

ISE 2.1 および AnyConnect 4.3 ポスチャ USB チェックの設定

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ASA](#)

[ISE](#)

[手順 1：ネットワーク デバイスの設定](#)

[手順 2：ポスチャの条件およびポリシーの設定](#)

[手順 3：クライアント プロビジョニングのリソースとポリシーの設定](#)

[手順 4：許可ルールの設定](#)

[確認](#)

[VPN セッションの確立前](#)

[VPN セッションの確立](#)

[クライアント プロビジョニング](#)

[ポスチャのチェックと CoA](#)

[トラブルシューティング](#)

[参考資料](#)

概要

このドキュメントでは、USB マス ストレージ デバイスが切断されている場合のみ、ネットワークへのフル アクセスを提供するよう、Cisco Identity Services Engine (ISE) を設定する手順について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- 適応型セキュリティ アプライアンス (ASA) CLI の設定およびセキュア ソケット レイヤ (SSL) VPN の設定に関する基本的知識
- ASA でのリモート アクセス VPN 設定に関する基本的な知識
- ISE サービスとポスチャ サービスに関する基本的な知識

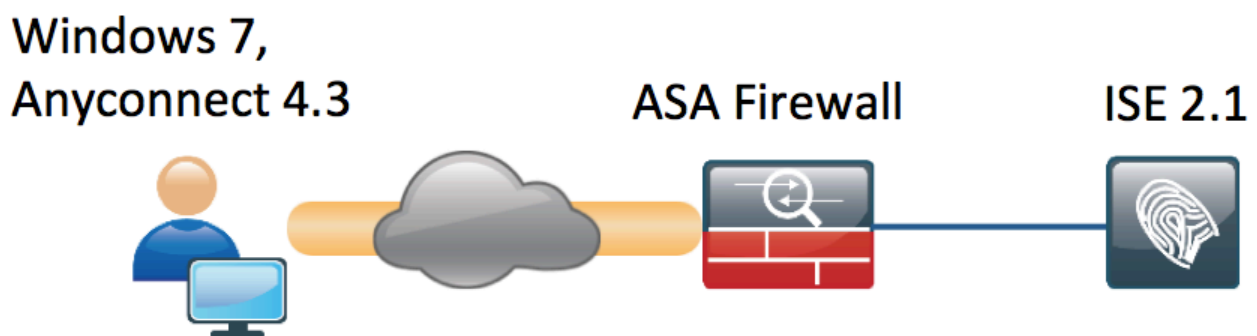
使用するコンポーネント

Cisco Identity Services Engine (ISE) バージョン 2.1 および AnyConnect Secure Mobility Client 4.3 は、USB マス ストレージのチェックおよび修復機能をサポートしています。このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco ASA ソフトウェア バージョン 9.2(4) 以降
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.3 以降を備えた Microsoft Windows Version 7
- Cisco ISE リリース 2.1 以降

設定

ネットワーク図



フローは次のとおりです。

- この時点では、ユーザはまだ VPN に接続していません。プライベートの USB マス ストレージ デバイスが接続され、ユーザはデバイス内のデータにアクセスできます。
- AnyConnect クライアントから開始された VPN セッションが ISE を介して認証されます。エンドポイントのポスチャ ステータスは不明です。「Posture_Unknown」というルールが該当し、この結果、セッションは ISE にリダイレクトされます。
- USB チェックにより、AC ISE ポスチャの新たなチェック クラスが導入されます。これにより、同一の ISE によって管理されるネットワークに属しているかぎり、エンドポイントは継続的にモニタされます。使用可能となる唯一の論理的な修復アクションは、ドライブ文字で識別された USB デバイスをブロックすることです。
- ASA 上の VPN セッションが更新され、リダイレクト ACL が削除され、フル アクセスが許可されます。

ここでは VPN セッションの例を挙げていますが、ポスチャ機能は、他のタイプのアクセスに対しても適切に機能します。

ASA

ASA は、AAA サーバとして ISE を使用して、リモート SSL VPN アクセス用に設定されています

。 RADIUS CoA、およびリダイレクト ACL は、次のように設定する必要があります。

```
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
```

