配置ISE 2.0並加密AnyConnect 4.2終端安全評估位加密

目錄

簡介

本文檔介紹如何使用Microsoft BitLocker加密終端的磁碟分割槽，以及如何配置思科身份服務引擎(ISE)，以便提供網路的完全訪問許可權（僅當配置了正確的加密時）。Cisco ISE版本2.0與AnyConnect安全移動客戶端4.2支援磁碟加密狀態。

必要條件

需求

思科建議您瞭解以下主題：

- 自適應安全裝置(ASA)CLI配置和安全套接字層(SSL)VPN配置
- ASA上的遠端訪問VPN配置
- ISE和終端安全評估服務

採用元件

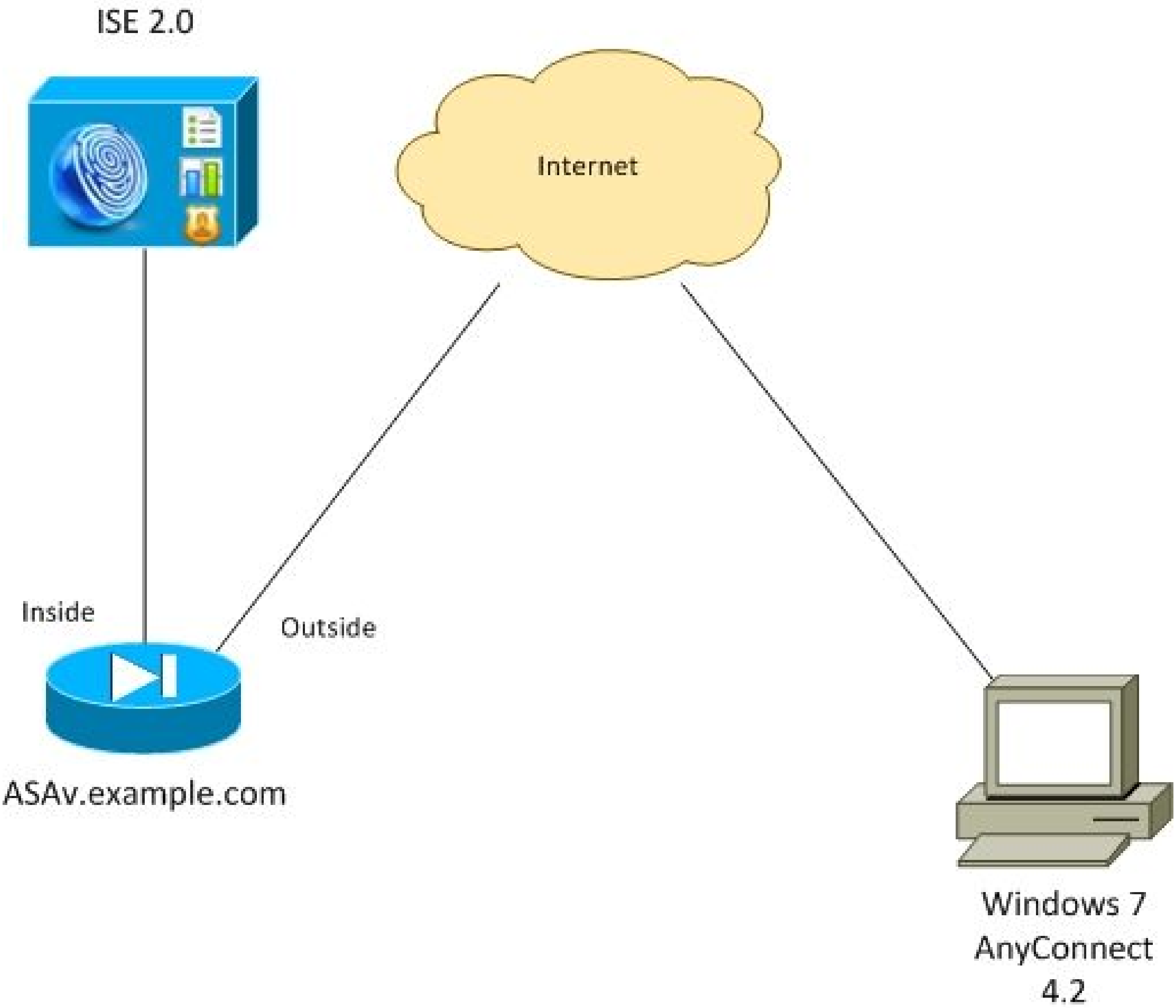
本檔案中的資訊是根據以下軟體版本：

- Cisco ASA軟體版本9.2.1及更高版本
- 搭載Cisco AnyConnect安全移動客戶端版本4.2及更高版本的Microsoft Windows版本7
- Cisco ISE 2.0版及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



流程如下：

- 由AnyConnect客戶端發起的VPN會話通過ISE進行身份驗證。終端的狀態未知，規則**ASA VPN unknown**命中，因此會話重定向到ISE進行調配

- 使用者開啟Web瀏覽器，ASA將HTTP流量重定向到ISE。ISE將最新版本的AnyConnect以及狀態和合規性模組推送到終端

- 執行狀態模組後，它會檢查分割槽**E:**由BitLocker完全加密。如果是，則報告被傳送到ISE，ISE觸發Radius授權更改(CoA)而無任何ACL（完全訪問）

- ASA上的VPN會話已更新，重定向ACL已刪除，且該會話具有完全訪問許可權

以VPN會話為例。狀態功能對其他型別的訪問也工作正常。

ASA

它配置為使用ISE作為身份驗證、授權和記帳(AAA)伺服器的遠端SSL VPN訪問。需要設定Radius CoA以及重新導向ACL:

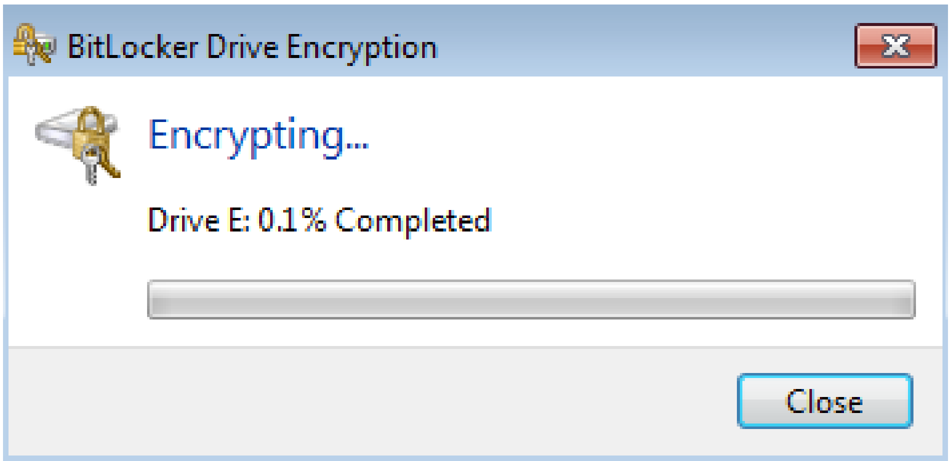
```
aaa-server ISE20 protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE20 (inside) host 10.48.17.235
 key cisco

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
```

