

配置ISE 2.1和AnyConnect 4.3狀態USB檢查

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[ASA](#)

[ISE](#)

[步驟1.配置網路裝置](#)

[步驟2.配置狀態條件和策略](#)

[步驟3.配置客戶端調配資源和策略](#)

[步驟4.配置授權規則](#)

[驗證](#)

[建立VPN會話之前](#)

[VPN會話建立](#)

[客戶端調配](#)

[狀況檢查和CoA](#)

[疑難排解](#)

[參考資料](#)

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)，使其僅在USB大容量儲存裝置斷開連線時提供網路的完全訪問。

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配置的基本知識
- ASA上遠端訪問VPN配置的基本知識
- ISE和狀態服務基礎知識

採用元件

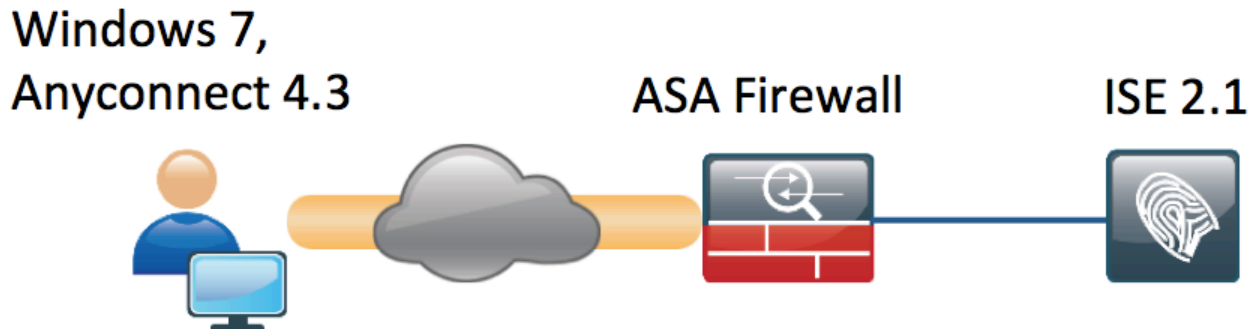
思科身份服務引擎(ISE)版本2.1和AnyConnect安全移動客戶端4.3支援USB大容量儲存檢查和補救。本檔案中的資訊是根據以下軟體版本：

- Cisco ASA軟體版本9.2(4)及更高版本

- 搭載Cisco AnyConnect安全移動客戶端版本4.3及更高版本的Microsoft Windows版本7
- Cisco ISE 2.1版及更高版本

設定

網路圖表



流程如下：

- 使用者尚未連線到VPN，私有USB大容量儲存裝置已插入，且內容可供使用者使用
- 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「Posture_Unknown」被命中，因此會話將重定向到ISE
- USB檢查在AC ISE狀態中引入了一類新的檢查，即只要終端仍位於同一個ISE控制的網路，它們就會持續監控該終端。唯一可用的邏輯補救操作是阻止由其驅動器號標識的USB裝置
- 更新ASA上的VPN會話，刪除重定向ACL並授予完全訪問許可權

VPN會話就是一個例子。狀態功能對於其他型別的訪問也工作正常。

ASA

ASA配置為使用ISE作為AAA伺服器進行遠端SSL VPN訪問。需要設定Radius CoA以及重新導向ACL:

```
aaa-server ISE21 protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE21 (outside) host 10.48.23.88
  key cisco
```

```
tunnel-group RA type remote-access
tunnel-group RA general-attributes
  address-pool POOL
```

```
authentication-server-group ISE21
accounting-server-group ISE21
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.3.00520-k9.pkg 1
anyconnect enable
tunnel-group-list enable
error-recovery disable
group-policy GP-SSL internal
group-policy GP-SSL attributes
  dns-server value 10.62.145.72
  vpn-tunnel-protocol ssl-client
```

```
access-list ACL_WEBAUTH_REDIRECT extended deny udp any any eq domain
access-list ACL_WEBAUTH_REDIRECT extended deny ip any host 10.48.23.88
access-list ACL_WEBAUTH_REDIRECT extended deny icmp any any
access-list ACL_WEBAUTH_REDIRECT extended permit tcp any any
```