詳細については、次のドキュメントを参照してください。

[AnyConnect 4.0 と ISE バージョン 1.3 統合の設定例](#)

ISE

手順 1：ネットワーク デバイスの設定

[Administration] > [Network Resources] > [Network Devices] の順に選択し、ASA を追加します。

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

手順 2 : ポスチャの条件およびポリシーの設定

次のように移動して、ポスチャの条件が更新されていることを確認します。これには、[Administration] > [System] > [Settings] > [Posture] > [Updates] > [Update now] オプションの順に選択します。

ISE 2.1 では、USB 条件が事前に設定されています。これにより、USB マスストレージ デバイスが接続されているかどうかチェックされます。

[Policy] > [Policy Elements] > [Conditions] > [Posture] > [USB Condition] の順に選択して、既存の条件を確認します。

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 ⓘ

[Policy] > [Policy Elements] > [Results] > [Posture] > [Requirements] の順に選択して、この条件を使用する、事前設定された要件を確認します。

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

[Policy] > [Posture] を選択して、すべての Windows がこの要件を使用するための条件を追加します。

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

[Policy] > [Policy Elements] > [Results] > [Posture] > [Remediation Actions] > [USB Remediations] の順に選択して、USB ストレージ デバイスをブロックする、事前設定された修復アクションを確認します。

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 Remediations
 - USB Remediations
 - Windows Server Update Services Remediations
 - Windows Update Remediations
 - Requirements
- Client Provisioning

手順 3 : クライアント プロビジョニングのリソースとポリシーの設定

[Policy] > [Policy Elements] > [Client Provisioning] > [Resources] の順に選択して、Cisco.com からコンプライアンス モジュールをダウンロードし、AnyConnect 4.3 パッケージを手動でアップロードします。

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

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Resources

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	

[Add] > [NAC Agent] または [AnyConnect Posture Profile] を使用して、AnyConnect Posture プロファイル (名前は 「 Anyconnect_Posture_Profile 」) をデフォルト設定で作成します。

[Add] > [AnyConnect Configuration] を使用して、AnyConnect 設定 (名前は 「 AnyConnect Configuration 」) を追加します。

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

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package: AnyConnectDesktopWindows 4.3.520.0

* Configuration Name: AnyConnect Configuration

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.2.330.0

Notes

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

[Policy] > [Client Provisioning] の順に選択して、Windows が 「 AnyConnect Configuration 」 を使用する新しいルール (Windows_Posture) を作成します。

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

手順 4 : 許可ルールの設定

[Policy] > [Policy Elements] > [Results] > [Authorization] の順に選択して、デフォルトのクライアントプロビジョニングポータルへリダイレクトする許可プロファイル (名前は「Posture_Redirect」) を追加します。

Identity Services Engine Home Context Directory Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authorization Profiles > Posture_Redirect

Authorization Profile

* Name: Posture_Redirect

Description: []

* 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

注 : ACL_WEBAUTH_REDIRECT ACL は ASA 上で定義されます。

[Policy] > [Authorization] の順に選択して、リダイレクトの許可ルールを作成します。ISE では、準拠デバイスに対する許可ルールが事前設定されています。

