ISE 2.0 y ejemplo de la configuración de encripción de BitLocker de la postura de AnyConnect 4.2

Contenido

Introducción

La versión 2.0 del Cisco Identity Services Engine (ISE) junto con el cliente seguro 4.2 de la movilidad de AnyConnect soporta la postura para el cifrado del disco. Este documento describe cómo cifrar la partición de disco del punto final usando Microsoft BitLocker y cómo configurar el ISE para proporcionar el acceso total a la red solamente cuando se configura el cifrado correcto.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración CLI del dispositivo de seguridad (ASA) y de la configuración VPN adaptantes del Secure Socket Layer (SSL)

- Conocimiento básico de la configuración del VPN de acceso remoto en el ASA
- Conocimiento básico del ISE y de los servicios de la postura

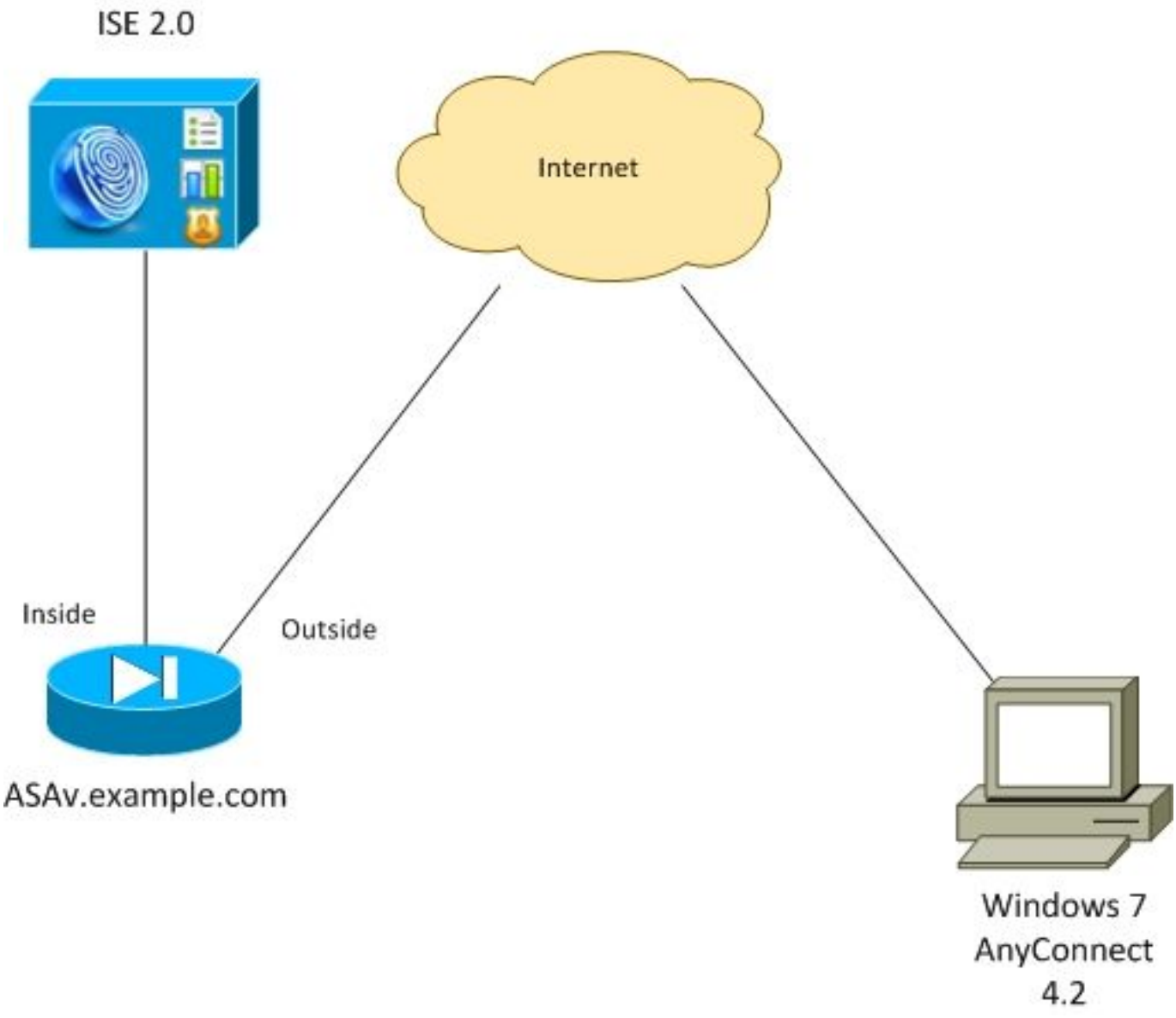
Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Versiones de software 9.2.1 de Cisco ASA y posterior
- Versión 7 de Microsoft Windows con la versión 4.2 y posterior del Cliente de movilidad Cisco AnyConnect Secure
- Cisco ISE, libera 2.0 y posterior

Configurar

Diagrama de la red



El flujo es el siguiente:

- Autentican a la sesión de VPN iniciada por el cliente de AnyConnect vía el ISE. El estatus de

la postura del punto final no se sabe, se golpea la regla “desconocido ASA VPN” y como consecuencia la sesión será reorientada al ISE para disposición.

- El usuario abre al buscador Web, tráfico HTTP es reorientado por el ASA al ISE. El ISE avanza la versión más reciente de AnyConnect junto con el módulo de la postura y de la conformidad al punto final

- Una vez que se ejecuta el módulo de la postura marca si la división “E: ” es cifrado completamente por BitLocker. Si el informe se envía sí al ISE, que está accionando el cambio del radio de la autorización (CoA) sin ningún ACL (el acceso total)

- La sesión de VPN en el ASA es actualizada, reorienta el ACL se quita y la sesión está teniendo acceso total

Han presentado la sesión de VPN apenas como el ejemplo. Las funciones de la postura están trabajando muy bien también para otros tipos del acceso.

ASA

Se configura del acceso del telecontrol SSL VPN usando el ISE como servidor de AAA. El CoA del radio junto con *REORIENTA EL* ACL necesita ser configurado:

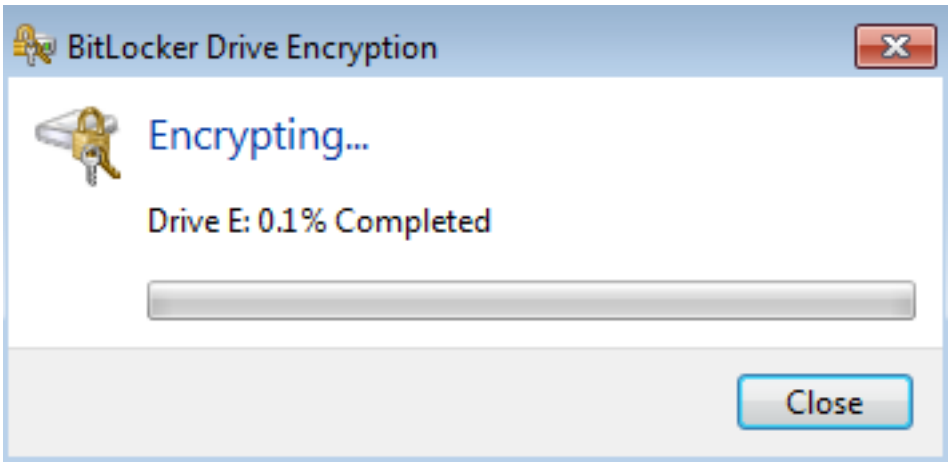
```
aaa-server ISE20 protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE20 (inside) host 10.48.17.235
 key cisco

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
```

Para más detalles satisfaga se refieren:

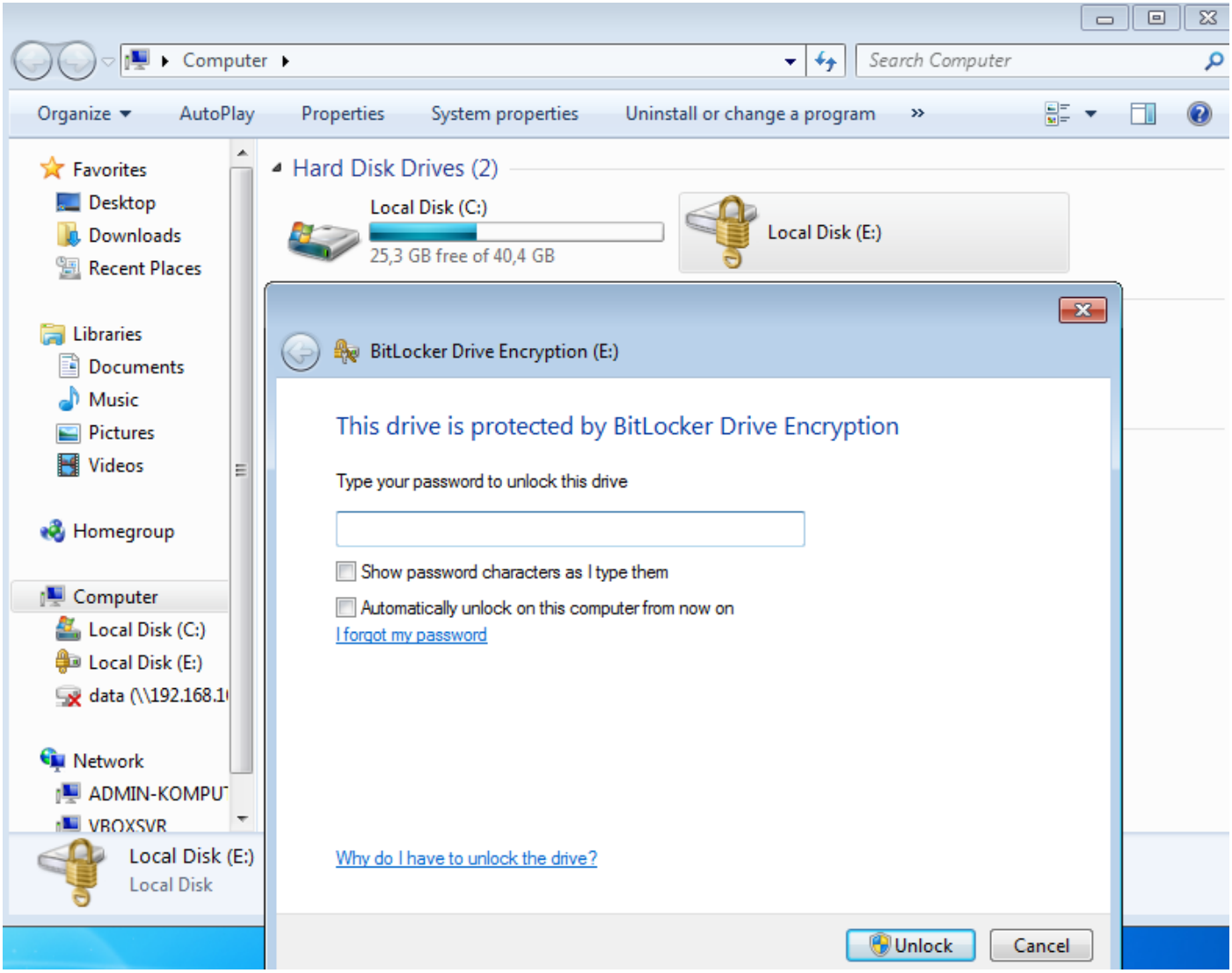
[Integración de AnyConnect 4.0 con el ejemplo de configuración de la versión 1.3 ISE]

BitLocker en Windows 7

Del panel de control - > sistema y Seguridad - > permiso E del *cifrado de la unidad de BitLocker*: cifrado de la división. Protéjalo por la contraseña (PIN).



Una vez que ha cifrado el soporte él (proporcionando a la contraseña) y aseegurese la es accesible:



Para más detalles siga la documentación de Microsoft:

[Guía paso a paso del cifrado de la unidad de Windows BitLocker]

ISE

Dispositivo de red Step1

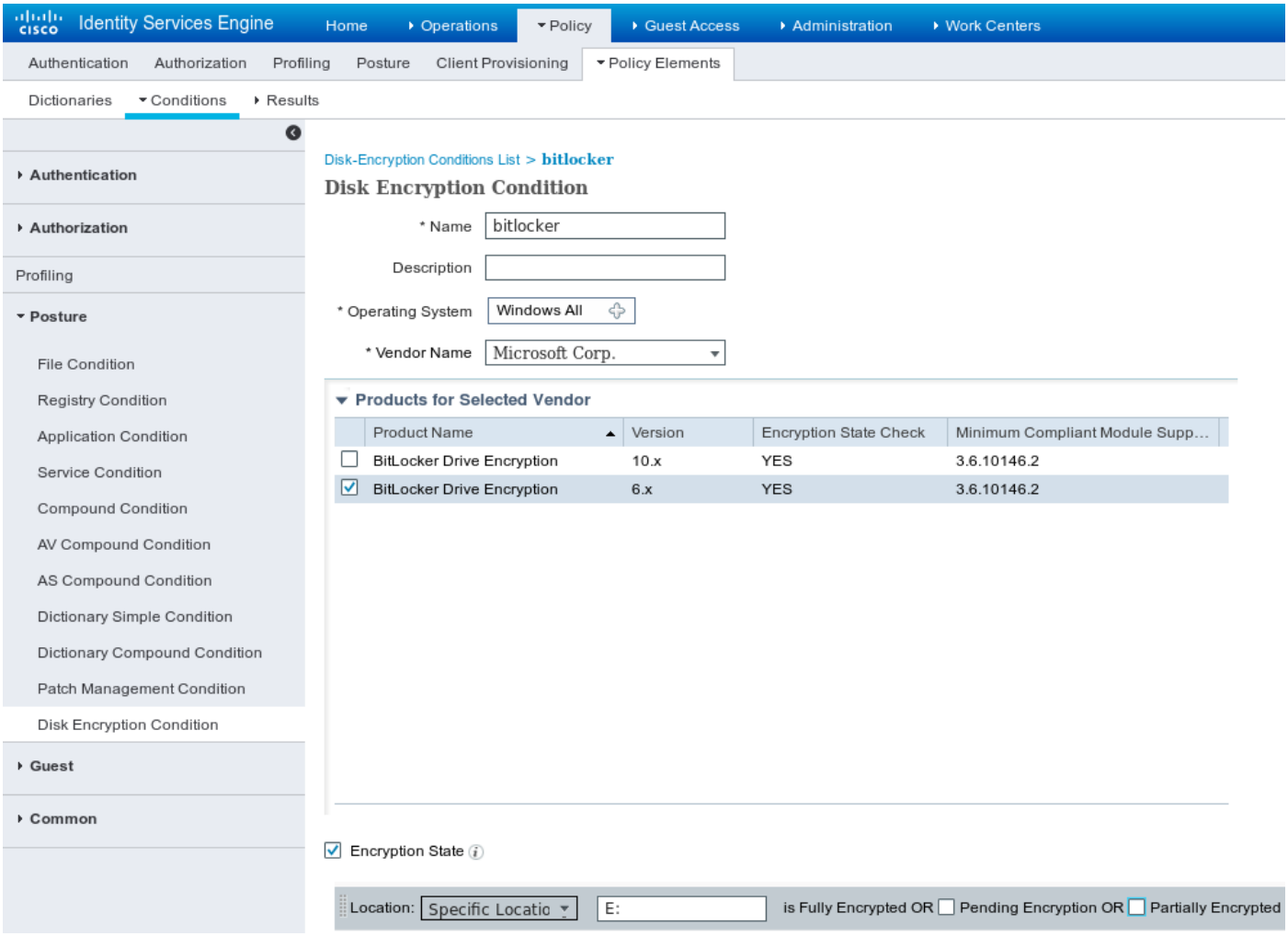
De la administración > de los recursos de red > de los dispositivos de red agregue el ASA con el tipo de dispositivo = el ASA. Eso será utilizada como condición en las reglas de la autorización pero no es obligatorio (otros tipos de condiciones pueden ser utilizados).

Si no existe el grupo de dispositivos de red apropiado créelo de la *administración > de los recursos de red > de los grupos de dispositivos de red.*

Condición y directivas de la postura Step2

Aseegurese las condiciones de la postura son actualizado: *De la administración - > sistema - > las configuraciones - > postura - >* ahora *ponen al día la* opción de la actualización.

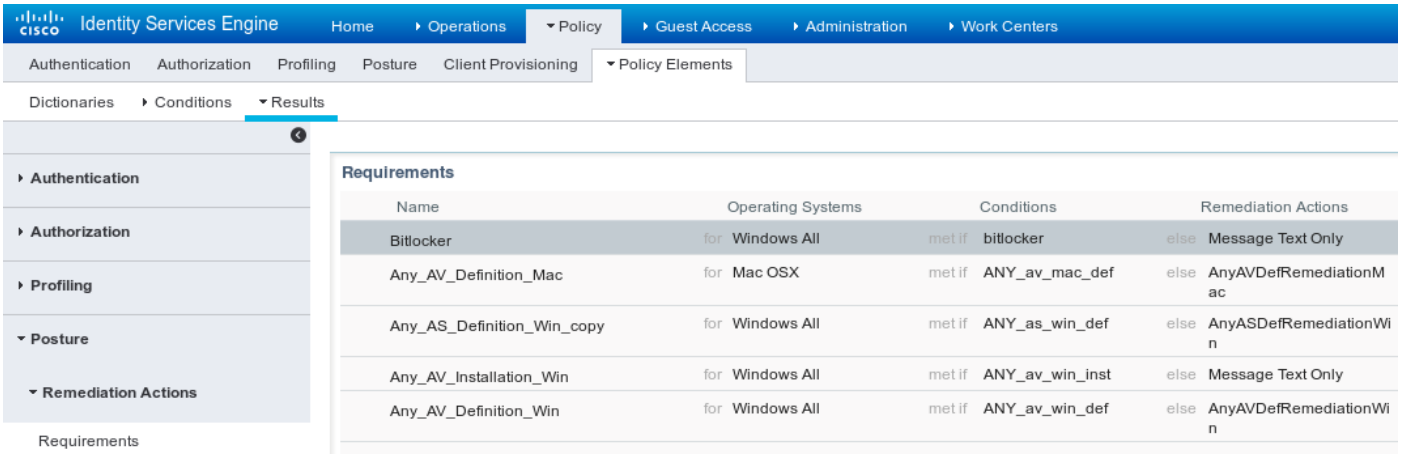
De la directiva - > los elementos de la directiva - > condiciona - > postura - > condición del cifrado del disco agregan una nueva condición:



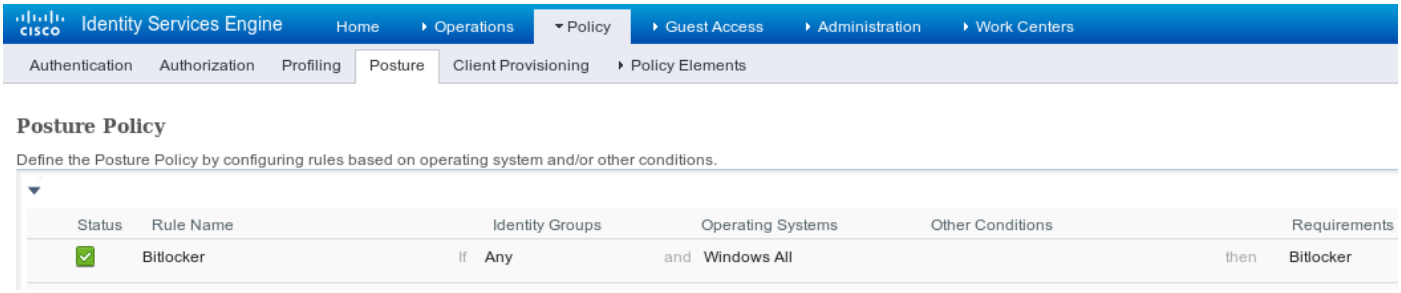
Esta condición marcará si BitLocker para Windows 7 está instalado y si E: la división se cifra

completamente. Note por favor que BitLocker es cifrado llano del disco y no soporta la *ubicación específica* con el argumento del trayecto, solamente carta del disco.

De la directiva - > los elementos de la directiva - > resultan - > postura - > los requisitos crean un nuevo requisito que esté utilizando esa condición:

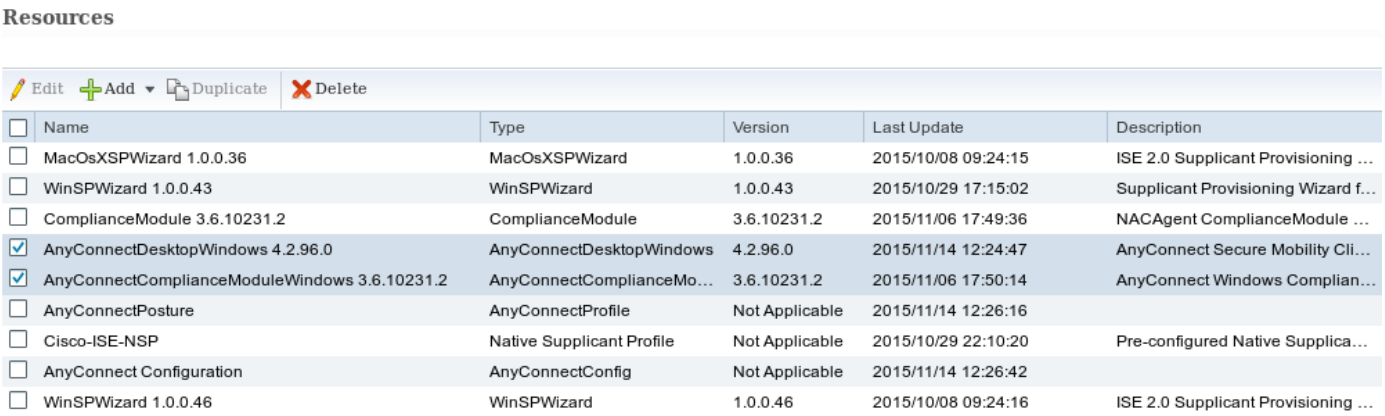


De la directiva - > la postura agrega una condición para que todo el Windows utilice ese requisito:



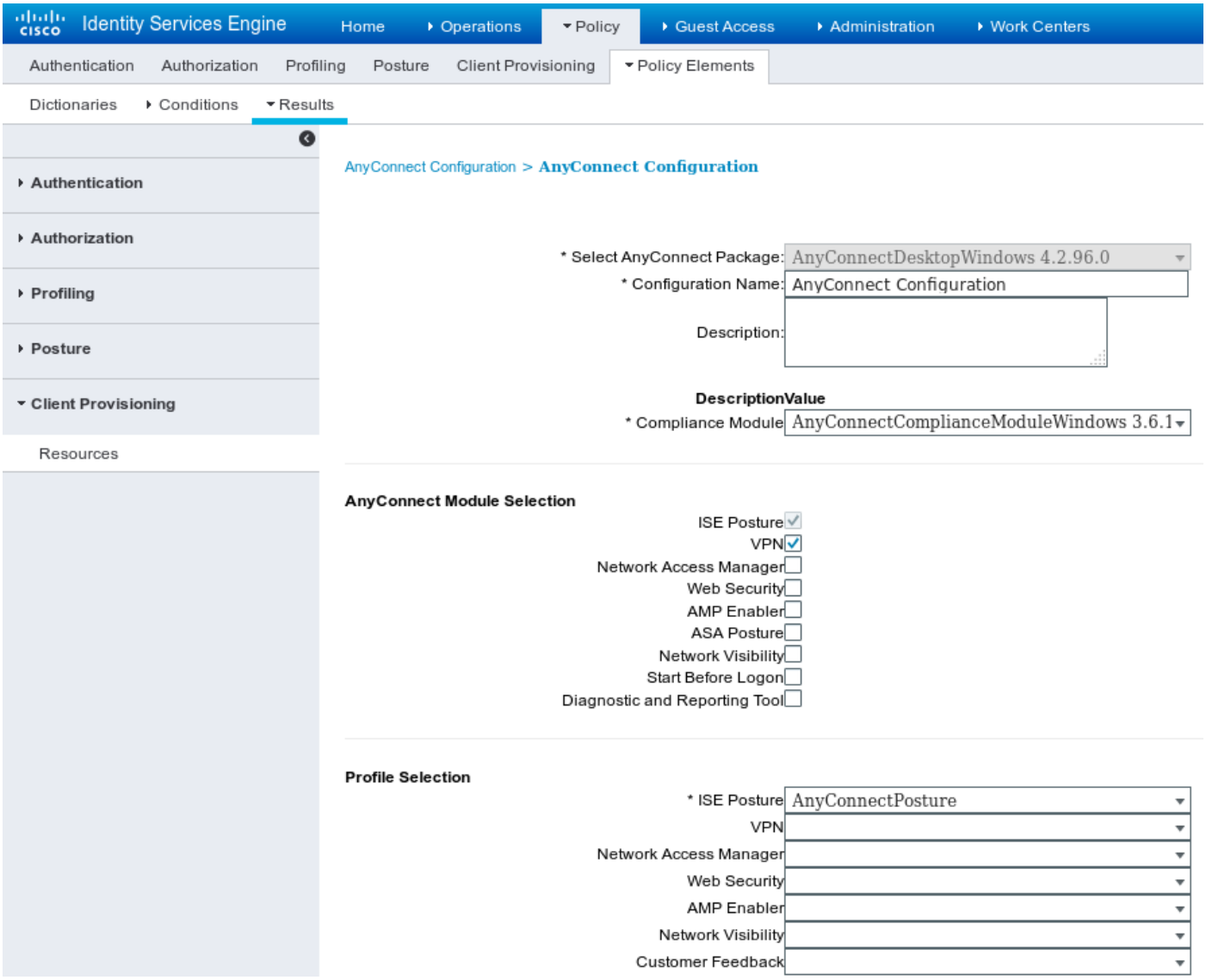
Recursos y directiva del aprovisionamiento del cliente Step3

De la directiva - > elementos de la directiva - > aprovisionamiento del cliente - > los recursos descargan el módulo de la conformidad del cisco.com y cargan manualmente el paquete de AnyConnect 4.2:

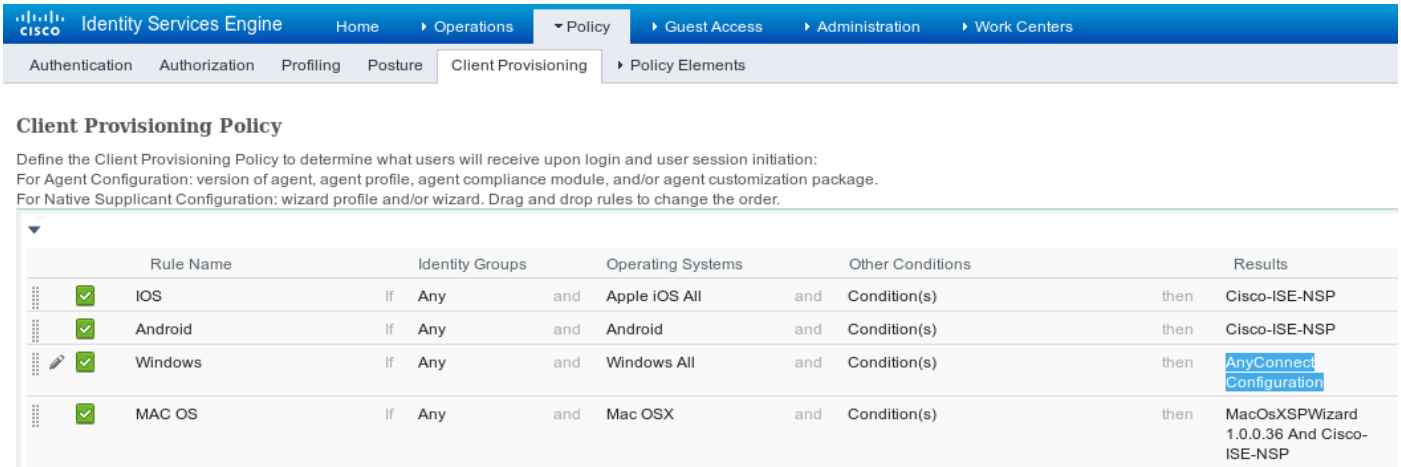


Usando *agregue - > el agente del NAC o el* perfil de la *postura de AnyConnect* crea el perfil de la postura de AnyConnect (nombre: *AnyConnectPosture*) con las configuraciones predeterminadas.

Usando *agregue - > la configuración de AnyConnect* agrega el perfil de AnyConnect (nombre: *Configuración de AnyConnect*):

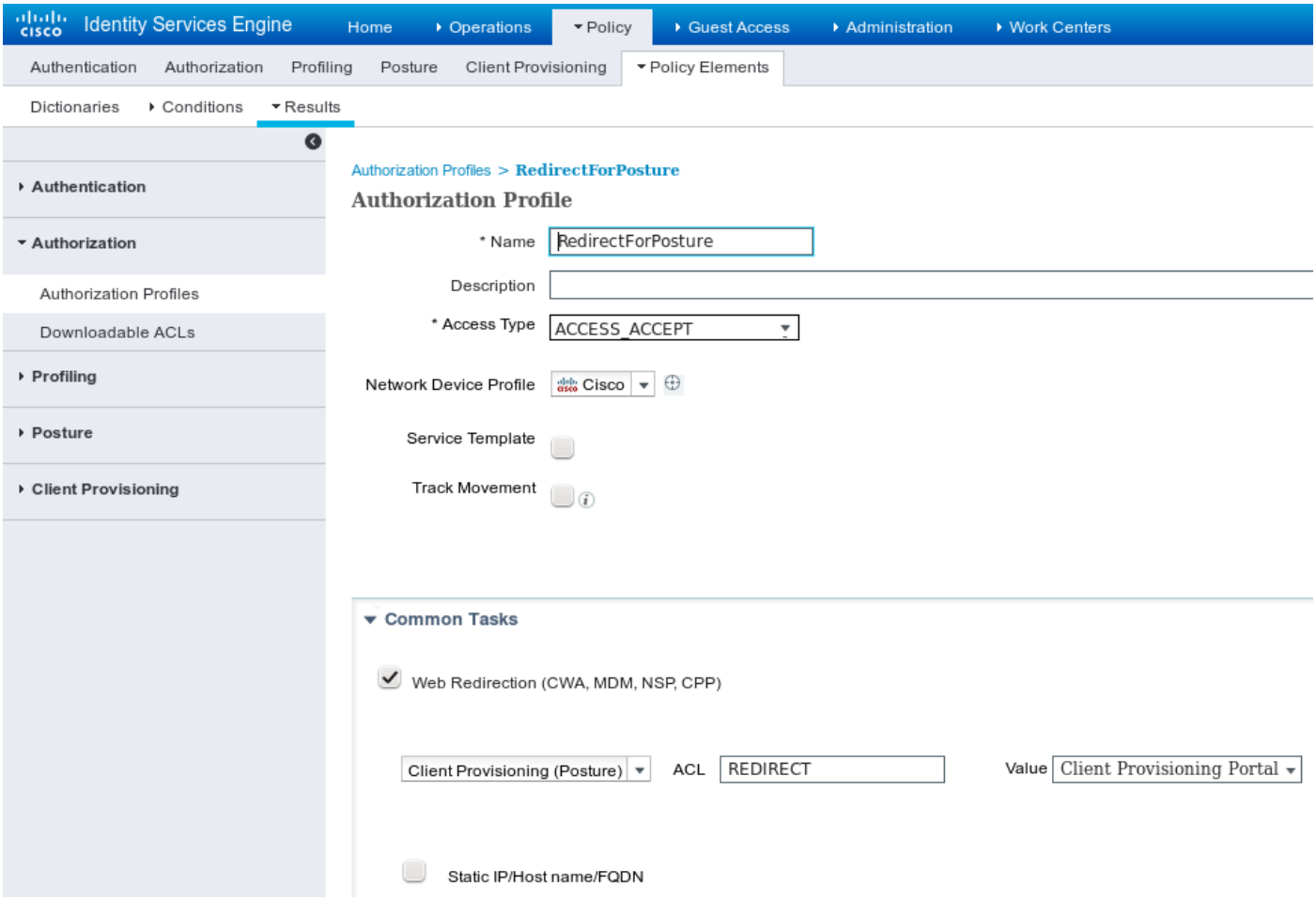


De la directiva - > el aprovisionamiento del cliente modifica la política predeterminada para que Windows utilice el perfil configurado de AnyConnect:



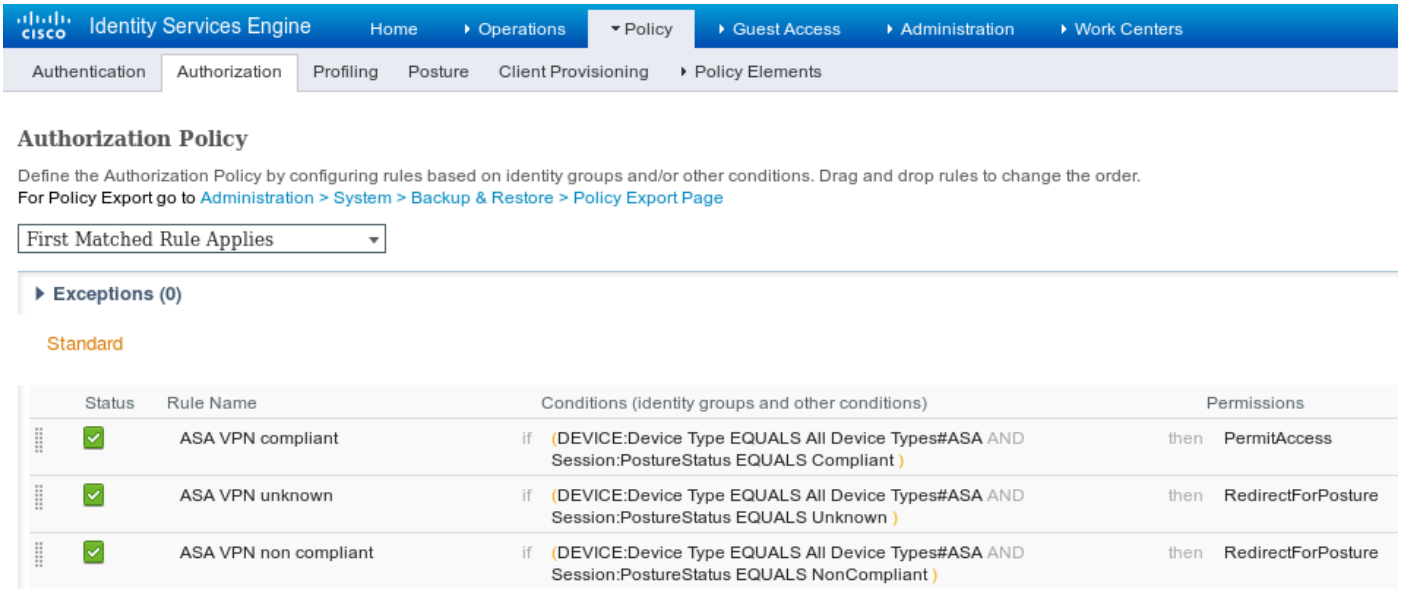
Reglas de la autorización Step4

De la directiva - > los elementos de la directiva - > resulta - > la autorización agrega el perfil de la autorización (nombre: *RedirectForPosture*) que reorienta a un portal de disposición del cliente predeterminado:



REORIENTE EL ACL se define en el ASA.