有關詳細資訊，請參閱：

AnyConnect 4.0與ISE 1.3版整合配置示例

Windows 7上的BitLocker

導航到**控制面板>系統和安全> BitLocker驅動器加密**，啟用**E:**分割槽加密。使用密碼(PIN)對其進行保護，如下圖所示。

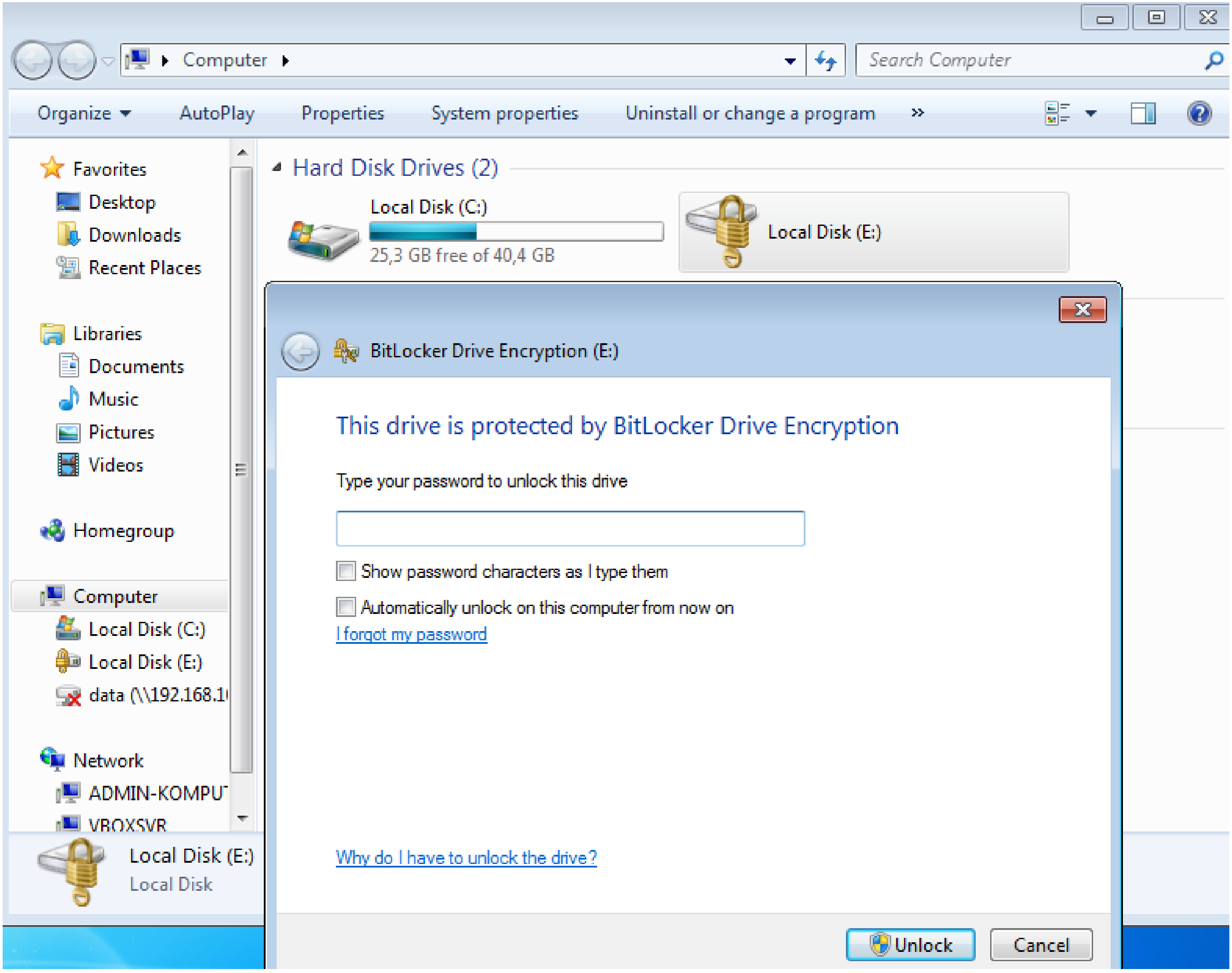


BitLocker Drive Encryption

Encrypting...

Drive E: 0.1% Completed

加密後，請將其裝入（提供密碼），並確保可訪問它，如下圖所示。



BitLocker Drive Encryption (E:)

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?

有關詳細資訊，請遵循Microsoft文檔：

[Windows BitLocker驅動器加密分步指南]

ISE

步驟1.網路裝置

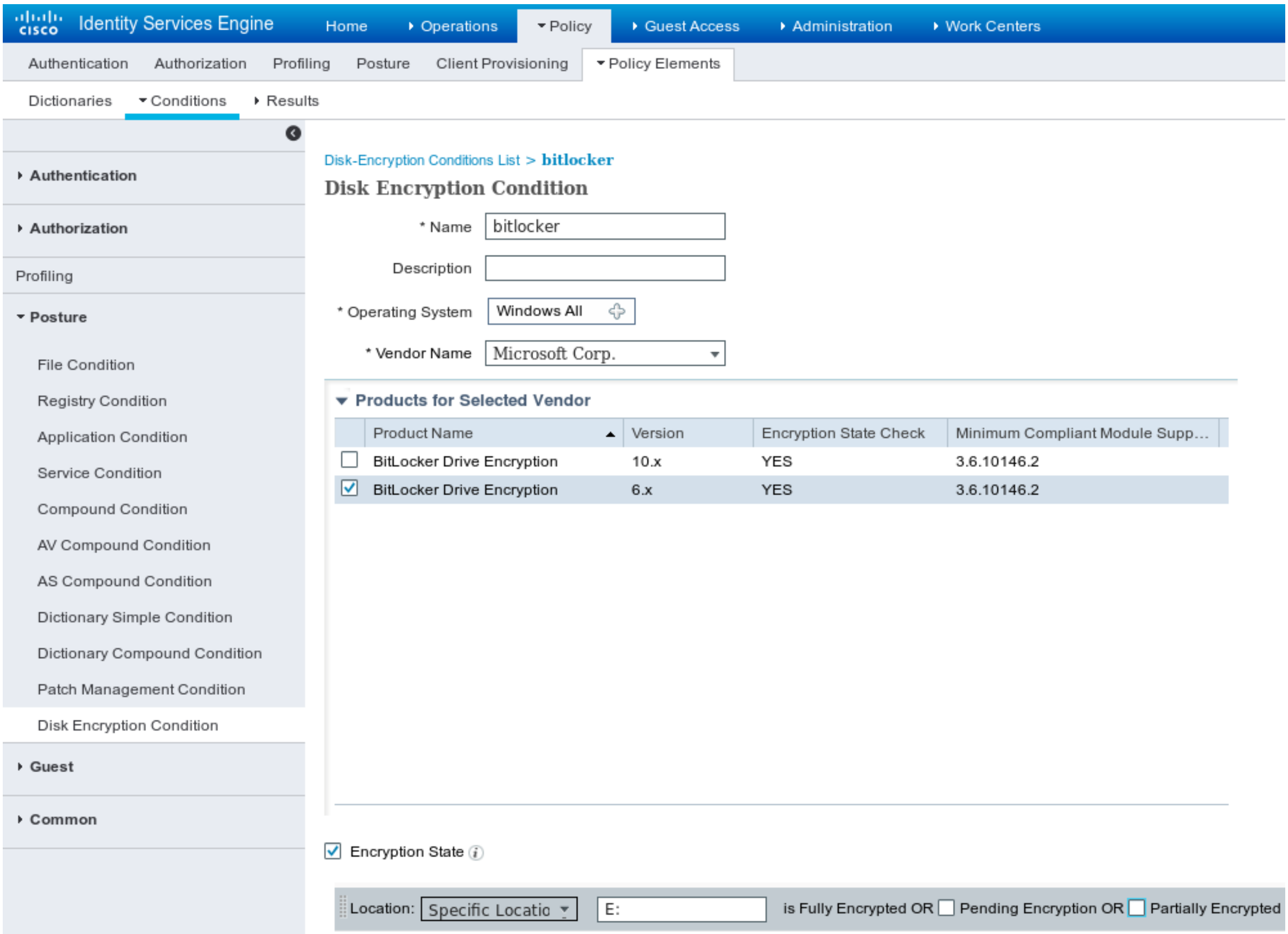
導航到**Administration > Network Resources > Network Devices**, Add **ASA with Device Type = ASA**。這在授權規則中用作條件，但不是強制條件（可以使用其他型別的條件）。

如果適用，網路裝置組不存在。若要建立，請導航到**管理>網路資源>網路裝置組**。

步驟2.狀態條件和策略

確保狀態條件已更新：導航到**Administration > System > Settings > Posture > Updates > Update Now**。

導覽至**Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition**，新增條件，如下圖所示。



Disk-Encryption Conditions List > **bitlocker**

Disk Encryption Condition

* Name	bitlocker
Description	
* Operating System	Windows All
* Vendor Name	Microsoft Corp.

Products for Selected Vendor

	Product Name	Version	Encryption State Check	Minimum Compliant Module Supp…
□	BitLocker Drive Encryption	10.x	YES	3.6.10146.2
☑	BitLocker Drive Encryption	6.x	YES	3.6.10146.2

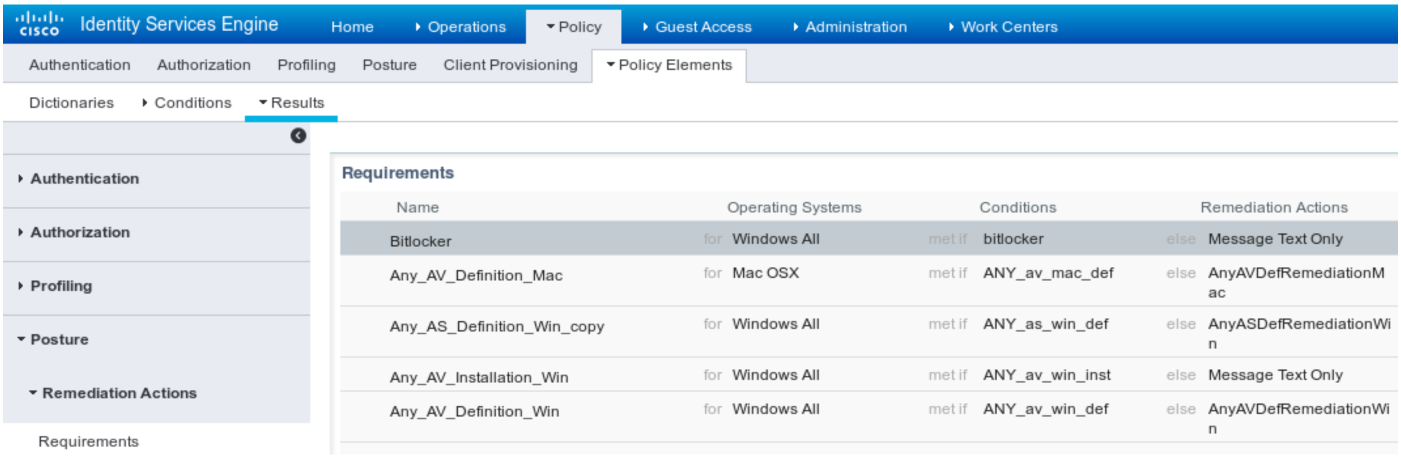
☑ Encryption State

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

此條件檢查是否已安裝用於Windows 7的BitLocker，以及**E:**分割槽已完全加密。

附註：BitLocker是磁碟級加密，不支援帶有路徑引數的特定位置，僅支援磁碟字母。

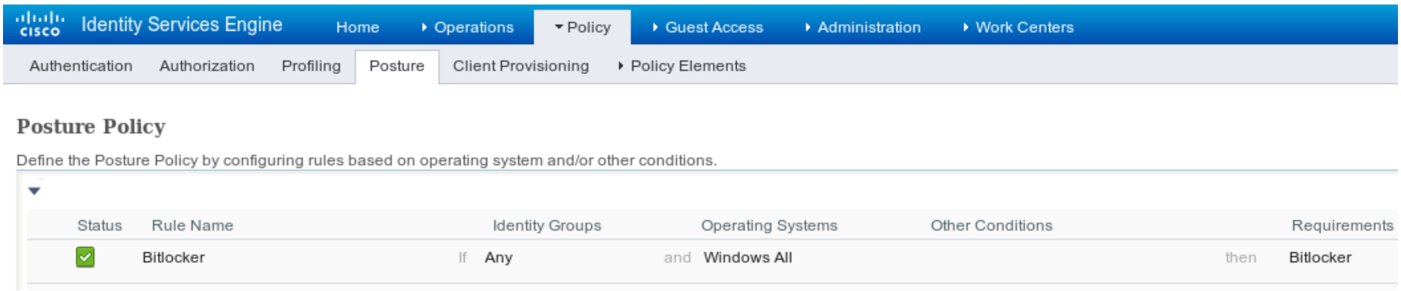
導覽至**Policy > Policy Elements > Results > Posture > Requirements**，以建立一個使用如圖所示條件的新要求。



