

Configurazione del controllo USB della postura di ISE 2.1 e AnyConnect 4.3

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[ASA](#)

[ISE](#)

[Passaggio 1. Configurare il dispositivo di rete](#)

[Passaggio 2. Configurare le condizioni e i criteri di postura](#)

[Passaggio 3. Configurare le risorse e i criteri di provisioning client](#)

[Passaggio 4. Configurare le regole di autorizzazione](#)

[Verifica](#)

[Prima della creazione della sessione VPN](#)

[Impostazione sessione VPN](#)

[Provisioning client](#)

[Controllo postura e CoA](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

Introduzione

In questo documento viene descritto come configurare Cisco Identity Services Engine (ISE) in modo da fornire l'accesso completo alla rete solo quando i dispositivi di archiviazione di massa USB sono disconnessi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di configurazione CLI di Adaptive Security Appliance (ASA) e configurazione VPN SSL (Secure Sockets Layer)
- Conoscenze base della configurazione VPN di accesso remoto sull'appliance ASA
- Conoscenze base di ISE e servizi di postura

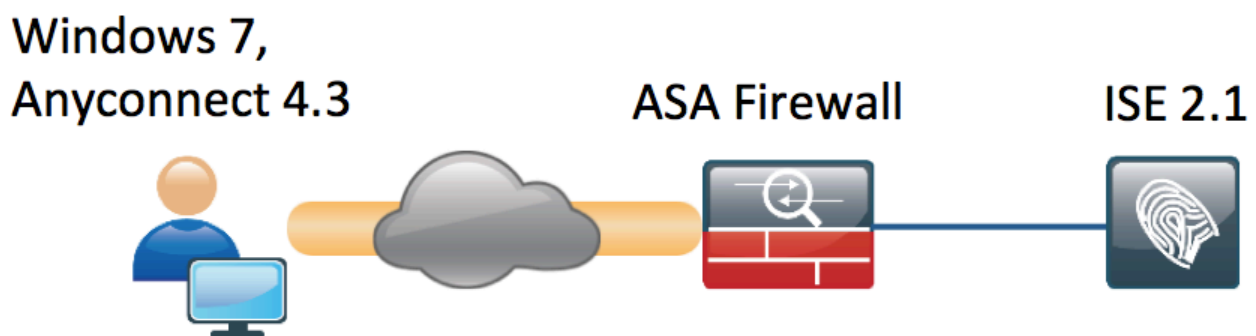
Componenti usati

Cisco Identity Services Engine (ISE) versione 2.1 con AnyConnect Secure Mobility Client 4.3 supporta il controllo e la risoluzione dei problemi di archiviazione di massa tramite USB. Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco ASA versione 9.2(4) e successive
- Microsoft Windows versione 7 con Cisco AnyConnect Secure Mobility Client versione 4.3 e successive
- Cisco ISE versione 2.1 e successive

Configurazione

Esempio di rete



Il flusso è il seguente:

- L'utente non è ancora connesso alla VPN, il dispositivo di archiviazione di massa USB privato è collegato e il contenuto è disponibile per l'utente
- La sessione VPN avviata dal client AnyConnect viene autenticata tramite ISE. Lo stato della postura dell'endpoint non è noto, la regola "Posture_Unknown" è stata trovata e la sessione verrà reindirizzata all'ISE
- I controlli USB introducono una nuova classe di controlli nella postura ISE CA, in quanto monitorano continuamente l'endpoint finché rimane nella stessa rete ISE controllata. L'unica azione di correzione logica disponibile è bloccare i dispositivi USB identificati dalla relativa lettera di unità
- La sessione VPN sull'appliance ASA viene aggiornata, l'ACL di reindirizzamento viene rimosso e viene concesso l'accesso completo

La sessione VPN è stata presentata come esempio. La funzionalità di postura funziona correttamente anche per altri tipi di accesso.

ASA

L'ASA è configurata per l'accesso VPN SSL remoto usando ISE come server AAA. È necessario

configurare Radius CoA con l'ACL di reindirizzamento:

```
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
```

Per maggiori informazioni, consultare:

[Esempio di configurazione dell'integrazione di AnyConnect 4.0 con ISE versione 1.3](#)

ISE

Passaggio 1. Configurare il dispositivo di rete

Da Amministrazione > Risorse di rete > Dispositivi di rete > aggiungere un'appliance 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

Passaggio 2. Configurare le condizioni e i criteri di postura

Assicuratevi che le condizioni di postura siano aggiornate: **Amministrazione > Sistema > Impostazioni > Postura > Aggiornamenti > Aggiorna ora**, opzione.