有關詳細資訊，請參閱：

[AnyConnect 4.0與ISE 1.3版整合配置示例](#)

ISE

步驟1.配置網路裝置

從Administration > Network Resources > Network Devices > add ASA。

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Network Devices List > BSNS-ASA5515-11

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

CoA Port

步驟2. 配置狀態條件和策略

確保狀態條件已更新：Administration > System > Settings > Posture > Updates > Update now 選項。

ISE 2.1 附帶預配置的USB條件，用於檢查USB海量儲存裝置是否已連線。

在 Policy > Policy Elements > Conditions > Posture > USB Condition 中驗證現有條件：

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

- Anti-Malware Condition
- Anti-Spyware Condition
- Anti-Virus Condition
- Application Condition
- Compound Condition
- Disk Encryption Condition
- File Condition
- Patch Management Condition
- Registry Condition
- Service Condition
- USB Condition

Dictionary Simple Condition

Dictionary Compound Condition

Guest

Common

Name USB_Check

Description Cisco Predefined Check: Checks if USB mass storage device is connected.

Operating System Windows All

Compliance Module 4.x or later ⓘ

在Policy > Policy Elements > Results > Posture > Requirements中，驗證使用該條件的預配置要求。

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Remediation Actions

Requirements

Client Provisioning

Requirements

Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
USB_Block	for Windows All	using 4.x or later	met if USB_Check	then USB_Block

在Policy > Posture中，為所有Windows新增一個條件以使用該要求：

Identity Services Engine Home > Context Directory > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Windows 7 USB check	If Any	and Windows 7 (All)	and 4.x or later	and	then USB_Block

在Policy > Policy Elements > Results > Posture > Remediation Actions > USB Remediations中，驗證預配置的補救操作以阻止USB儲存裝置：

Identity Services Engine Home > Context Directory > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys > Conditions > Results

USB Remediations

Edit Add Duplicate Delete

Name	Description	Type
<input type="checkbox"/> USB_Block	Cisco Predefined Remediation: ...	Automatic

- Authentication
- Authorization
- Profiling
- Posture
 - Remediation Actions
 - Anti-Malware Remediations
 - Anti-Spyware Remediations
 - Anti-Virus Remediations
 - File Remediations
 - Launch Program Remediations
 - Link Remediations
 - Patch Management Remedia...
 - USB Remediations
 - Windows Server Update Ser...
 - Windows Update Remediations
 - Requirements
- Client Provisioning

步驟3.配置客戶端調配資源和策略

在Policy > Policy Elements > Client Provisioning > Resources中，從Cisco.com下載合規性模組並手動上傳AnyConnect 4.3軟體包：

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Directory > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. Under Policy Elements, there are sub-menus for Dictionaries, Conditions, and Results. The Resources table is displayed with the following data:

Name	Type	Version	Last Update	Description
<input checked="" type="checkbox"/> AnyConnectDesktopWindows 4.3.520.0	AnyConnectDesktopWindows	4.3.520.0	2016/03/11 11:10:47	AnyConnect Secure Mobility Clie...
<input checked="" type="checkbox"/> AnyConnectComplianceModuleWind...	AnyConnectComplianceMo...	4.2.330.0	2016/03/11 11:11:16	AnyConnect Windows Complian...
<input type="checkbox"/> WinSPWizard 2.1.0.50	WinSPWizard	2.1.0.50	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
<input type="checkbox"/> AnyConnect Configuration	AnyConnectConfig	Not Applicable	2016/03/11 11:12:42	
<input type="checkbox"/> MacOSXSPWizard 2.1.0.39	MacOsXSPWizard	2.1.0.39	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
<input type="checkbox"/> Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
<input type="checkbox"/> Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
<input type="checkbox"/> Anyconnect_Posture_Profile	AnyConnectProfile	Not Applicable	2016/03/11 14:39:03	

使用Add > NAC Agent或AnyConnect Posture Profile建立AnyConnect Posture配置檔案(名稱 : Anyconnect_Posture_Profile)。

使用Add > AnyConnect Configuration新增AnyConnect配置(名稱 : AnyConnect配置):

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an AnyConnect Configuration. The breadcrumb navigation is: Home > Context Directory > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. Under Policy Elements, there are sub-menus for Dictionaries, Conditions, and Results. The configuration page is titled "AnyConnect Configuration > AnyConnect Configuration".