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

導覽至**Policy > Posture**，為所有Windows新增條件以使用需求，如下圖所示。



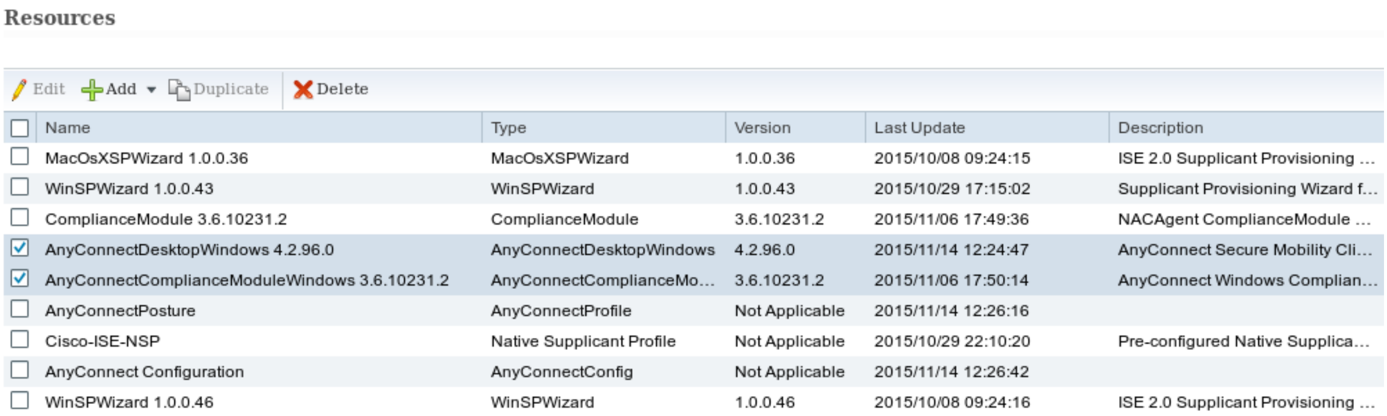
Posture Policy

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
☑	Bitlocker	If	Any	and	Windows All		then	Bitlocker

步驟3.客戶端調配資源和策略

導覽至**Policy > Policy Elements > Client Provisioning > Resources**，從Cisco.com下載**Compliance Module**，然後手動上傳**AnyConnect 4.2軟體包**，如下圖所示。

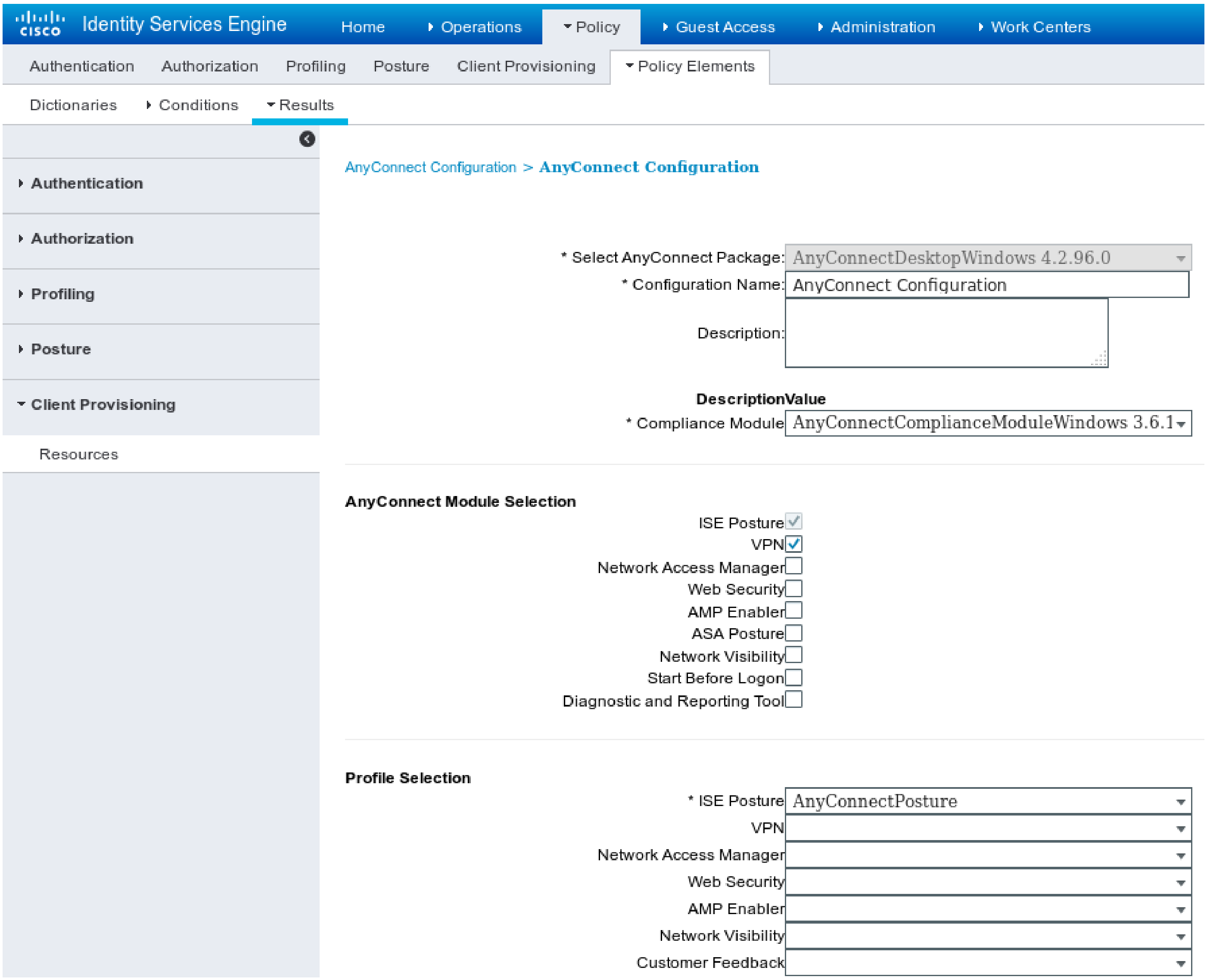


Resources

□	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 ...
☑	AnyConnectDesktopWindows 4.2.96.0	AnyConnectDesktopWindows	4.2.96.0	2015/11/14 12:24:47	AnyConnect Secure Mobility Cli...
☑	AnyConnectComplianceModuleWindows 3.6.10231.2	AnyConnectComplianceMo...	3.6.10231.2	2015/11/06 17:50:14	AnyConnect Windows Complian...
□	AnyConnectPosture	AnyConnectProfile	Not Applicable	2015/11/14 12:26:16	
□	Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2015/10/29 22:10:20	Pre-configured Native Supplica...
□	AnyConnect Configuration	AnyConnectConfig	Not Applicable	2015/11/14 12:26:42	
□	WinSPWizard 1.0.0.46	WinSPWizard	1.0.0.46	2015/10/08 09:24:16	ISE 2.0 Supplicant Provisioning ...

導航到**Add > NAC Agent或AnyConnect Posture Profile**，建立AnyConnect Posture profile(名稱：**AnyConnectPosture**)。

導航到**Add > AnyConnect Configuration**，新增AnyConnect配置檔案(名稱：**AnyConnect配置**)，如下圖所示。



AnyConnect Configuration > **AnyConnect Configuration**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.96.0

* Configuration Name: AnyConnect Configuration

Description:

DescriptionValue

* Compliance Module AnyConnectComplianceModuleWindows 3.6.1

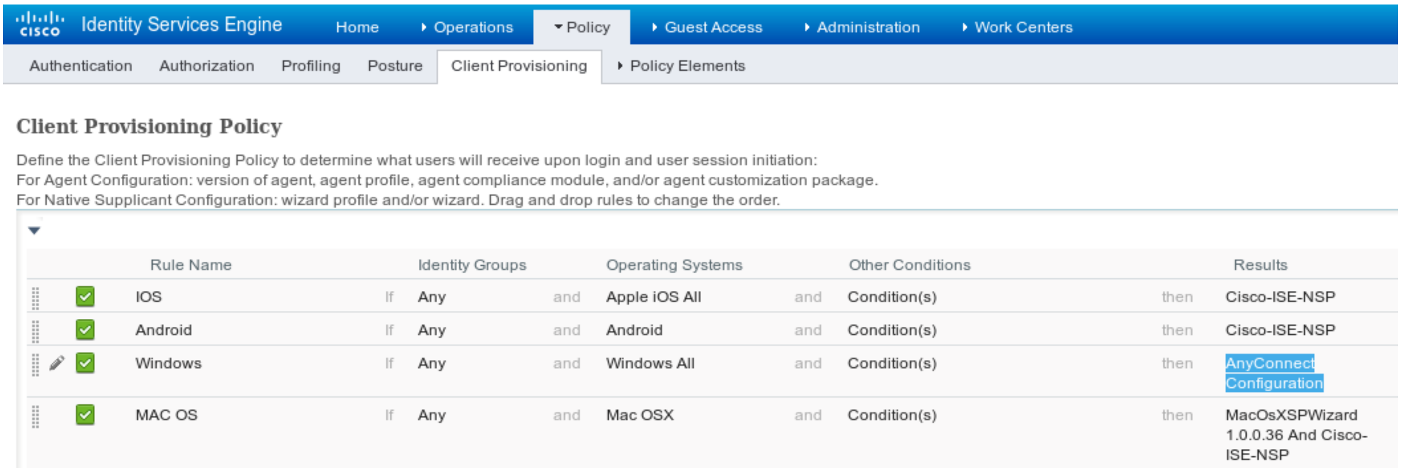
AnyConnect Module Selection

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

導覽至**Policy > Client Provisioning**，並修改Windows的預設策略，以便使用已配置的AnyConnect配置檔案，如下圖所示。