ISE 2.1 viene fornito con una condizione USB preconfigurata che verifica se un dispositivo di archiviazione di massa USB è collegato.

Da **Criteri > Elementi criterio > Condizioni > Postura > Condizione USB** verificare la condizione esistente:

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys 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 ⓘ

Da Criteri > Elementi criterio > Risultati > Postura > Requisiti, verificare i requisiti preconfigurati che utilizzano tale condizione.

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys 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

Da Criterio > Postura, aggiungere una condizione affinché tutte le finestre utilizzino tale requisito:

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
✓	Windows 7 USB check	If Any	and Windows 7 (All)	and 4.x or later	and	then USB_Block

Da Policy > Policy Elements > Results > Posture > Remediation Actions > USB Remediations verificare l'azione di correzione preconfigurata per bloccare i dispositivi di archiviazione USB:

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary 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

Passaggio 3. Configurare le risorse e i criteri di provisioning client

Da Policy > Policy Elements > Client Provisioning > Resources scaricare il modulo di conformità da Cisco.com e caricare manualmente il pacchetto AnyConnect 4.3:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation bar includes Home, Context Directory, Operations, Policy, Administration, and Work Centers. The main menu has Authentication, Authorization, Profiling, Posture, and Client Provisioning. The left sidebar shows a tree view with Authentication, Authorization, Profiling, Posture, and Client Provisioning expanded. The main content area is titled 'Resources' and contains a table of configuration items.

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	

Utilizzando **Add > NAC Agent o AnyConnect Posture Profile**, creare un profilo AnyConnect Posture (nome: *Anyconnect_Posture_Profile*) con impostazioni predefinite.

Utilizzando **Add > AnyConnect Configuration**, aggiungere una configurazione AnyConnect (nome: AnyConnect):

The screenshot shows the 'AnyConnect Configuration' page in the Cisco ISE interface. The breadcrumb trail is 'AnyConnect Configuration > AnyConnect Configuration'. The page contains several form fields and sections:

- 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
- 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)
 - Network Access Manager: (dropdown)
 - Web Security: (dropdown)
 - AMP Enabler: (dropdown)
 - Network Visibility: (dropdown)
 - Customer Feedback: (dropdown)

Da **Criteri > Provisioning client** creare un nuovo criterio (Windows_Posture) per Windows in modo che utilizzi la configurazione AnyConnect:

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
<input checked="" type="checkbox"/> 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

Passaggio 4. Configurare le regole di autorizzazione

Da **Criteri > Elementi criterio > Risultati > Autorizzazione** aggiungere un profilo di autorizzazione (nome: Posture_Redirect) che reindirizza a un portale di provisioning client predefinito:

Cisco 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)

Nota: ACL WEBAUTH REDIRECT L'ACL è definito sull'appliance ASA.

Da **Criteri > Autorizzazione** creare una regola di autorizzazione per il reindirizzamento. Una regola di autorizzazione per dispositivi conformi è preconfigurata su ISE:

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

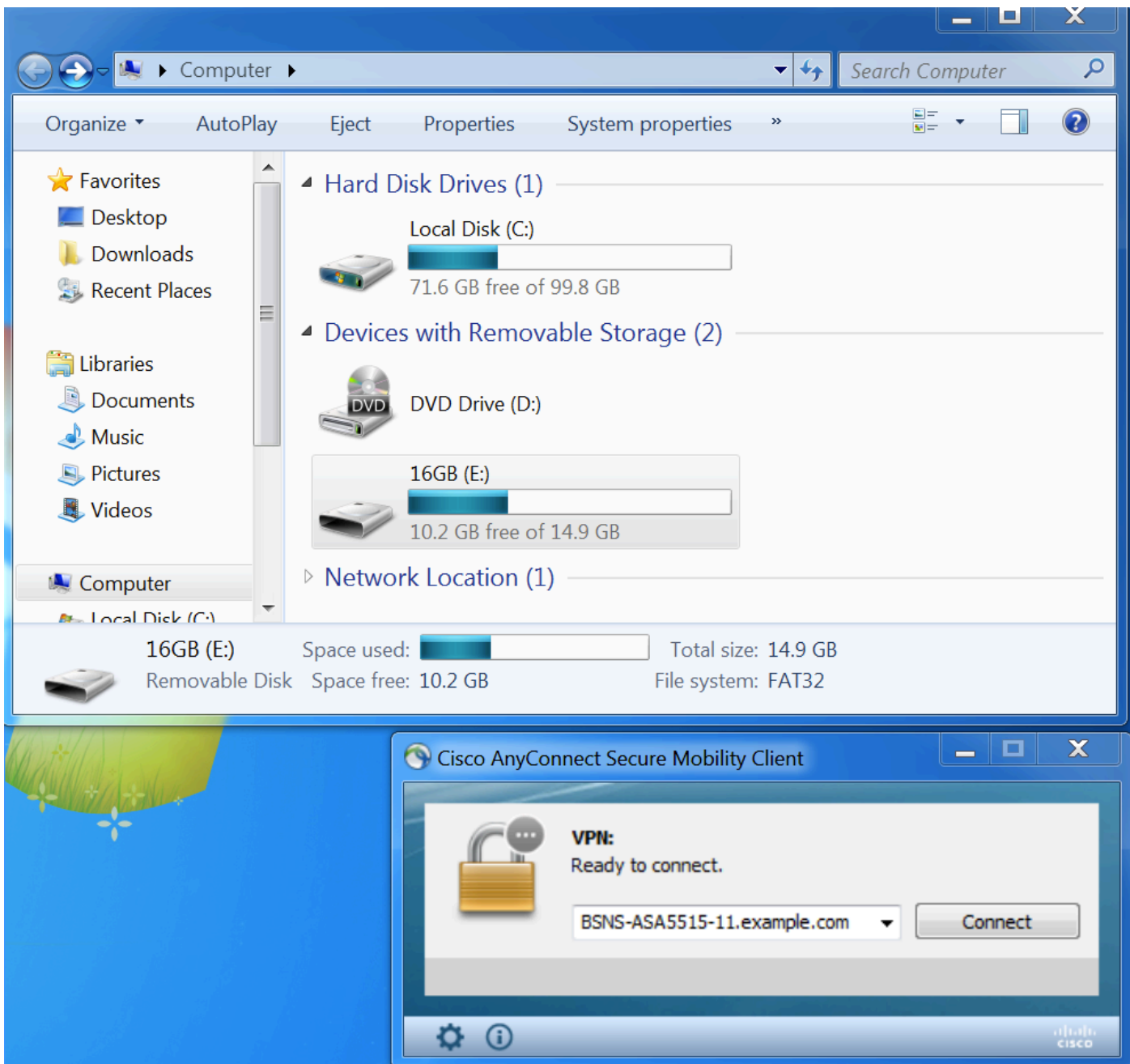
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
✔	Posture_Unknown	if Session:PostureStatus NOT_EQUALS Compliant	then Posture_Redirect

Se l'endpoint è conforme, viene fornito l'accesso completo. Se lo stato è sconosciuto o non conforme, viene restituito il reindirizzamento per il provisioning client.

Verifica

Prima della creazione della sessione VPN

dispositivo USB collegato e il relativo contenuto è disponibile per l'utente.



Impostazione sessione VPN

Durante l'autenticazione, ISE restituirà l'elenco degli accessi reindirizzati e l'URL di reindirizzamento come parte del profilo di autorizzazione Posture_Redirect

Cisco Identity Services Engine											
Operations > Policy > Administration > Work Centers											
RADIUS TC-NAC Live Logs > TACACS Legacy Dashboard > Reports > Troubleshoot > Adaptive Network Control											
Live Logs Live Sessions											
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

Una volta stabilita la sessione VPN, il traffico ASA proveniente dal client verrà reindirizzato in base

all'elenco degli accessi reindirizzati:

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

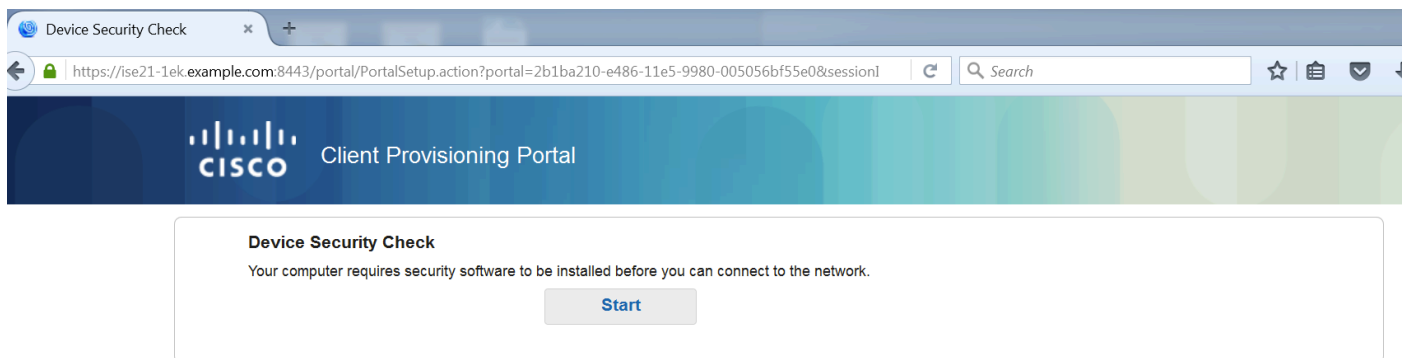
Idle Time Out: 30 Minutes Idle TO Left : 26 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 1294 Bytes Rx : 16389
Pkts Tx : 10 Pkts Rx : 126
Pkts Tx Drop : 0 Pkts Rx Drop : 0