The configuration form includes the following fields:

- * Select AnyConnect Package: AnyConnectDesktopWindows 4.3.520.0
- * Configuration Name: AnyConnect Configuration
- Description: (Empty text box)
- DescriptionValue: (Empty text box)
- * Compliance Module: AnyConnectComplianceModuleWindows 4.2.330.0

Below the form, there are two sections:

- AnyConnect Module Selection:**
 - ISE Posture
 - VPN
 - Network Access Manager
 - Web Security
 - AMP Enabler
 - ASA Posture
 - Network Visibility
 - Start Before Logon
 - Dagnostic and Reporting Tool
- Profile Selection:**
 - * ISE Posture: Anyconnect_Posture_Profile
 - VPN: (Dropdown menu)
 - Network Access Manager: (Dropdown menu)
 - Web Security: (Dropdown menu)
 - AMP Enabler: (Dropdown menu)
 - Network Visibility: (Dropdown menu)
 - Customer Feedback: (Dropdown menu)

在Policy > Client Provisioning中，為Windows建立一個新策略(Windows_Posture)以使用AnyConnect配置：

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 WinSPWizard 2.1.0.50 And Cisco-ISE-NSP
Windows_Posture	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration
MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOsXSPWizard 2.1.0.39 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

步驟4. 配置授權規則

在Policy > Policy Elements > Results > Authorization中新增授權配置檔案(名稱: Posture_Redirect), 重定向到預設客戶端調配門戶:

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authorization Profiles > Posture_Redirect

Authorization Profile

* Name: Posture_Redirect

Description: [Empty]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: ACL_WEBAUTH_REDIRECT Value: Client Provisioning Portal (defa)

附註: ACL WEBAUTH REDIRECT ACL是在ASA上定義的。

從Policy > Authorization為重定向建立授權規則。在ISE上預配置合規裝置的授權規則:

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

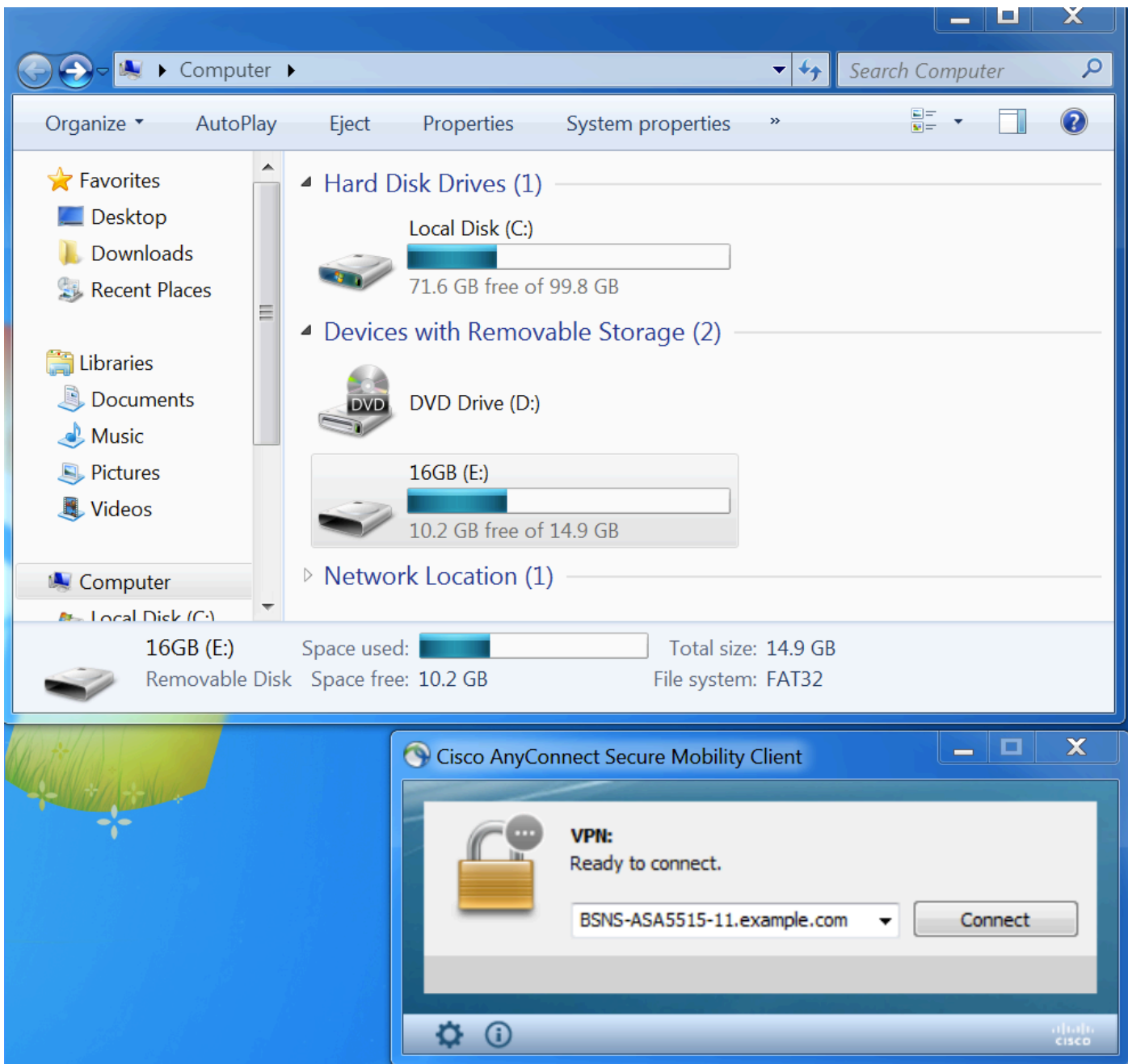
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
☑	Posture_Unknown	if Session:PostureStatus NOT_EQUALS Compliant	then Posture_Redirect

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

建立VPN會話之前

已插入USB裝置，其內容可供使用者使用。



VPN會話建立

在身份驗證期間，ISE將返回重定向訪問清單和重定向url，作為Posture_Redirect授權配置檔案的一部分

Cisco Identity Services Engine											
RADIUS											
Misconfigured Supplicants		Misconfigured Network Devices		RADIUS Drops		Client Stopped Responding		Repeat Counter			
0		0		6		0		0			
Refresh Every 1 minute Show Latest 20 records Within Last 5 minutes											
Time	Sta...	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Pr...	IP Address	Network De...	Posture Status	Server
Mar 11, 2016 03:57:40.126 PM			cisco	00:0C:29:C9:...	Default >> Default >> Default	Default >> Posture_Un...	Posture_Redirect	10.10.10...		Pending	ISE21-1
Mar 11, 2016 03:57:39.598 PM			cisco	00:0C:29:C9:...	Default >> Default >> Default	Default >> Posture_Un...	Posture_Redirect		BSNS-ASA55...	Pending	ISE21-1

建立VPN會話後，來自客戶端的ASA流量將根據重定向訪問清單進行重定向：

BSNS-ASA5515-11# **sh vpn-sessiondb detail anyconnect**

Session Type: AnyConnect Detailed

Username : cisco Index : 29
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 14696 Bytes Rx : 18408
Pkts Tx : 20 Pkts Rx : 132
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GP-SSL Tunnel Group : RA
Login Time : 15:57:39 CET Fri Mar 11 2016
Duration : 0h:07m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a3042ca0001d00056e2dce3
Security Grp : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 29.1
Public IP : 10.229.16.34
Encryption : none Hashing : none
TCP Src Port : 61956 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes
Client OS : win
Client OS Ver: 6.1.7601 Service Pack 1
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 6701 Bytes Rx : 774
Pkts Tx : 5 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 29.2
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 61957
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 6701 Bytes Rx : 1245
Pkts Tx : 5 Pkts Rx : 5
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 29.3
Assigned IP : 10.10.10.10 Public IP : 10.229.16.34
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 55708
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 26 Minutes
Client OS : Windows