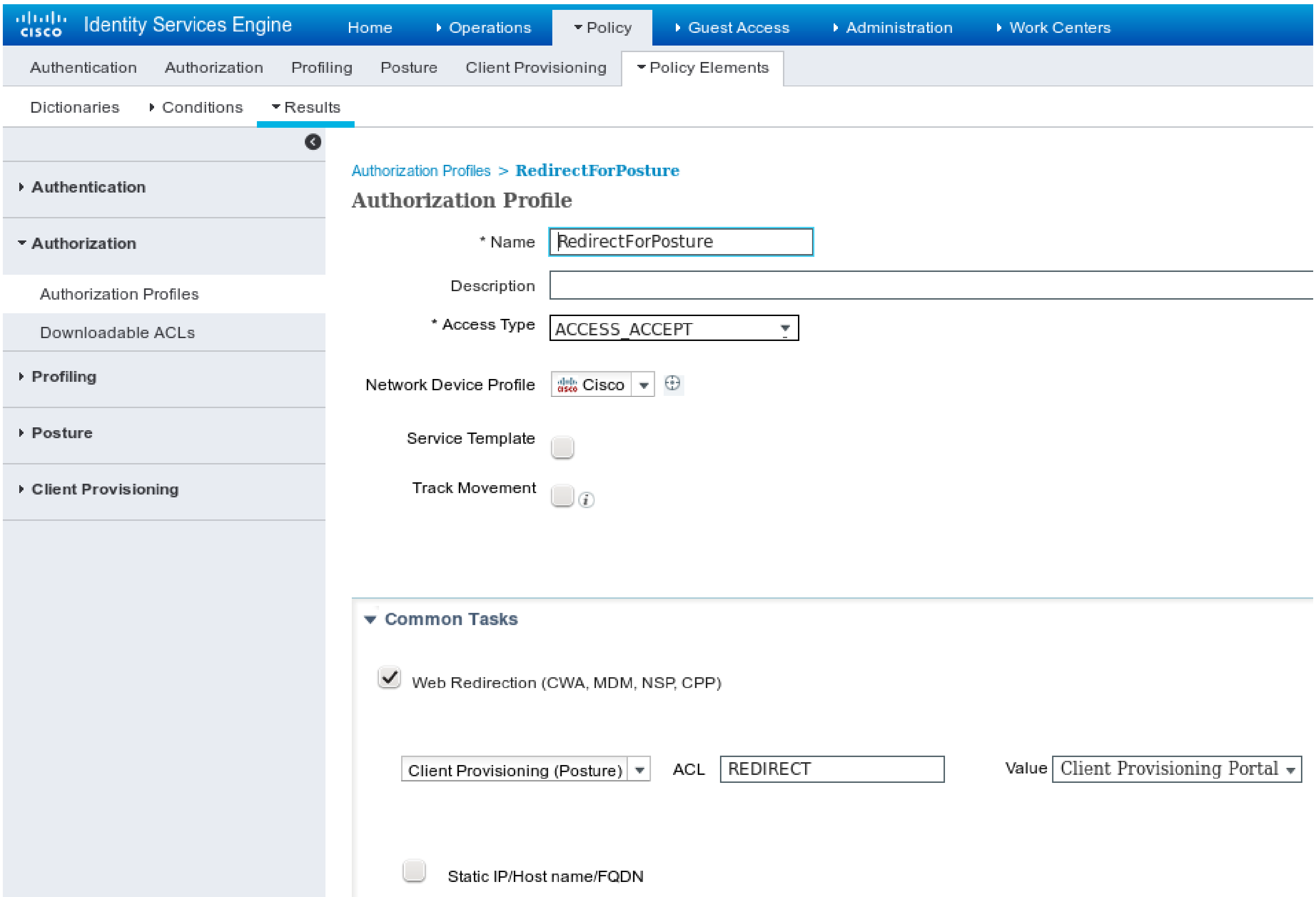
Client Provisioning Policy

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

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	AnyConnect Configuration
☑	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	MacOsXSPWizard 1.0.0.36 And Cisco-ISE-NSP

步驟4.授權規則

導航到**Policy > Policy Elements > Results > Authorization**，新增授權配置檔案(名稱：**RedirectForPosture**)，重定向到預設客戶端調配門戶，如下圖所示。



Authorization Profiles > RedirectForPosture

Authorization Profile

* Name: RedirectForPosture

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: □

Track Movement: □

Common Tasks

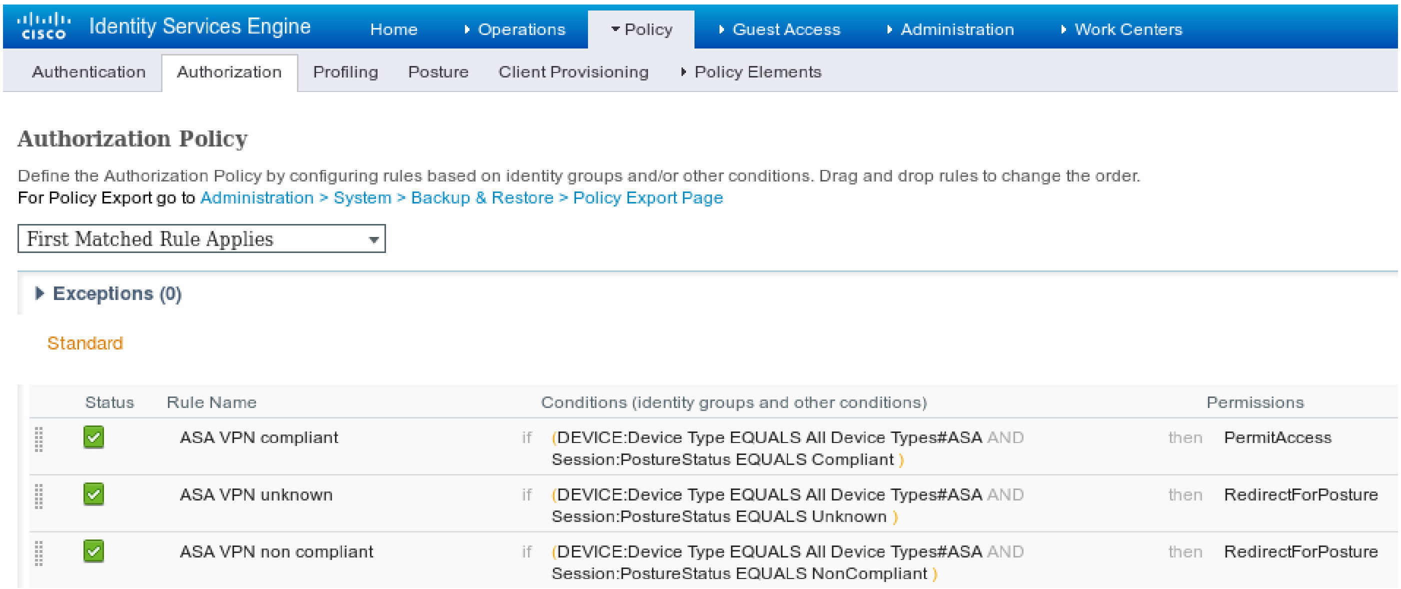
☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: REDIRECT Value: Client Provisioning Portal

□ Static IP/Host name/FQDN

REDIRECT ACL在ASA上定義。

導覽至**Policy > Authorization**，建立3個授權規則，如下圖所示。



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	ASA VPN compliant	if	(DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Compliant)	then	PermitAccess
☑	ASA VPN unknown	if	(DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Unknown)	then	RedirectForPosture
☑	ASA VPN non compliant	if	(DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS NonCompliant)	then	RedirectForPosture