ISE Posture:

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

Provisioning client

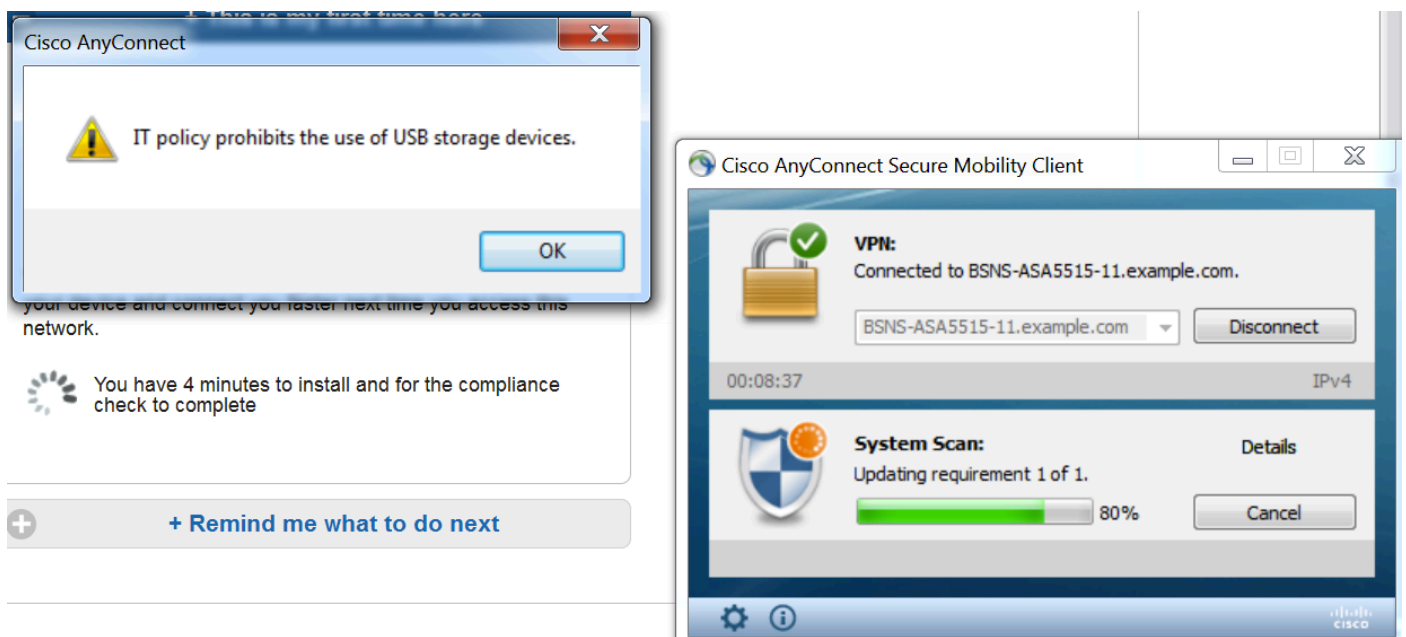
In questa fase, il traffico del browser Web dell'endpoint viene reindirizzato ad ISE per il provisioning del client:



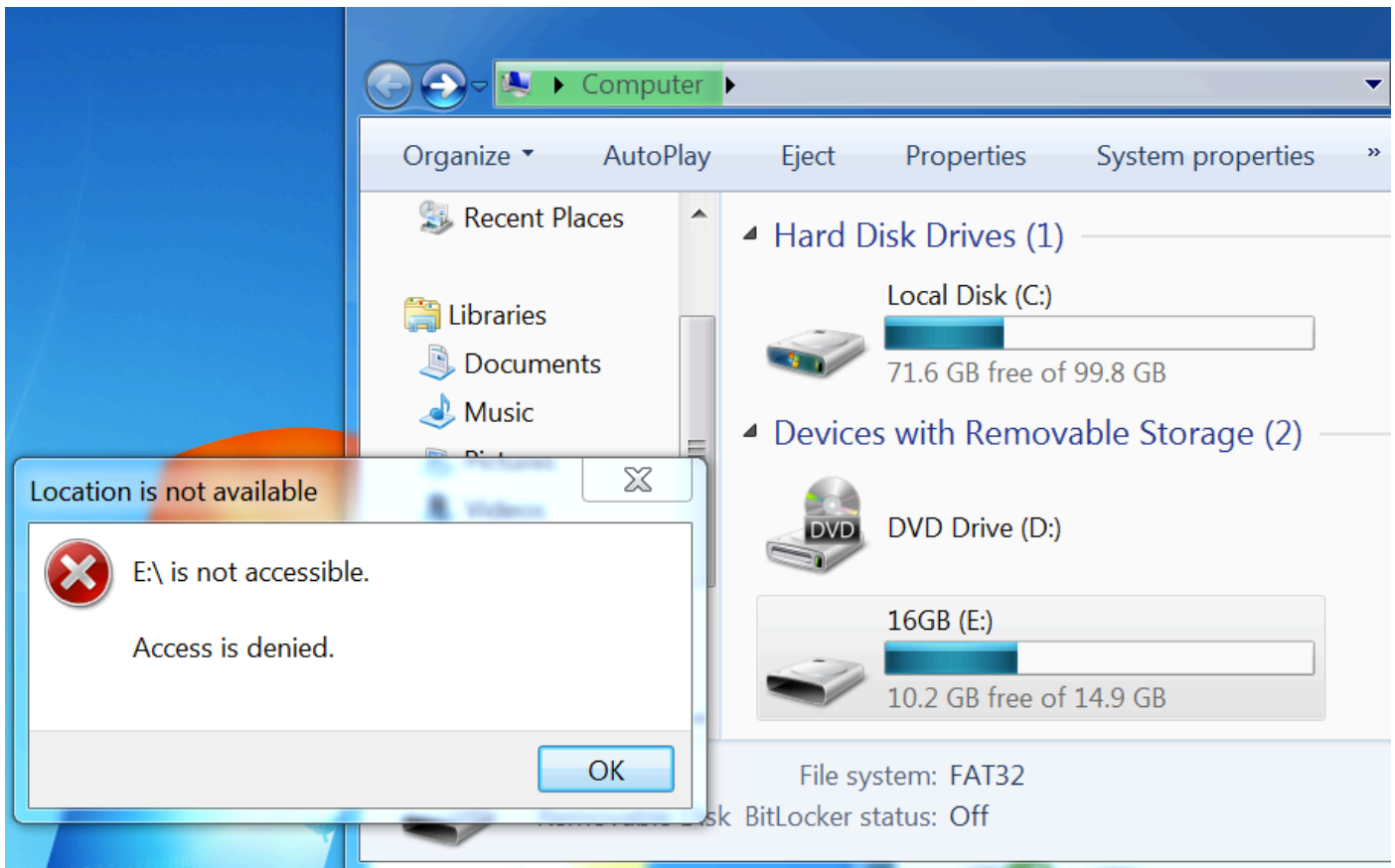
Se necessario, AnyConnect viene aggiornato insieme al modulo Postura e conformità.