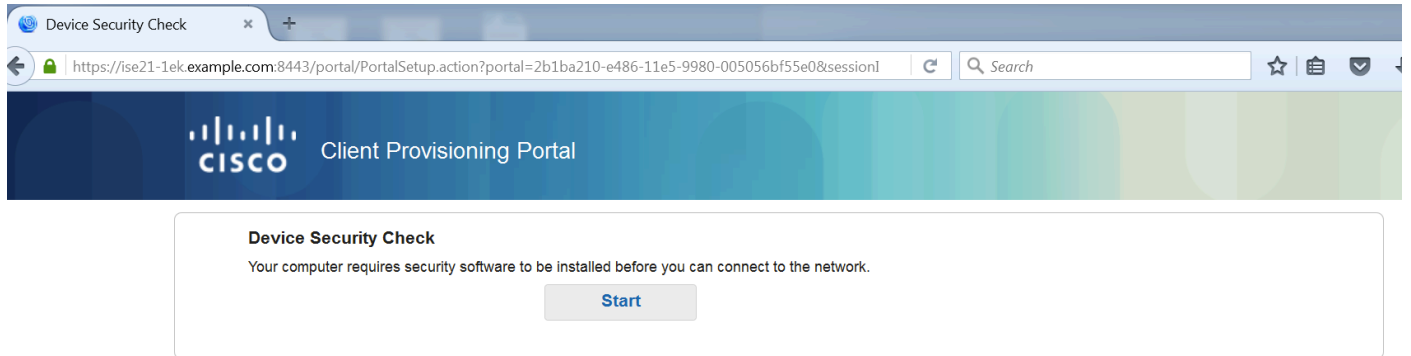
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 1294 Bytes Rx : 16389
Pkts Tx : 10 Pkts Rx : 126
Pkts Tx Drop : 0 Pkts Rx Drop : 0

ISE Posture:

Redirect URL : <https://ISE21-1ek.example.com:8443/portal/gateway?sessionId=0a3042ca0001d00056e2dce3&portal=2b1ba210-e...>
Redirect ACL : ACL_WEBAUTH_REDIRECT