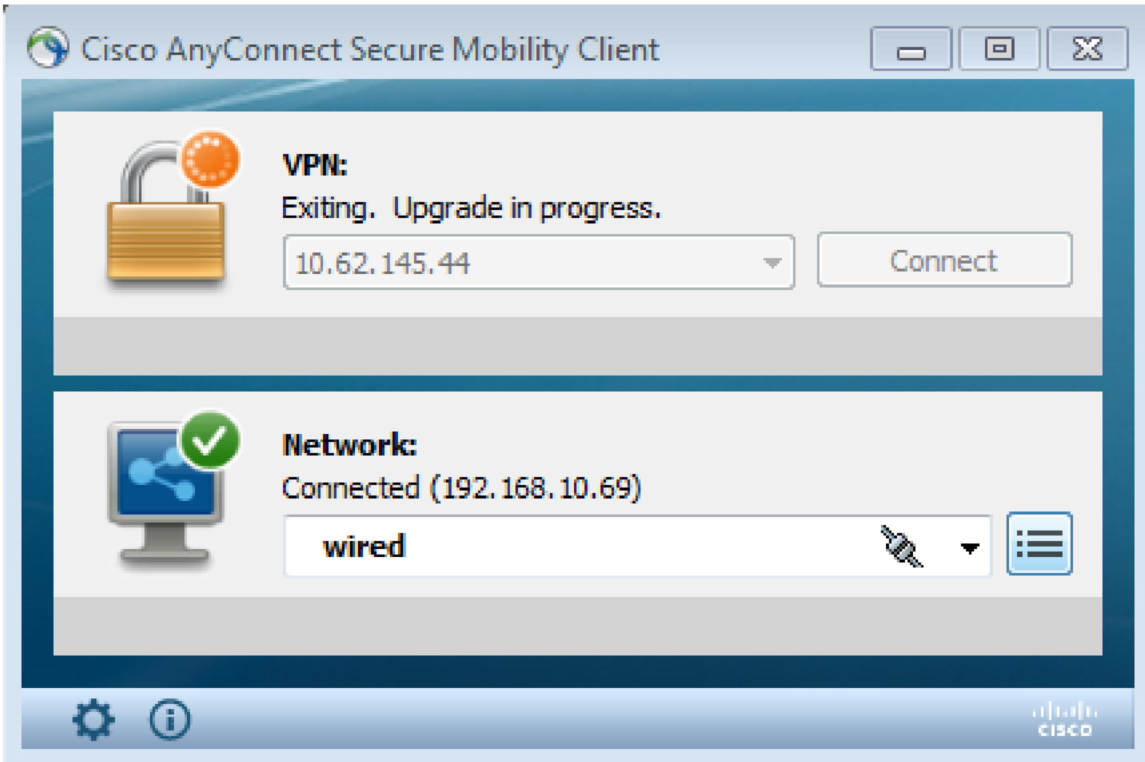
如果終端符合要求，則提供完全訪問。如果狀態未知或不相容，將返回客戶端預配的重定向。

驗證

使用本節內容，確認您的組態是否正常運作。

步驟1. VPN會話建立

建立VPN會話後，ASA可能希望執行AnyConnect模組的升級，如下圖所示。



Cisco AnyConnect Secure Mobility Client

VPN:
Exiting. Upgrade in progress.

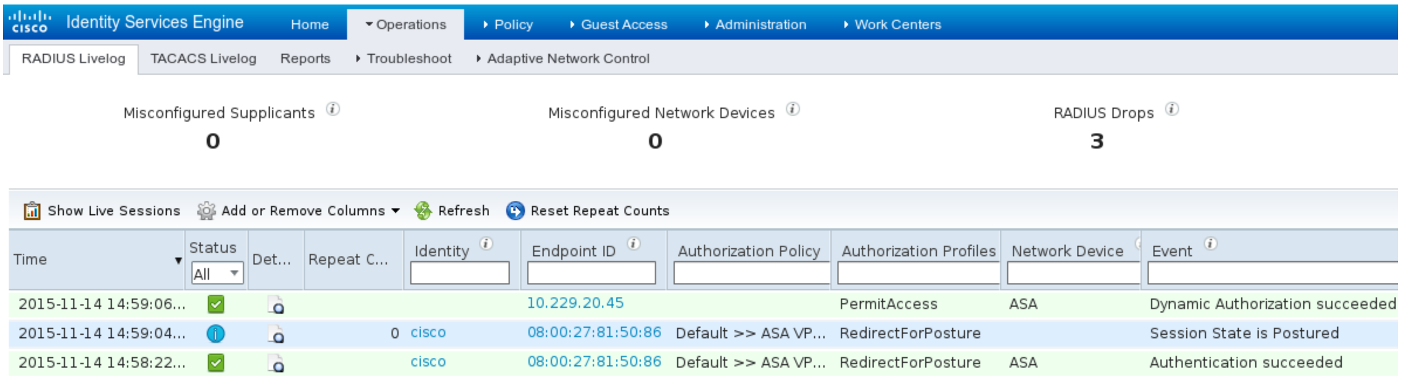
10.62.145.44

Connect

Network:
Connected (192.168.10.69)

wired

在ISE上，最後一條規則被命中，結果**RedirectForPosture**許可權被返回，如下圖所示。



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 3

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

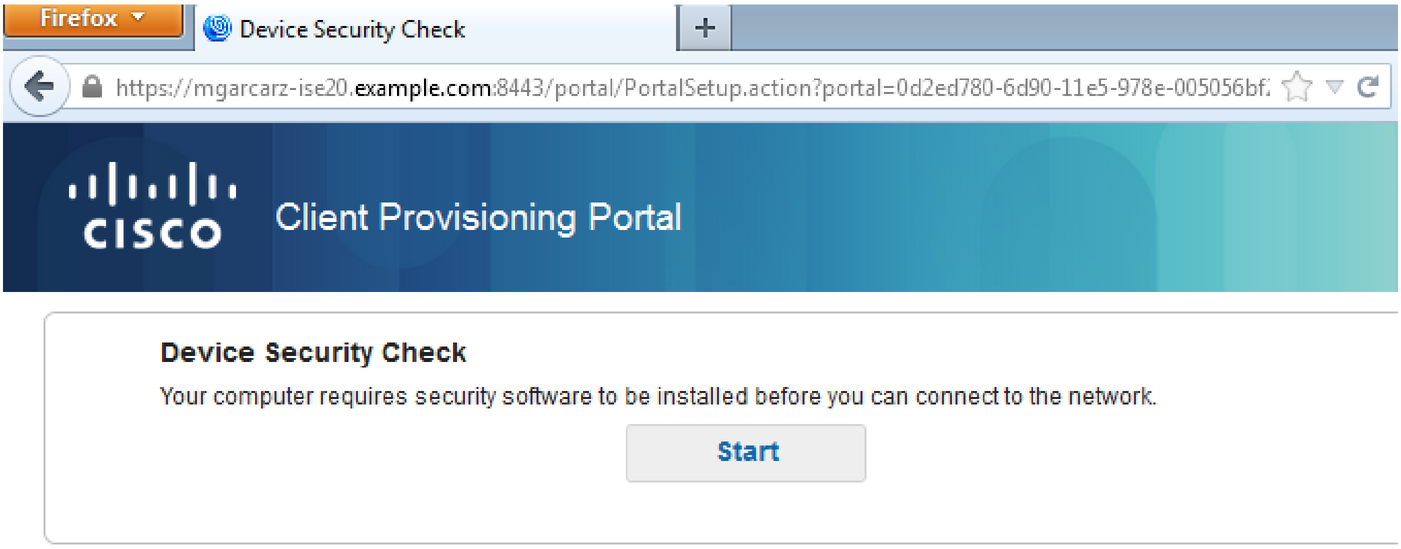
ASA完成VPN會話構建後，會報告必須發生重定向：

```
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 : c0a801010000200005647a7ce
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
```

步驟2.客戶端調配

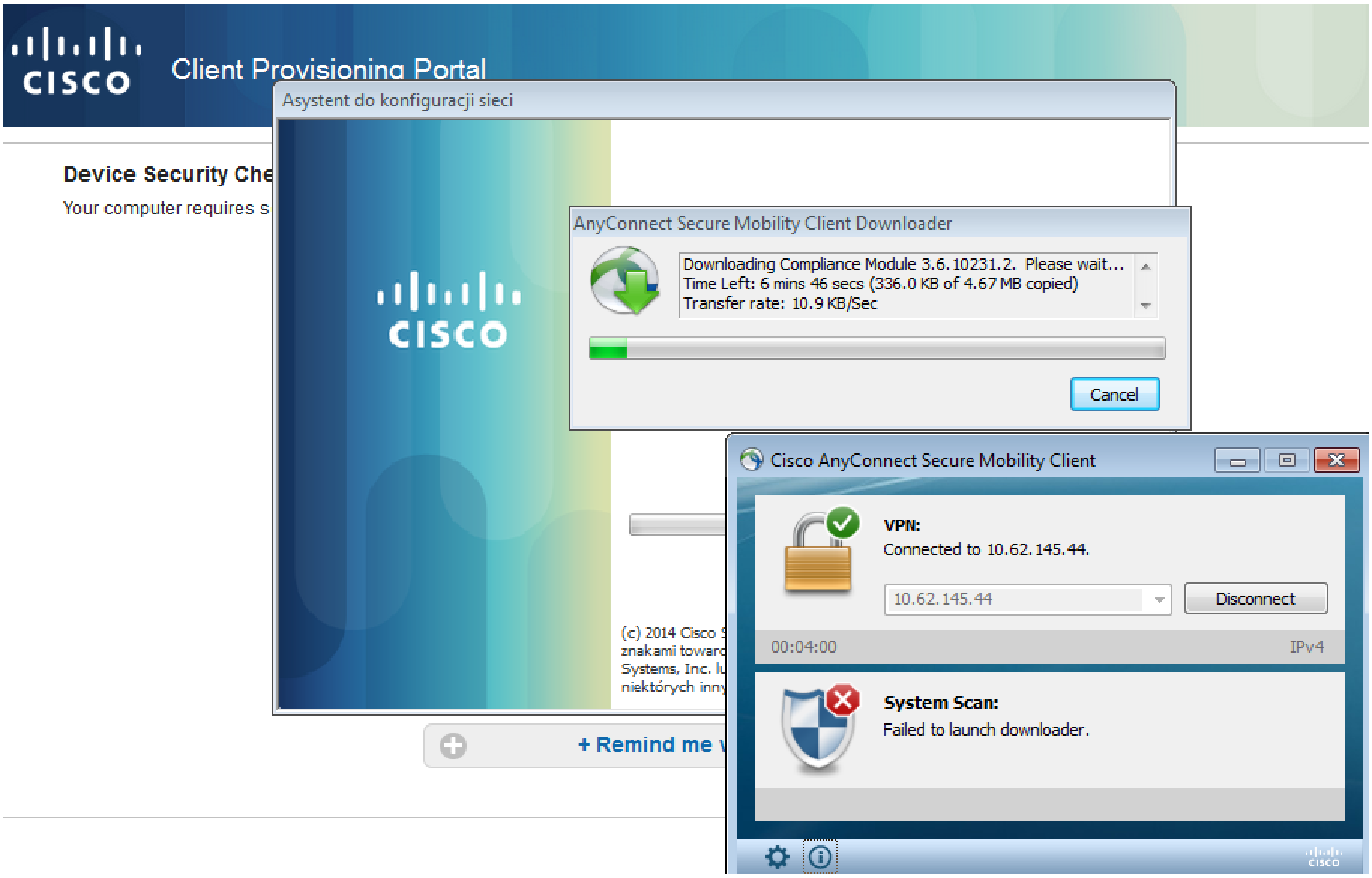
在此階段，終端Web瀏覽器流量重定向到ISE進行客戶端調配，如圖所示。


Firefox
Device Security Check
https://mgarcarz-ise20.example.com:8443/portal/PortalSetup.action?portal=0d2ed780-6d90-11e5-978e-005056bf
Client Provisioning Portal
Start

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

如果需要，會更新AnyConnect以及Posture and compliance模組，如下圖所示。



Client Provisioning Portal
Asystent do konfiguracji sieci
AnyConnect Secure Mobility Client Downloader
Cancel
Cisco AnyConnect Secure Mobility Client
Disconnect
+ Remind me v

Device Security Che

Your computer requires s

Downloading Compliance Module 3.6.10231.2. Please wait...
Time Left: 6 mins 46 secs (336.0 KB of 4.67 MB copied)
Transfer rate: 10.9 KB/Sec

(c) 2014 Cisco S
znakami toward
Systems, Inc. lu
niektórych inny

VPN:
Connected to 10.62.145.44.

