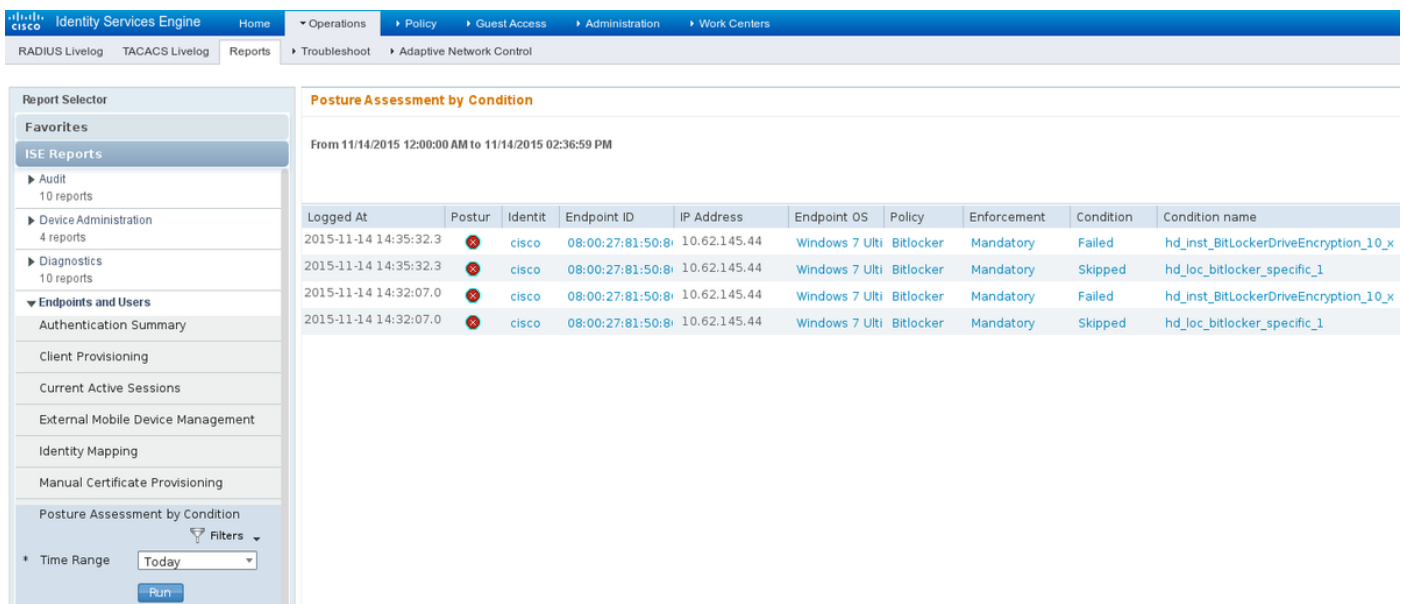
Troubleshooting

Esta seção fornece informações que você pode usar na solução de problemas de sua configuração.

Se o valor-limite é NON-complacente, está relatado por AnyConnect UI (a remediação igualmente configurada é executada) segundo as indicações da imagem.



O ISE pode fornecer os detalhes nas circunstâncias de falha, segundo as indicações da imagem.



O mesmos podem ser verificados dos logs CLI (os exemplos do entram a seção verificam).

Informações Relacionadas

- [Como configurar um servidor externo para autorização de usuário de dispositivo de segurança](#)
- [Guia de configuração de CLI para VPN da Cisco ASA Series, 9.1](#)
- [Guia do administrador do Cisco Identity Services Engine, liberação 2.0](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)