De la directiva - > la autorización crea 3 reglas de la autorización:

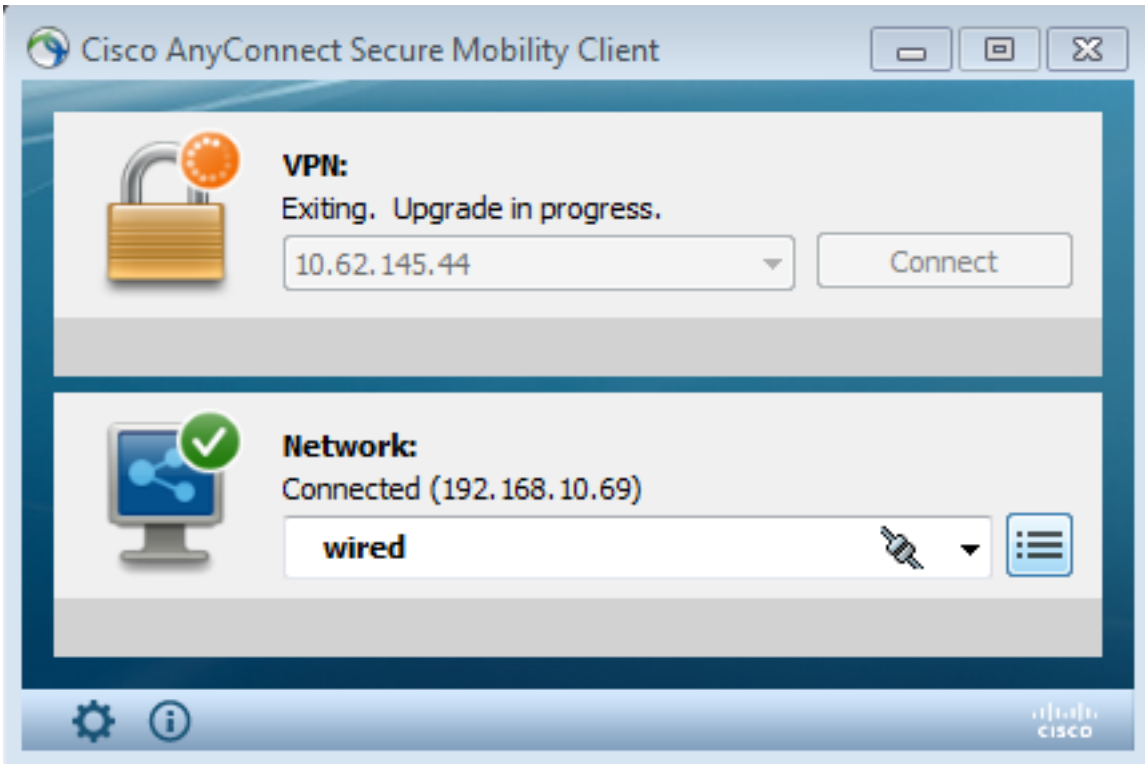


Si el punto final es obediente se proporciona el acceso total. Si el estatus es desconocido o el cambio de dirección no obediente para el aprovisionamiento del cliente se vuelve.

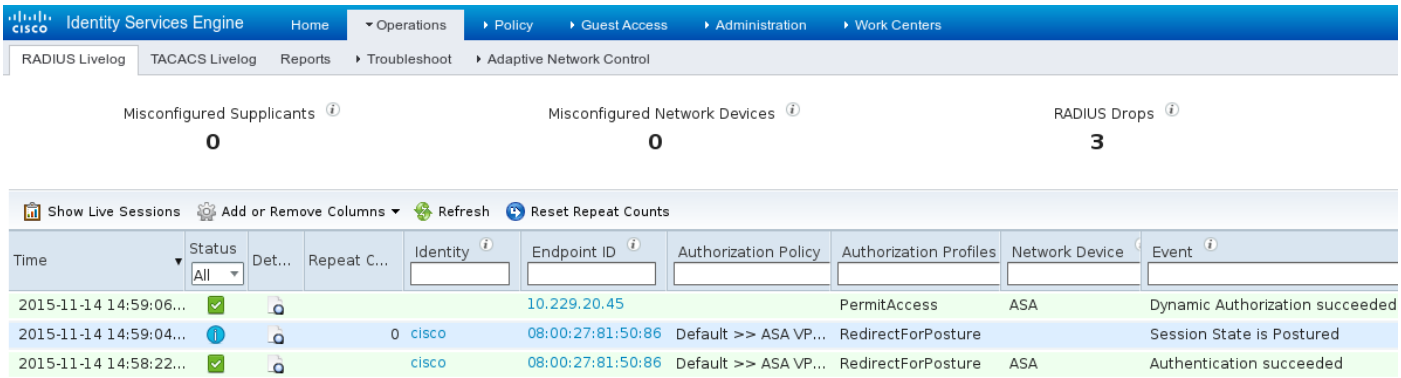
Verificación

Establecimiento de la sesión de VPN Step1

Una vez que establecen a la sesión de VPN el ASA pudo querer realizar la actualización de los módulos de AnyConnect:



En el ISE se golpea la regla más reciente, como consecuencia los permisos de *RedirectForPosture* se devuelven:



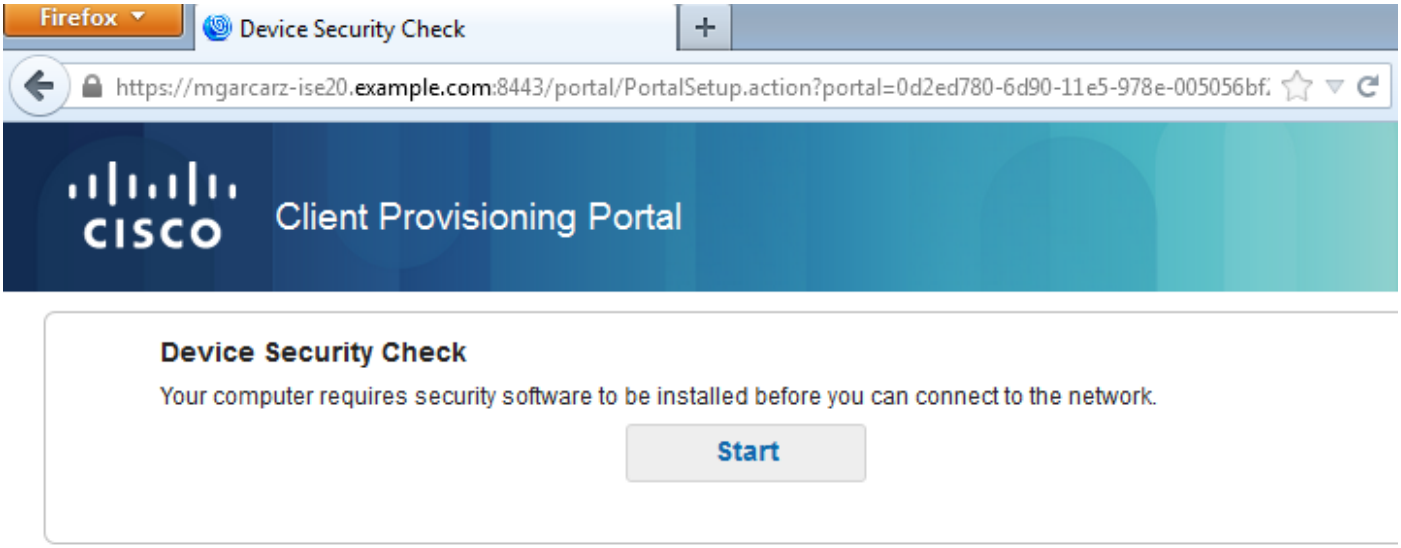
Una vez que el ASA acaba de construir a la sesión de VPN señala que el cambio de dirección debe ocurrir:

```
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
```