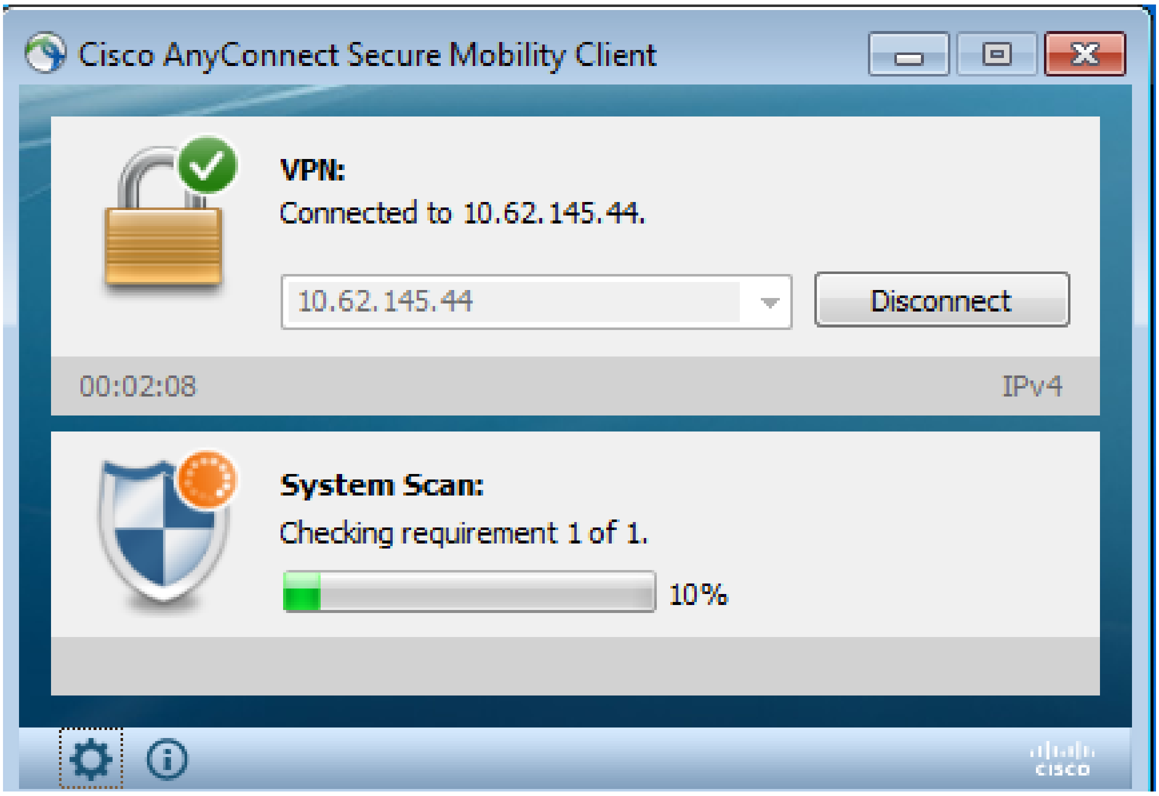
10.62.145.44

00:04:00 IPv4

System Scan:
Failed to launch downloader.

步驟3.狀態檢查和CoA

執行狀態模組，發現ISE(可能需要為enroll.cisco.com設定DNS A記錄才能成功)，下載並檢查狀態條件，如圖所示。



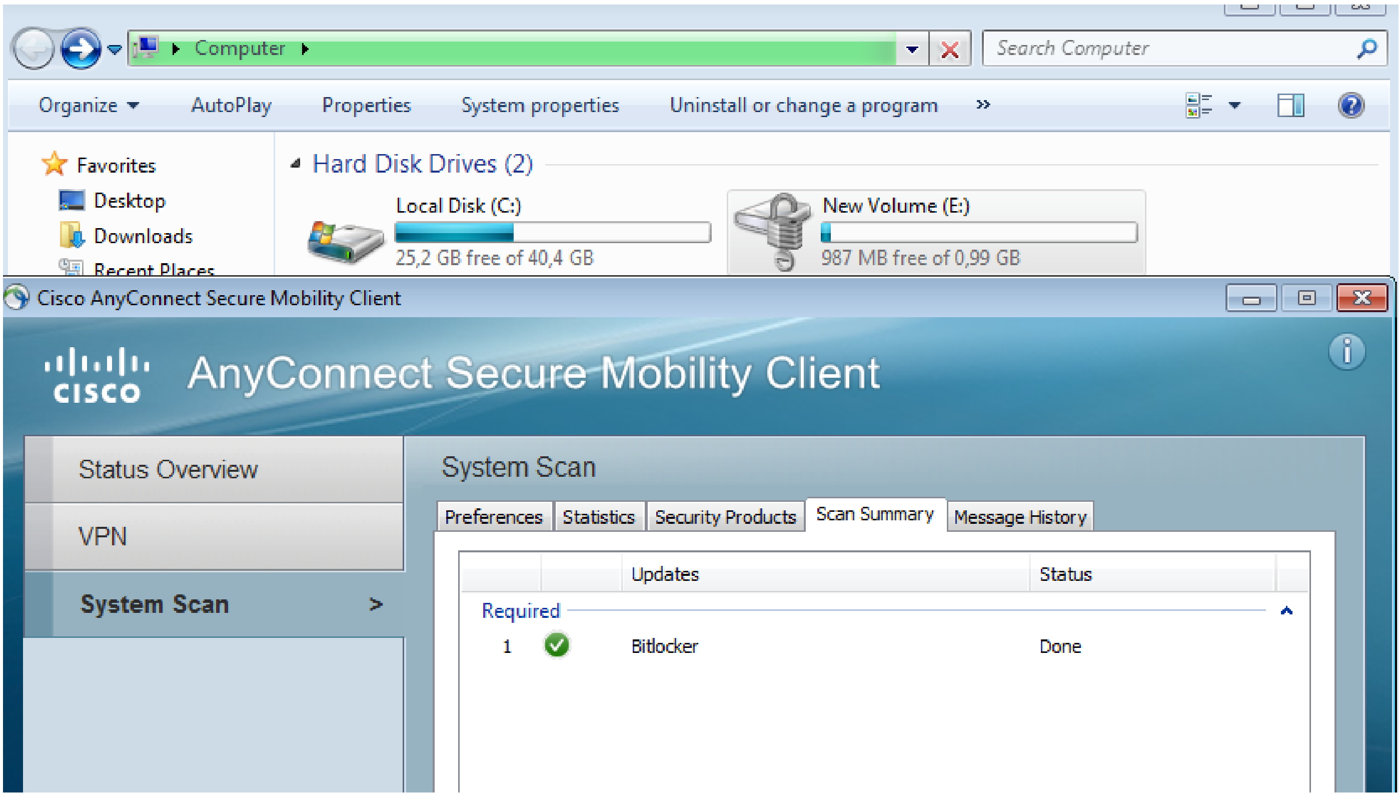
VPN:
Connected to 10.62.145.44.