客戶端調配

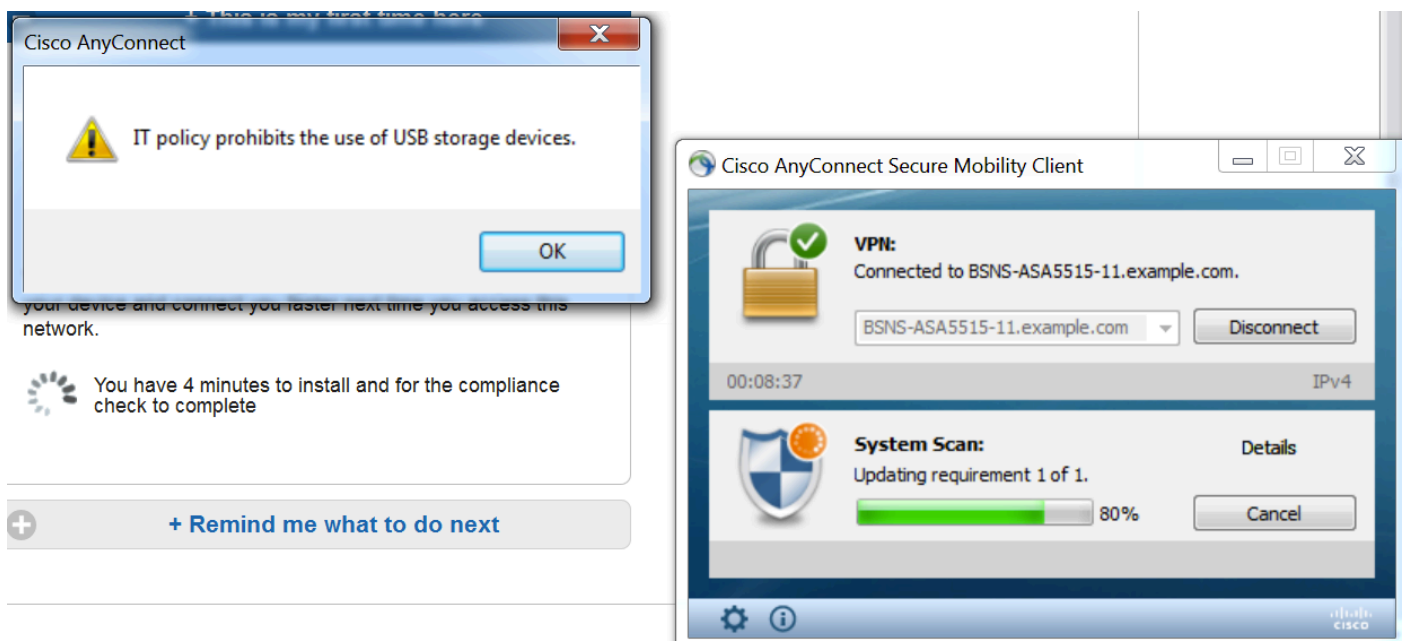
在此階段，終端Web瀏覽器流量重定向到ISE進行客戶端調配：



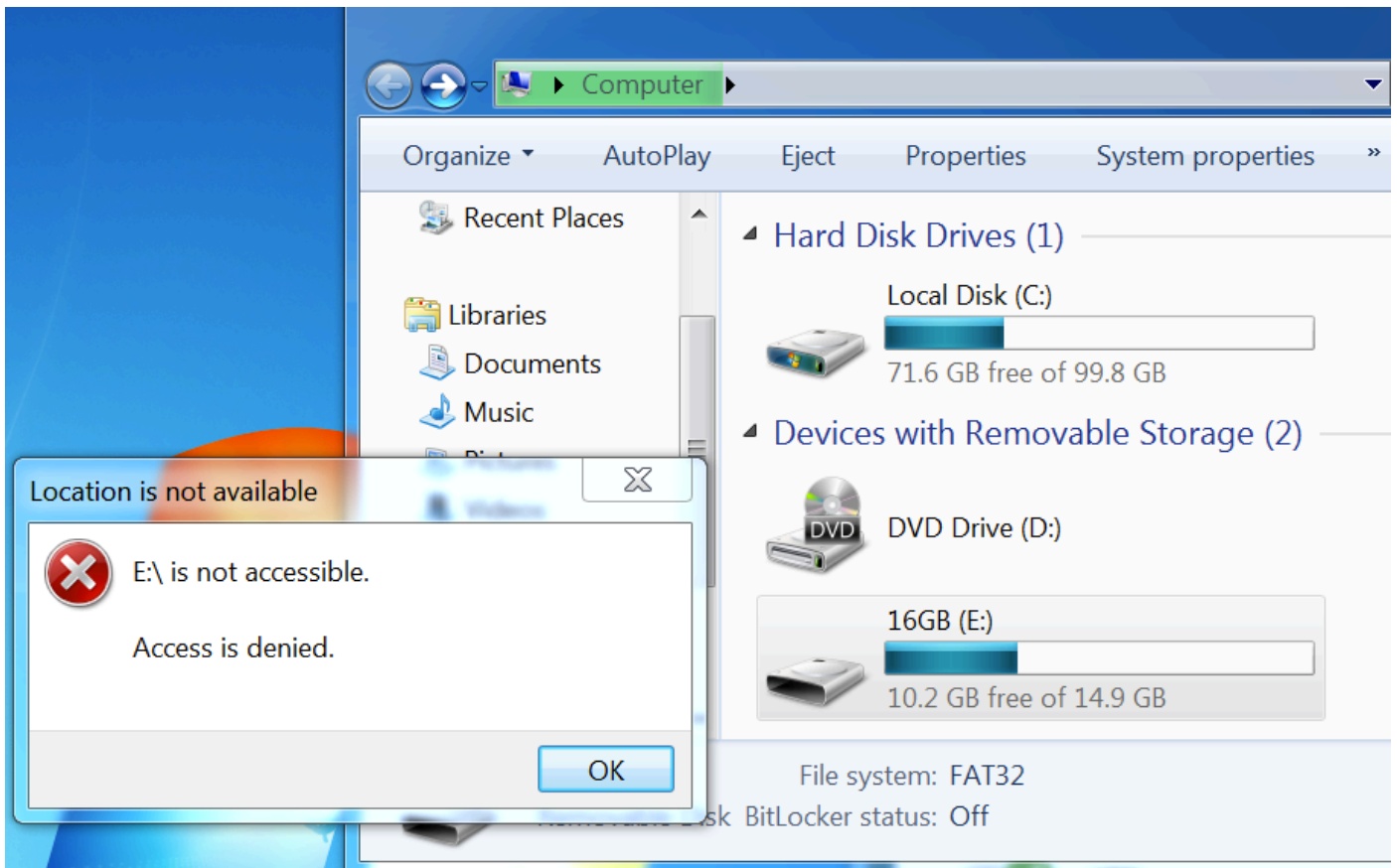
如果需要，會更新AnyConnect以及Posture and Compliance模組。