Controllo postura e CoA

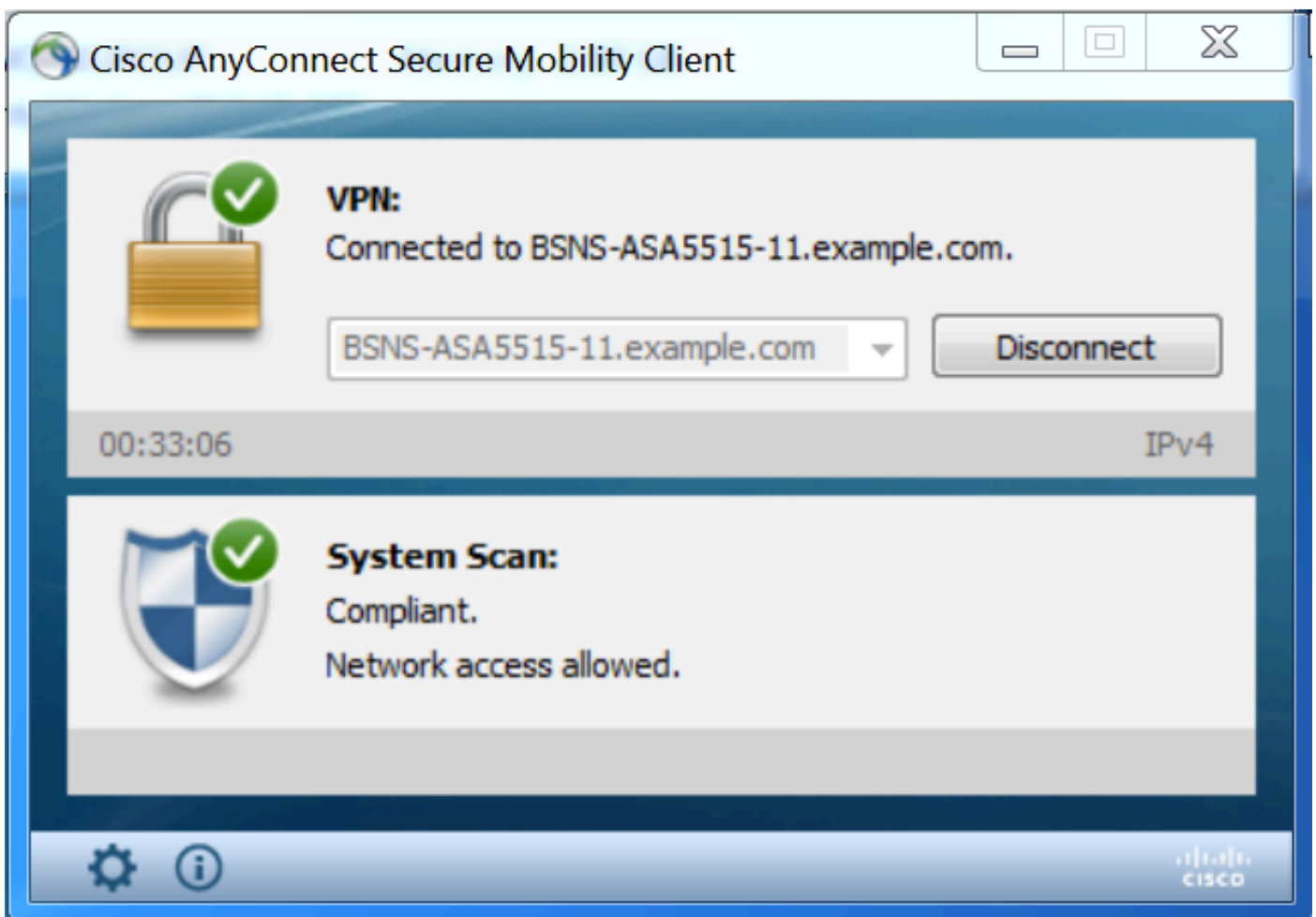
Modulo di postura eseguito, scoprire ISE (potrebbe essere necessario avere un record A DNS per enroll.cisco.com), scaricare e controllare le condizioni di postura, nuovo OPSWAT v4 blocco USB dispositivo azione. Verrà visualizzato il messaggio configurato per l'utente:



Una volta confermato il messaggio, il dispositivo USB non è più disponibile per l'utente:



L'ASA rimuove l'ACL di reindirizzamento fornendo l'accesso completo. AnyConnect segnala la conformità:



Anche report dettagliati sull'ISE possono confermare che le condizioni richieste sono state rispettate.

Valutazione postura per condizione:

The screenshot shows the Cisco ISE interface with the 'Posture Assessment by Condition' report selected. The report is filtered for 'Today' and shows four entries, all with a 'Passed' status.

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

Valutazione postura per endpoint:

The screenshot shows the Cisco ISE interface with the 'Posture Assessment by Endpoint' report selected. The report is filtered for 'Today' and shows four entries, all with a 'Passed' status.

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

Dettagli del report degli endpoint:


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: 0a3042ca001d00056e2dce3
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		

Risoluzione dei problemi

L'ISE è in grado di fornire i dettagli sulle condizioni che hanno causato il guasto; è necessario adottare le misure necessarie.

Riferimenti

- [Configurazione di un server esterno per l'autorizzazione utente di Security Appliance](#)
- [Guida alla configurazione di Cisco ASA VPN CLI, 9.1](#)
- [Guida dell'amministratore di Cisco Identity Services Engine, versione 2.0](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)