10.62.145.44

00:02:08 IPv4

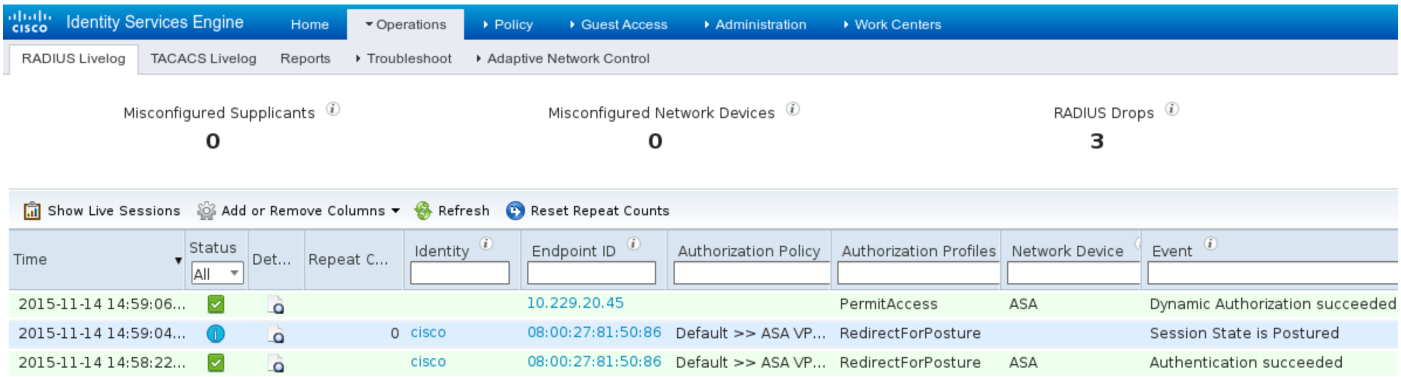
System Scan:
Checking requirement 1 of 1.
10%

一旦確認E:分割槽由BitLocker完全加密，正確的報告將傳送到ISE，如下圖所示。



		Updates	Status
Required			
1	✓	Bitlocker	Done

這會觸發CoA重新授權VPN會話，如圖所示。



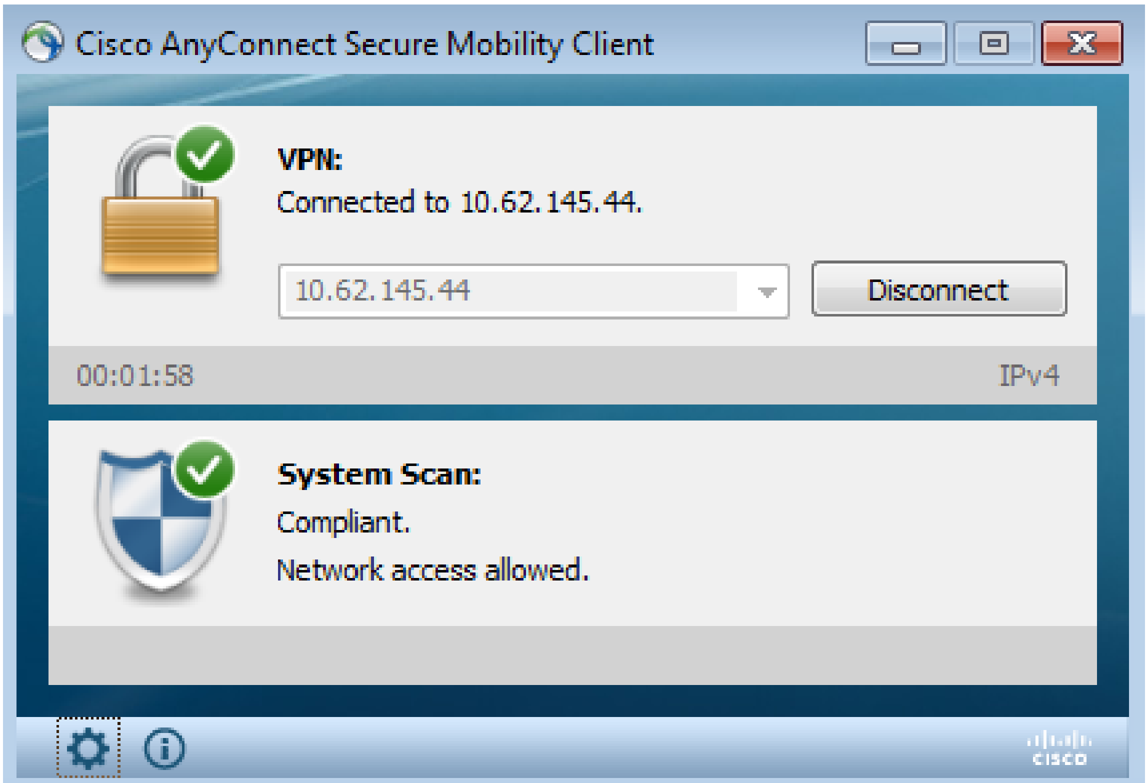
Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 3

Time	Status All	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

ASA刪除提供完全訪問許可權的重定向ACL。AnyConnect報告合規性，如下圖所示。



Cisco AnyConnect Secure Mobility Client

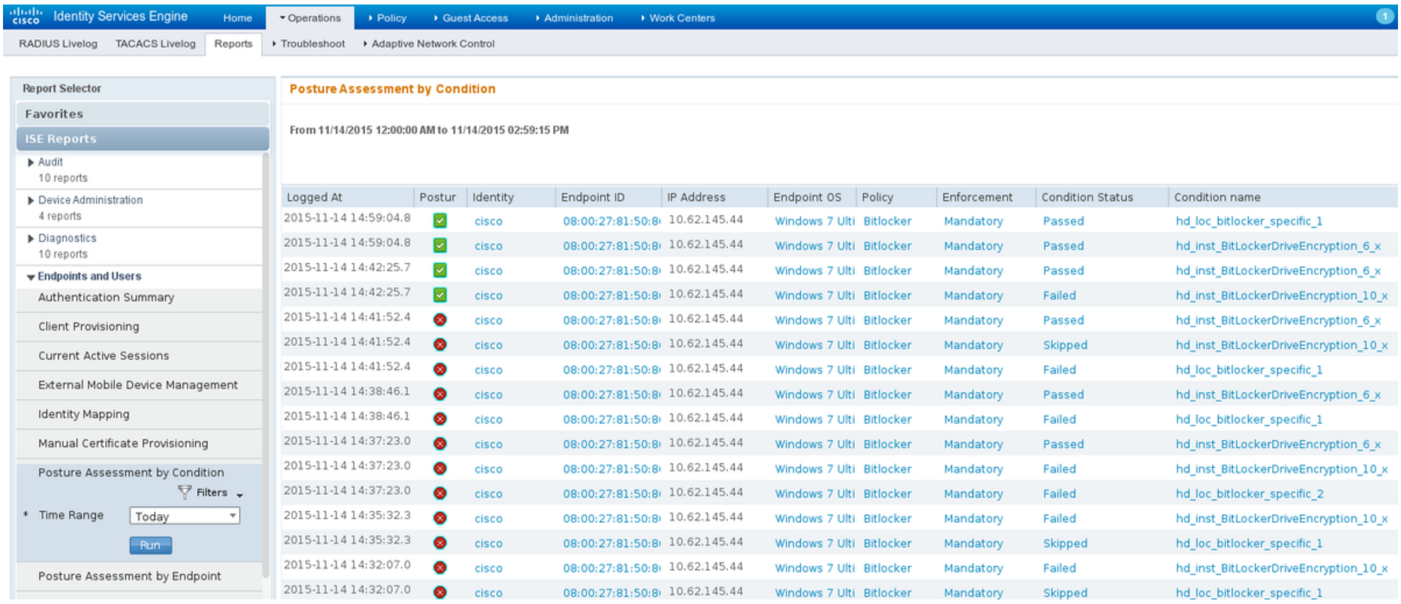
VPN:
Connected to 10.62.145.44.

10.62.145.44

00:01:58 IPv4

System Scan:
Compliant.
Network access allowed.

此外，有關ISE的詳細報告可以確認兩個條件都得到了滿足(**Posture Assessment by Condition**是顯示每個條件的新ISE 2.0報告)。 第一個條件(**hd_inst_BitLockerDriveEncryption_6_x**)檢查安裝/處理過程，第二個條件(**hd_loc_bitlocker_specific_1**)檢查特定位置(E:)是否已完全加密，如下圖所示。



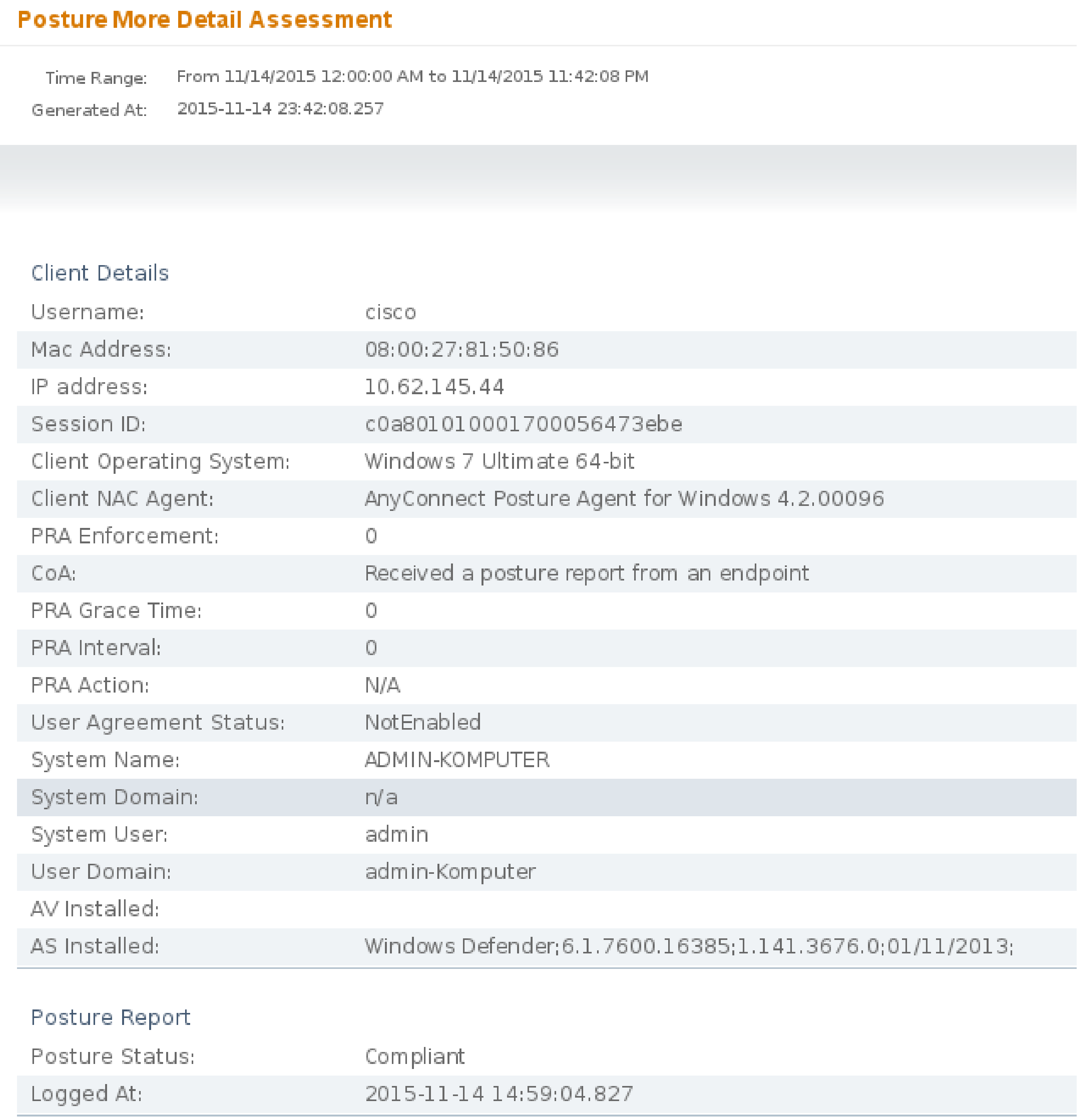
Time Range: Today

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**報告確認滿足所有條件，如圖所示。



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

可從ise-psc.log debugs中確認相同情況。ISE接收的終端安全評估請求和響應：

```
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) )
```