狀況檢查和CoA

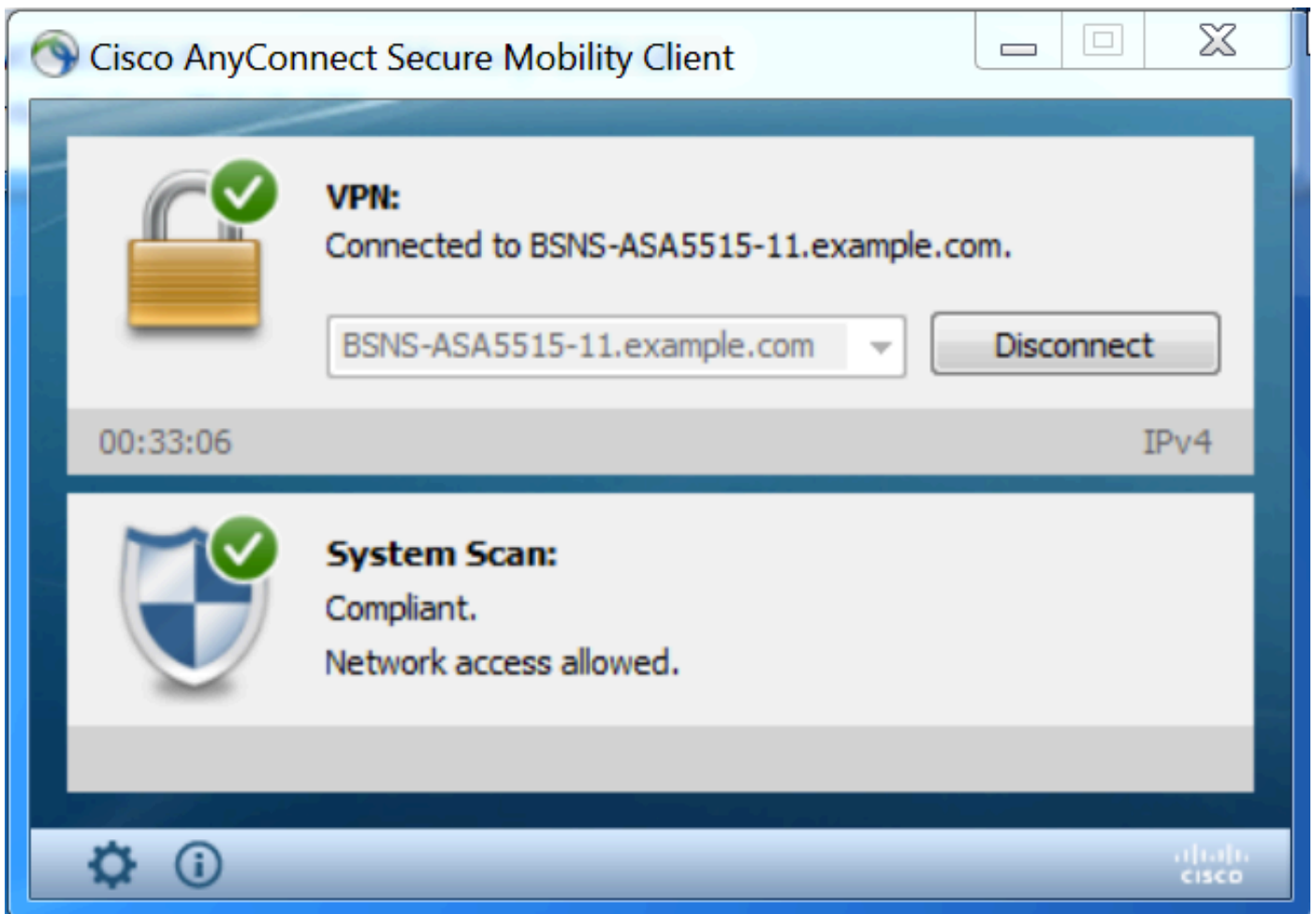
執行狀態模組，發現ISE(可能需要enroll.cisco.com的DNS A記錄才能成功)、下載並檢查狀態條件、新的OPSWAT v4阻止USB裝置操作。將為使用者顯示配置消息：