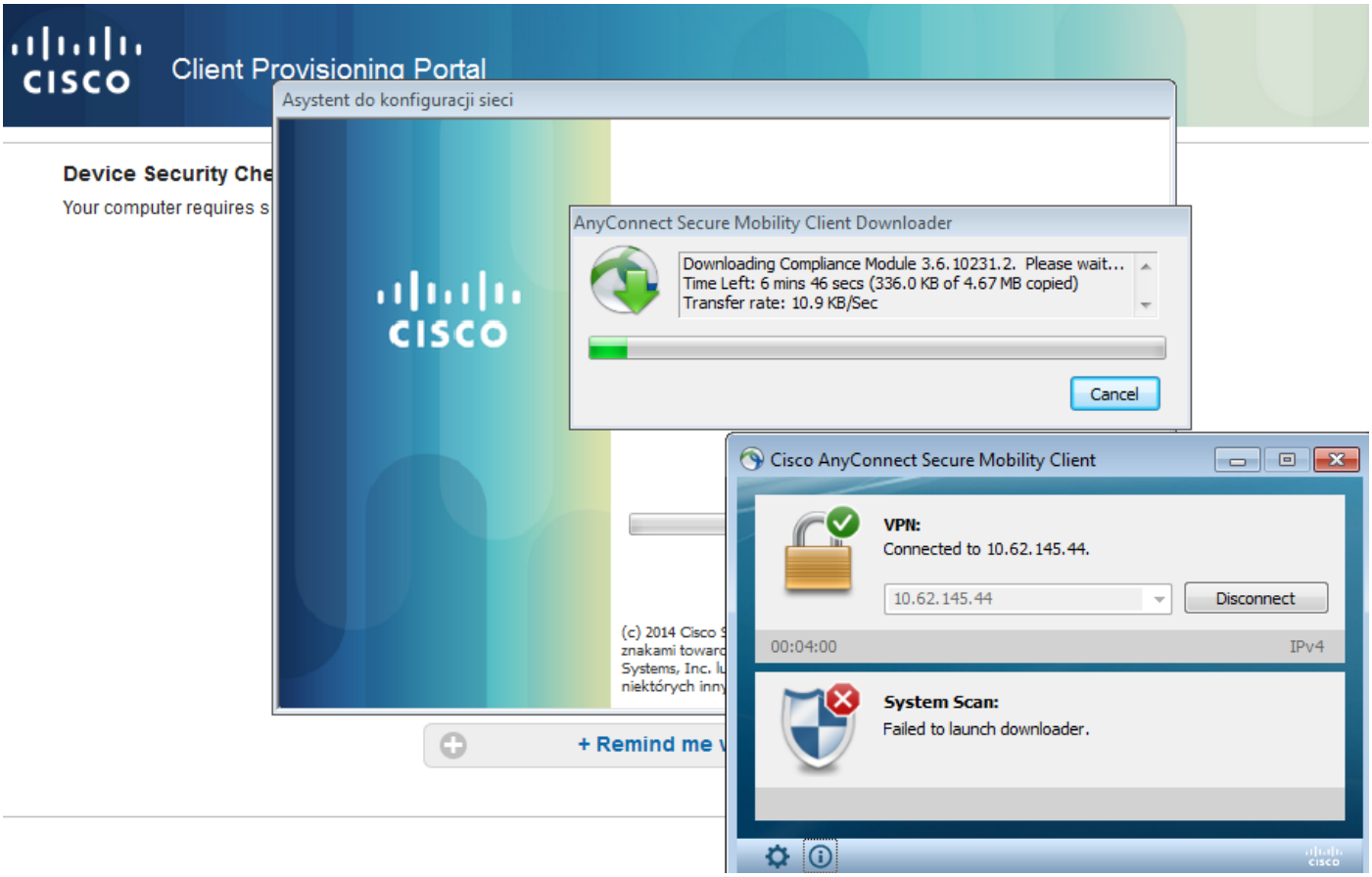
```
Login Time   : 21:29:50 UTC Sat Nov 14 2015
Duration     : 0h:56m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801010002000056647a7ce
Security Grp : none

<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
```

Aprovisionamiento del cliente Step2

En ese tráfico del buscador Web del punto final de la etapa se reorienta al ISE para el aprovisionamiento del cliente:

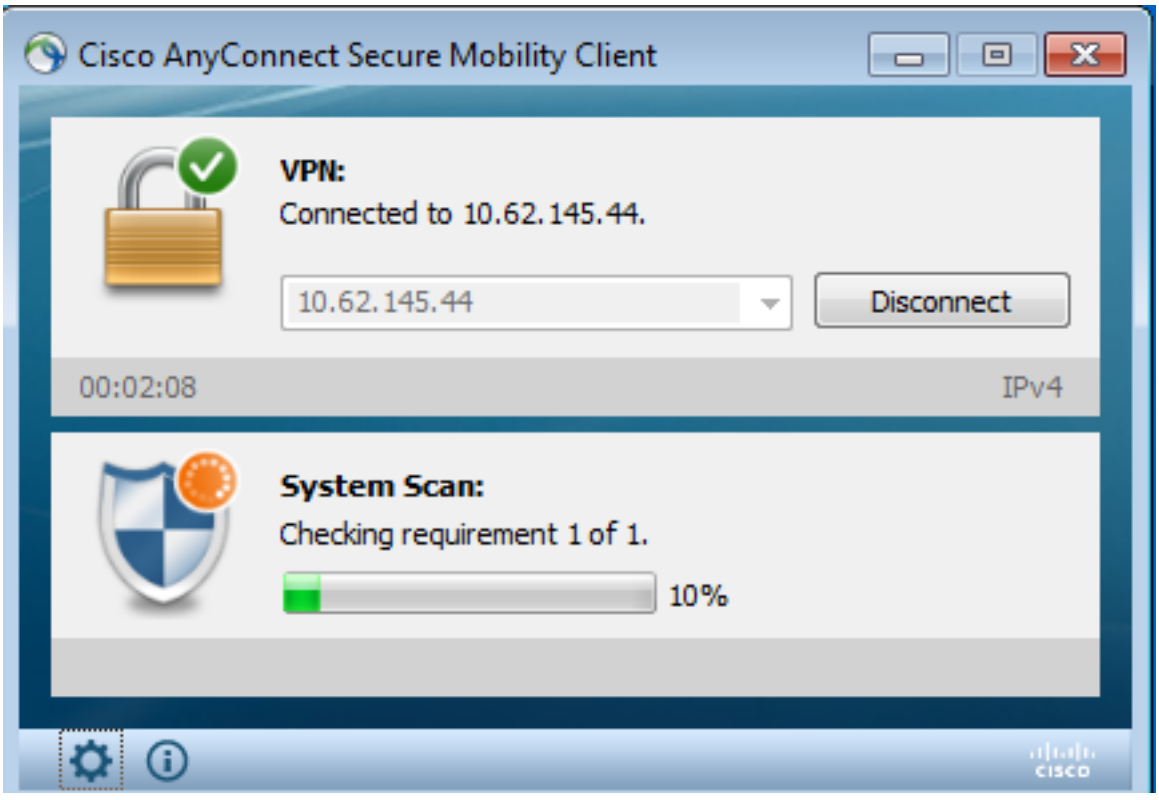


Si es necesario AnyConnect junto con el módulo de la postura y de la conformidad es actualizado:



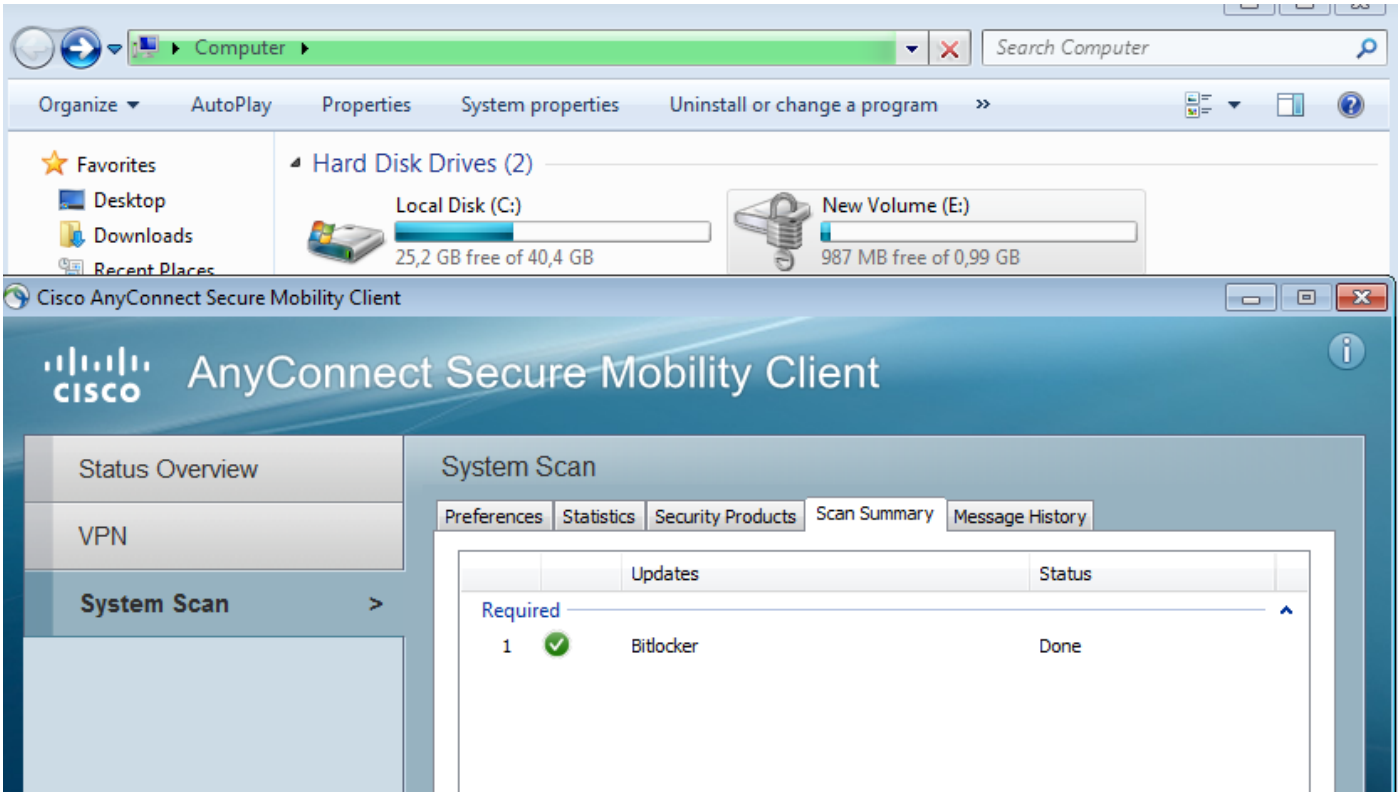
Control de la postura Step3 y CoA

El módulo de la postura se ejecuta, descubre ISE (puede ser que sea requerido para tener expediente DNS A para que enroll.cisco.com tenga éxito), descarga y marca las condiciones de la postura:

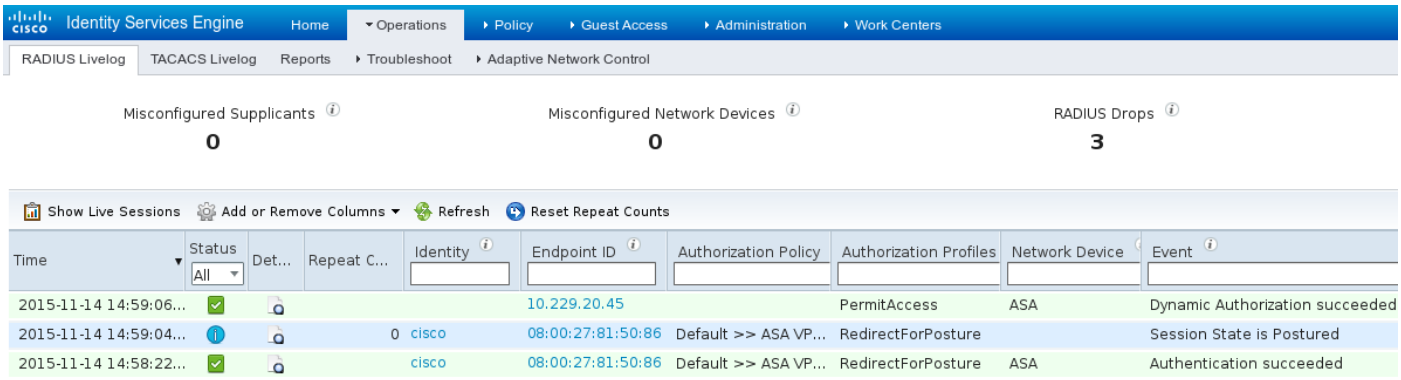


Una vez que ha confirmado eso “E: la” división es cifrada completamente por BitLocker que el

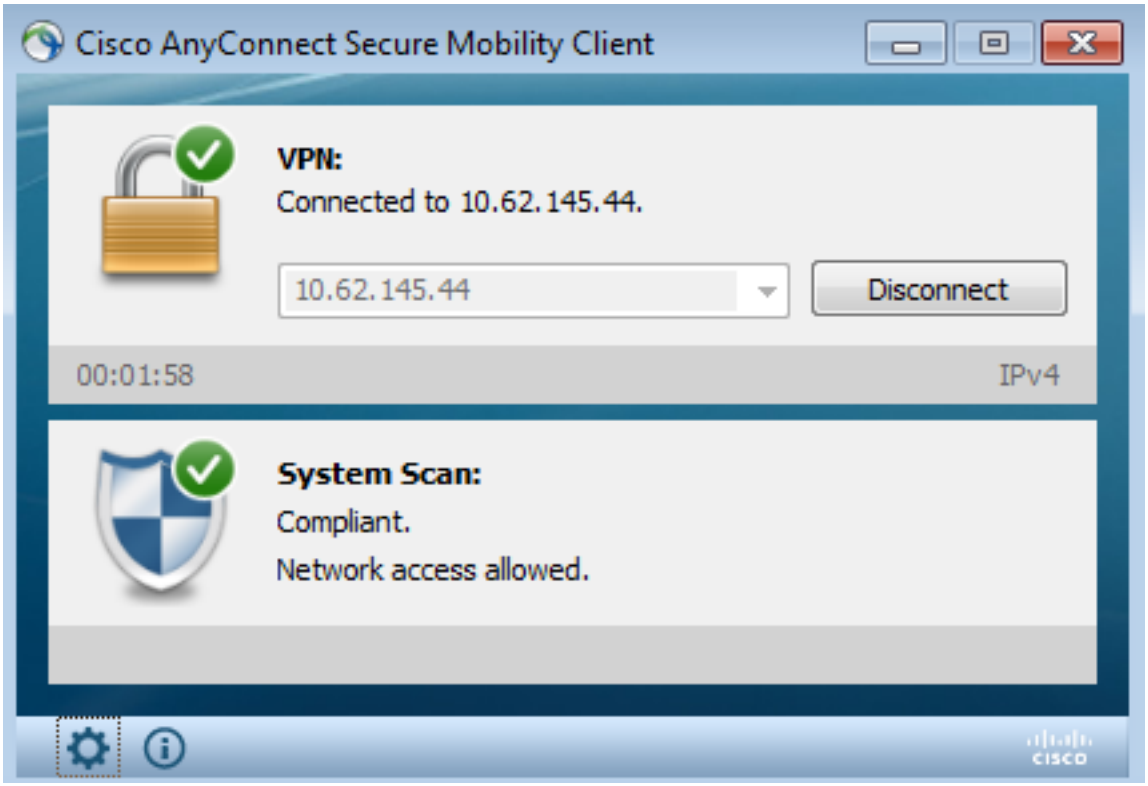
informe correcto se envía al ISE



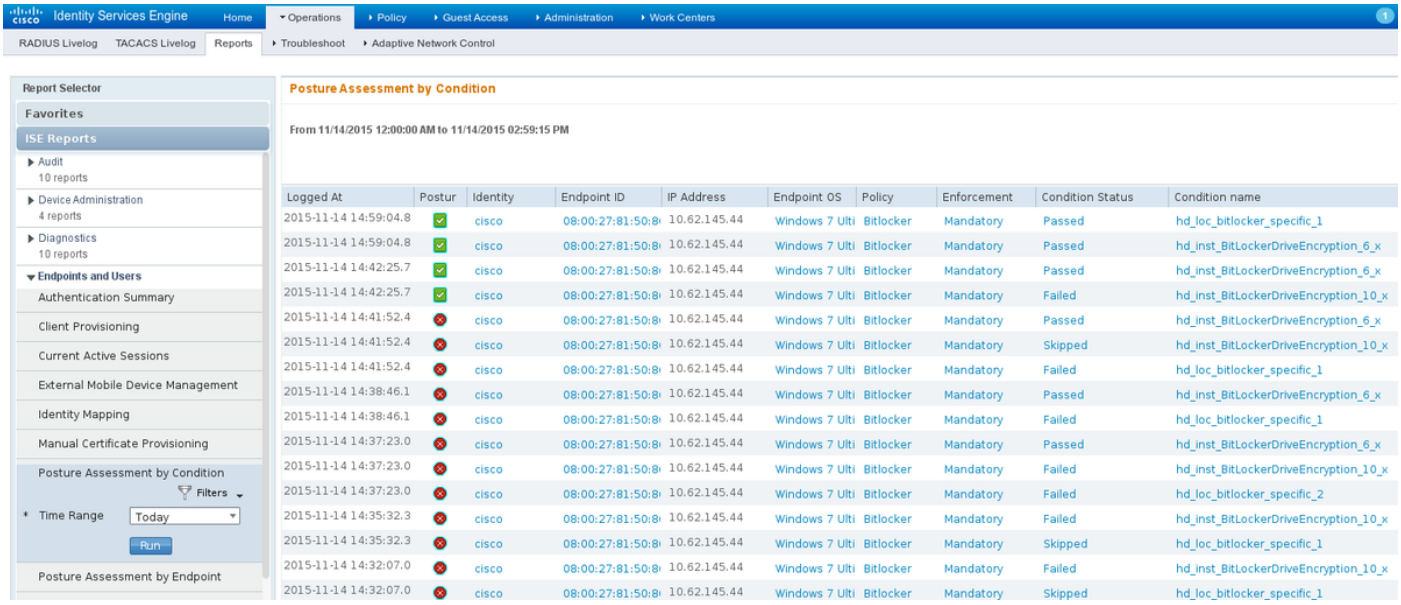
Eso está accionando a la sesión de VPN reauthorizing CoA:



El ASA quita el cambio de dirección ACL que proporciona al acceso total. AnyConnect señala la conformidad:



También los informes detallados sobre el ISE pueden confirmar que ambas condiciones están satisfechas (la *evaluación de la postura por la condición* es nuevo informe ISE 2.0 que muestra cada condición). La primera condición (*hd_inst_BitLockerDriveEncryption_6_x*) está marcando para saber si hay la instalación/el proceso, segundo (*hd_loc_bitlocker_specific_1*) está marcando si la ubicación específica ("E: ") se cifra completamente:



La evaluación de la postura ISE *por el* informe del *punto final* confirma todas las condiciones se satisface:

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

Lo mismo se podían confirmar de los debugs de ise-psc.log. Petición de la postura recibida por el ISE y la respuesta:

```
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 respuesta con el requisito de la postura (condición + corrección) está en el 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) )  &amp;amp;
(hd_loc_bitlocker_specific_1) ) )</criteria>
 </package>
</cleanmachines>
```

Después del informe cifrado es recibido por el 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><o
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>1.141.3676.0</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><**chk_status>1</chk_status**></check></package></report>]]

La estación se marca como obediente y el ISE está enviando el CoA:

```
2015-11-14 14:59:04,823 INFO   [portal-http-service28][]
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8010100017000056473ebe:::- 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
```

También la configuración final es enviada por el ISE:

```
2015-11-14 14:59:04,823 INFO   [portal-http-service28][]
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8010100017000056473ebe:::- 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
```

Esos pasos se pueden también confirmar del lado del 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 el *análisis del sistema de* AnyConnect UI de la sesión exitosa*/el historial del mensaje* señala:

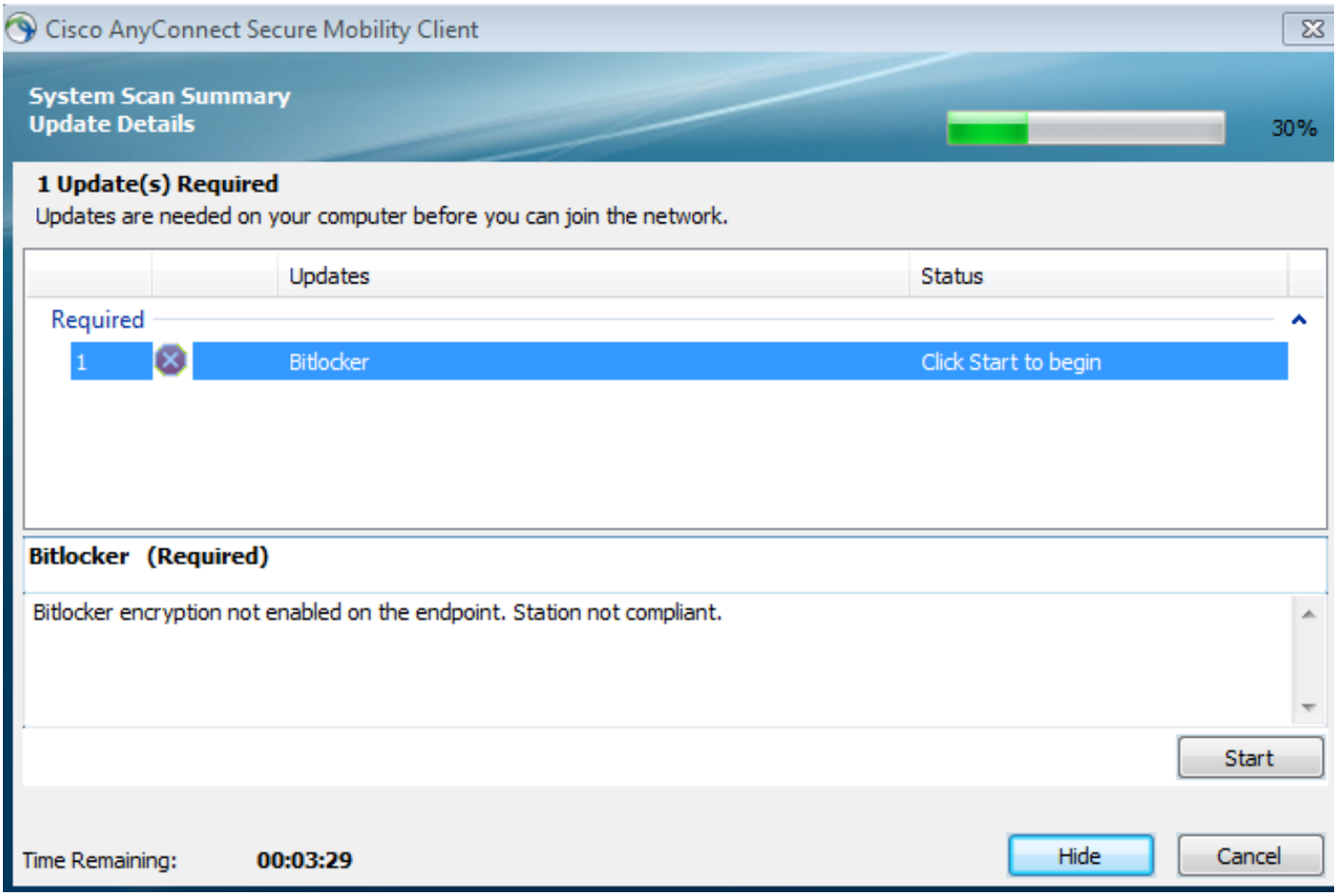
```
 14:41:59    Searching for policy server.
14:42:03    Checking for product updates...
14:42:03    The AnyConnect Downloader is performing update checks...
14:42:04    Checking for profile updates...
14:42:04    Checking for product updates...
14:42:04    Checking for customization updates...
14:42:04    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.
```

Bug

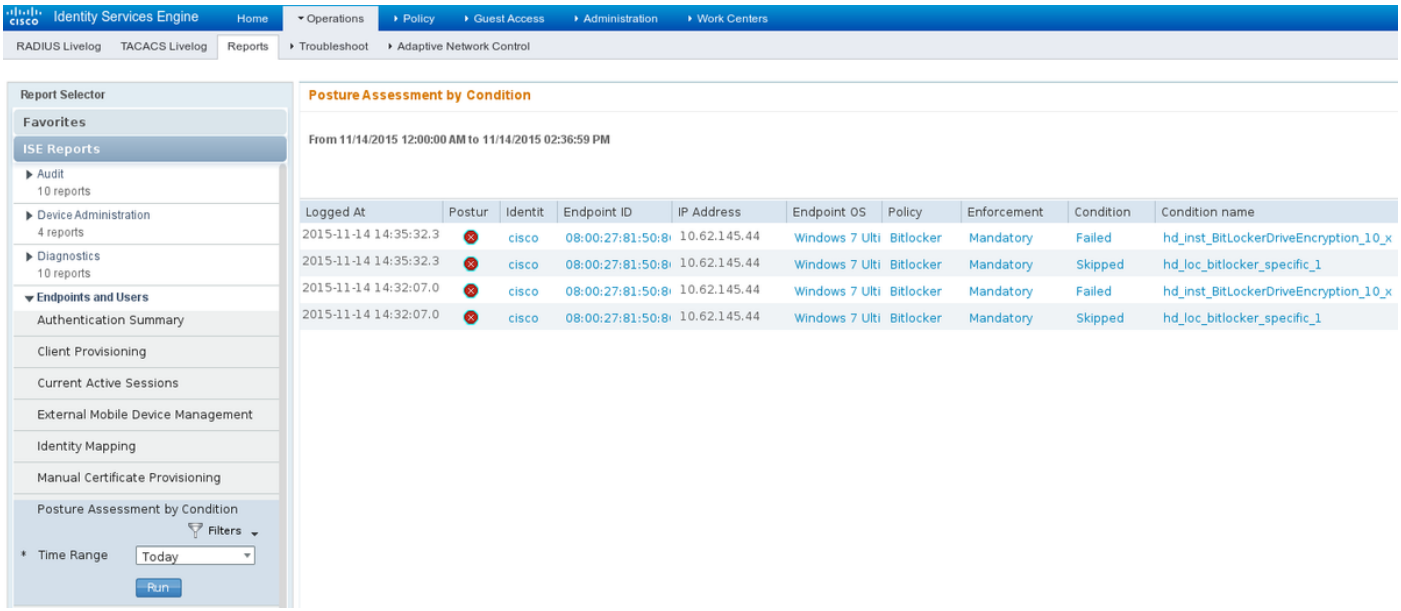
CSCux15941 - ISE 2.0 y cifrado del bitlocker de la postura AC4.2 con el fall de la ubicación (\/del char no soportado)

Troubleshooting

Si se ejecuta el punto final es que es señalado por AnyConnect UI (corrección también configurada no obediente):



El ISE puede proporcionar los detalles en las condiciones que fallan:



Lo mismo se pueden marcar de los registros CLI (los ejemplos del abren una sesión la sección verifican)

Referencias

- Configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad
- Guía de configuración CLI de la serie VPN de Cisco ASA, 9.1
- Guía del administrador del Cisco Identity Services Engine, versión 2.0
- Soporte Técnico y Documentación - Cisco Systems