具有狀態要求（條件+補救）的響應採用XML格式：

```
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) )  &amp;
(hd_loc_bitlocker_specific_1) ) )</criteria>
 </package>
</cleanmachines>
```

ISE收到加密報告後：

```
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>1.141.36
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> ]]
```

站點被標籤為符合，ISE傳送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
```

此外，最終配置由ISE傳送：

```
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--> ]]
```

也可以從客戶端(AnyConnect DART)確認這些步驟：

```
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 ... ]

******************************************
```

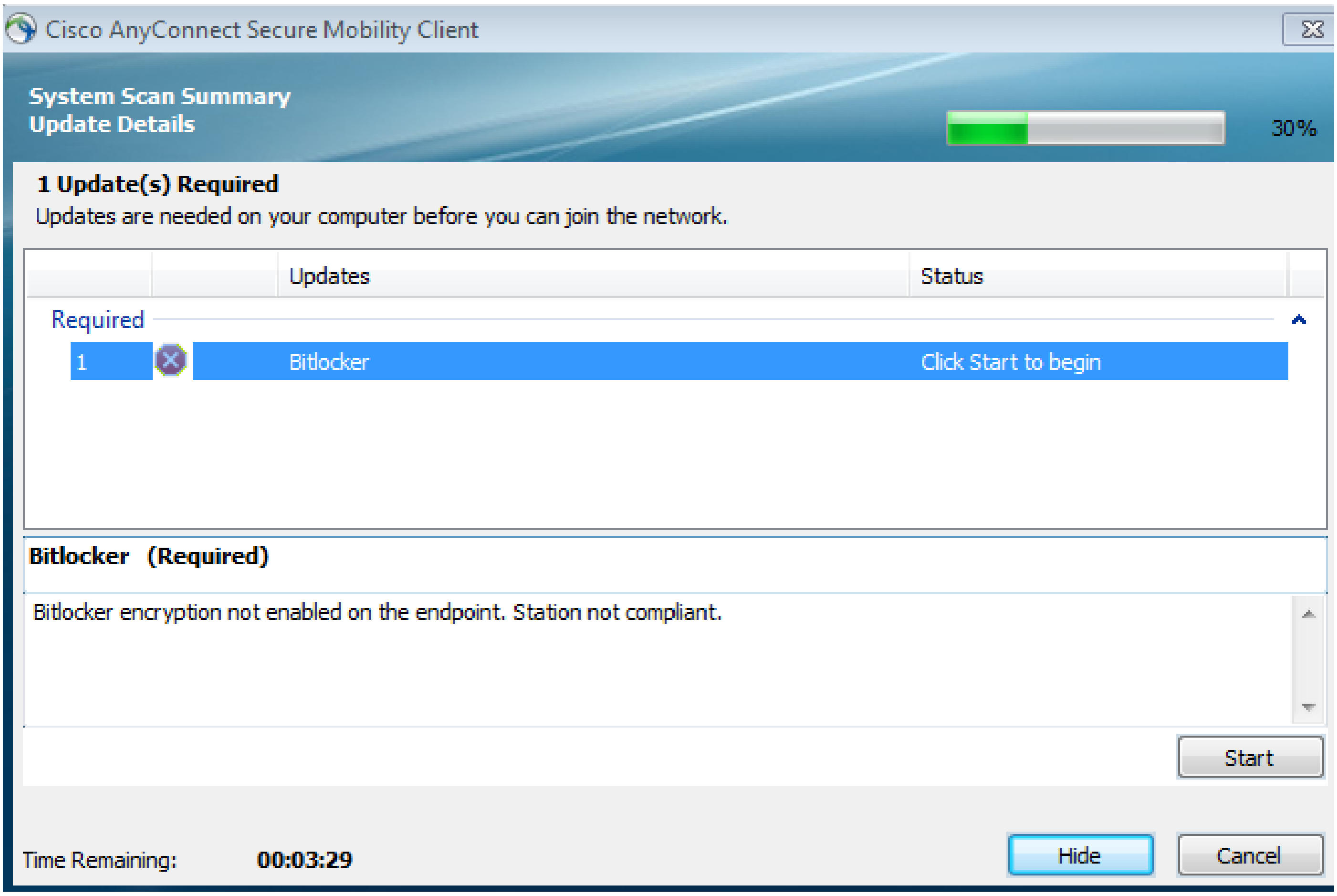
```
Date         : 11/14/2015
Time         : 14:58:43
Type         : Warning
Source       : acvpnui

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.
```

要成功完成會話，AnyConnect UI System Scan / Message History報告：

```
     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.
```

錯誤CSCux15941 — 位置失敗的ISE 2.0和AC4.2狀態bitlocker加密（字元\ /不支援）疑難排解

本節提供的資訊可用於對組態進行疑難排解。如果端點不相容，則會由AnyConnect UI報告（也執行配置的補救），如下圖所示。



1 Update(s) Required

Updates are needed on your computer before you can join the network.

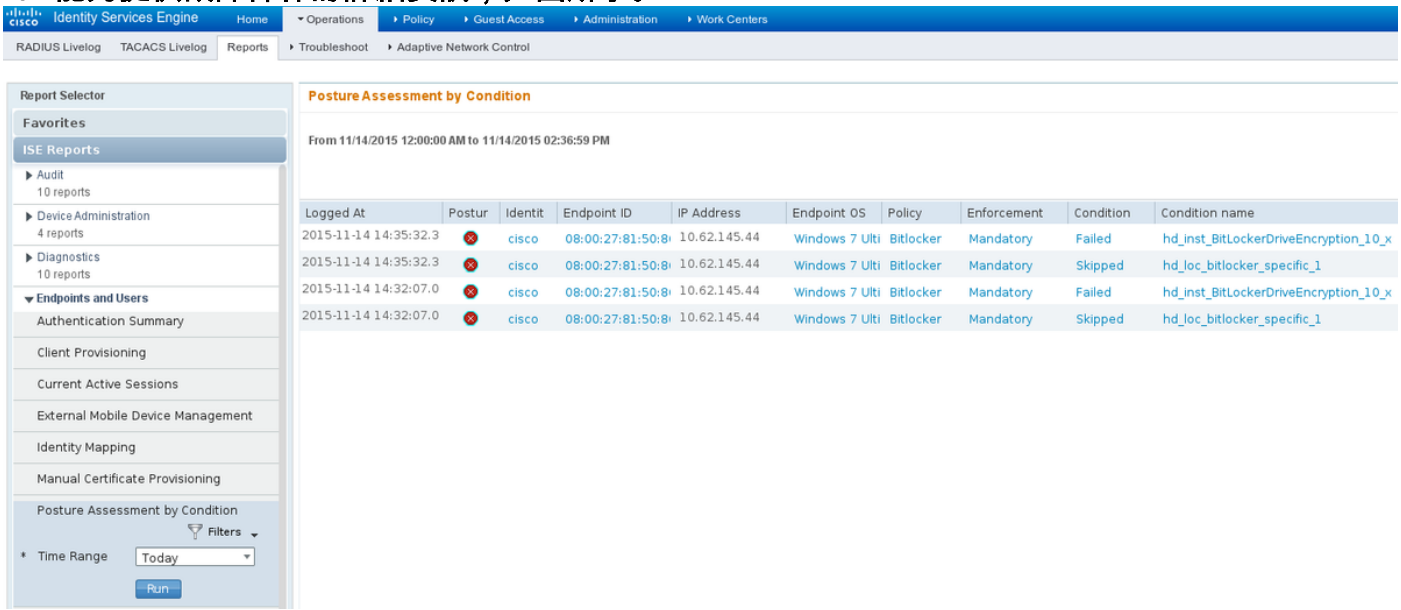
		Updates	Status
Required			
1	☒	Bitlocker	Click Start to begin

Bitlocker (Required)

Bitlocker encryption not enabled on the endpoint. Station not compliant.

Time Remaining: 00:03:29

ISE能夠提供故障條件的詳細資訊，如圖所示。



Posture Assessment by Condition

From 11/14/2015 12:00:00 AM to 11/14/2015 02:36:59 PM

Logged At	Postur	Identit	Endpoint ID	IP Address	Endpoint OS	Policy	Enforcement	Condition	Condition name
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

也可以從CLI日誌中檢查相同內容（「驗證」一節中的日誌示例）。

相關資訊

- 配置外部伺服器以進行安全裝置使用者授權
- Cisco ASA系列VPN CLI配置指南9.1
- 思科身份服務引擎管理員指南2.0版
- 技術支援與文件 - Cisco Systems