確認消息後，使用者無法再使用USB裝置：



ASA刪除提供完全訪問許可權的重定向ACL。AnyConnect報告合規性：



此外，有關ISE的詳細報告可以確認通過所需的條件。

按條件進行的狀態評估：

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

RADIUS TC-NAC Live Logs TACACS Legacy Dashboard Reports Troubleshoot Adaptive Network Control

Report Selector

Posture Assessment by Condition

From 03/11/2016 12:00:00.000 AM to 03/11/2016 04:37:13.253 PM

Logged At	Posture	Identity	Endpoint ID	IP Address	Location	Endpoint OS	Policy	Enforcement Type	Condition Status	Condition name
2016-03-11 16:06:24.974	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:31:53.456	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:26:57.007	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check
2016-03-11 11:16:33.483	✓	cisco	00:0C:29:C9:D9:37	10.48.66.202	All Locations	Windows 7 Ultim	Windows 7 USB check	Mandatory	Passed	USB_Check

Time Range: Today Run

終端安全評估：

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

RADIUS TC-NAC Live Logs TACACS Legacy Dashboard Reports Troubleshoot Adaptive Network Control

Report Selector

Posture Assessment by Endpoint

From 03/11/2016 12:00:00.000 AM to 03/11/2016 04:33:39.111 PM

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2016-03-11 16:06:24.974	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint
2016-03-11 11:31:53.456	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint
2016-03-11 11:26:57.007	✓		logoff	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Posture service received a USB-check report from an endpoint
2016-03-11 11:16:33.483	✓		N/A	cisco	00:0C:29:C9:D9:37	10.48.66.202	Windows 7 Ultim	AnyConnect P...	Received a posture report from an endpoint

Time Range: Today Run

終端報告的詳細資訊：

Posture More Detail Assessment

Time Range: From 03/11/2016 12:00:00 AM to 03/11/2016 04:34:03.708 PM
Generated At: 2016-03-11 16:34:03.708

Username: cisco
Mac Address: 00:0C:29:C9:D9:37
IP address: 10.48.66.202
Location: All Locations
Session ID: 0a3042ca0001d00056e2dce3
Client Operating System: Windows 7 Ultimate 64-bit
Client NAC Agent: AnyConnect Posture Agent for Windows 4.3.00520
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: WIN7-PC
System Domain: n/a
System User: Win7
User Domain: Win7-PC
AV Installed:
AS Installed:
AM Installed: Windows Defender;6.1.7600.16385;1.215.699.0;03/09/2016;

Posture Report
Posture Status: Compliant
Logged At: 2016-03-11 16:06:24.974

Posture Policy Details

Policy	Name	Enforcement Type	Status	Passed Conditions	Failed Conditions	Skipped Conditions
Windows 7 USB check	USB_Block	Mandatory		USB_Check		

疑難排解

ISE能夠提供故障條件的詳細資訊，應相應地採取行動。

參考資料

- [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](#)