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

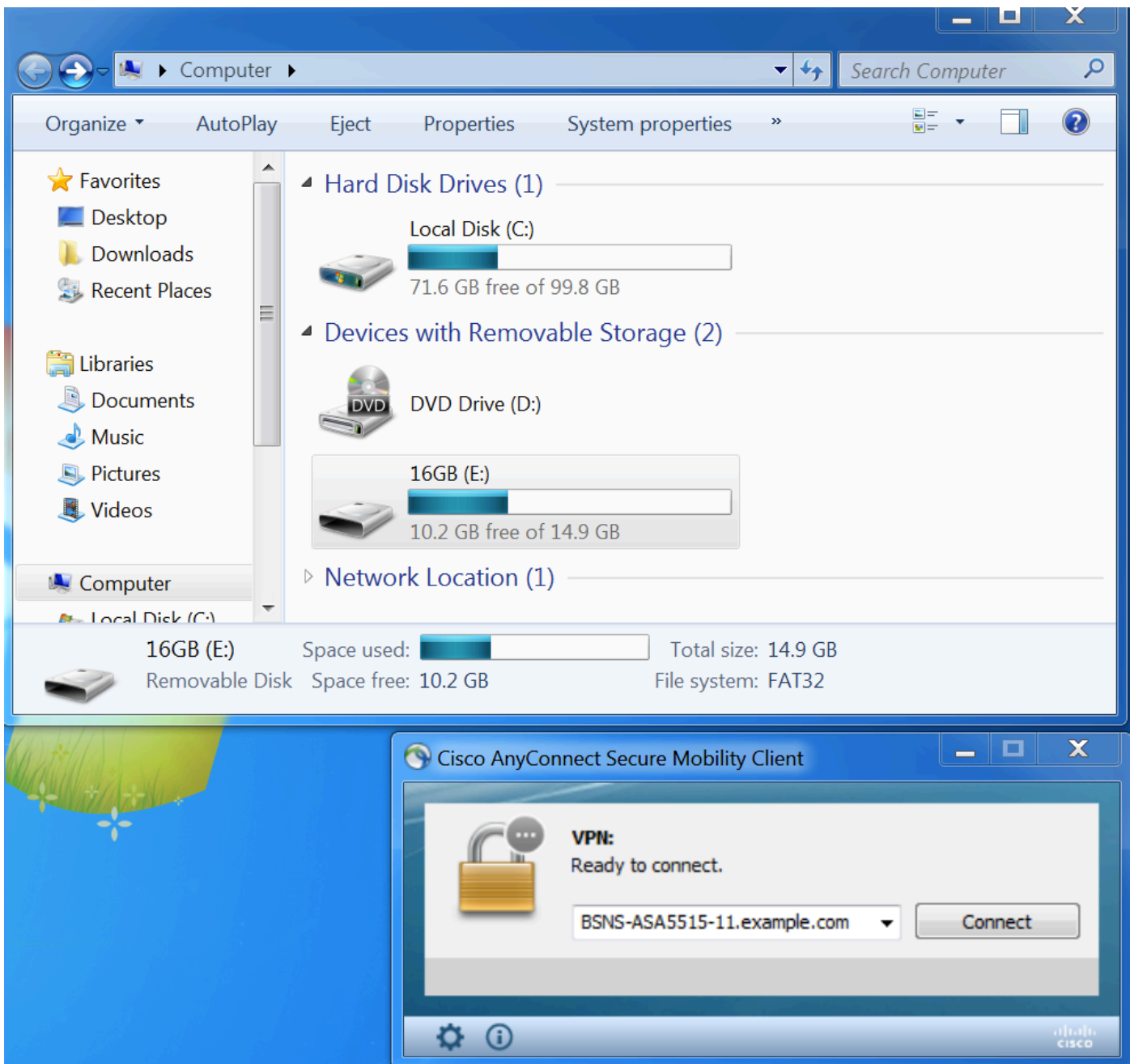
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
✔	Posture_Unknown	if Session:PostureStatus NOT_EQUALS Compliant	then Posture_Redirect

エンドポイントがルールに準拠している場合は、フル アクセスが許可されます。ステータスが不明、または非準拠のエンドポイントに対しては、クライアント プロビジョニングのリダイレクションが返されます。

確認

VPN セッションの確立前

USB デバイスが接続され、ユーザがこのデバイス内のデータにアクセスできます。



VPN セッションの確立

認証中、ISE は Posture_Redirect Authorization プロファイルの一環として、リダイレクトアクセスリストおよびリダイレクト URL を返します。

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		Reset Repeat Counts		Export To		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

VPN セッションの確立後は、クライアントからの ASA トラフィックはリダイレクト アクセスリ

ストに基づきリダイレクトされます。

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

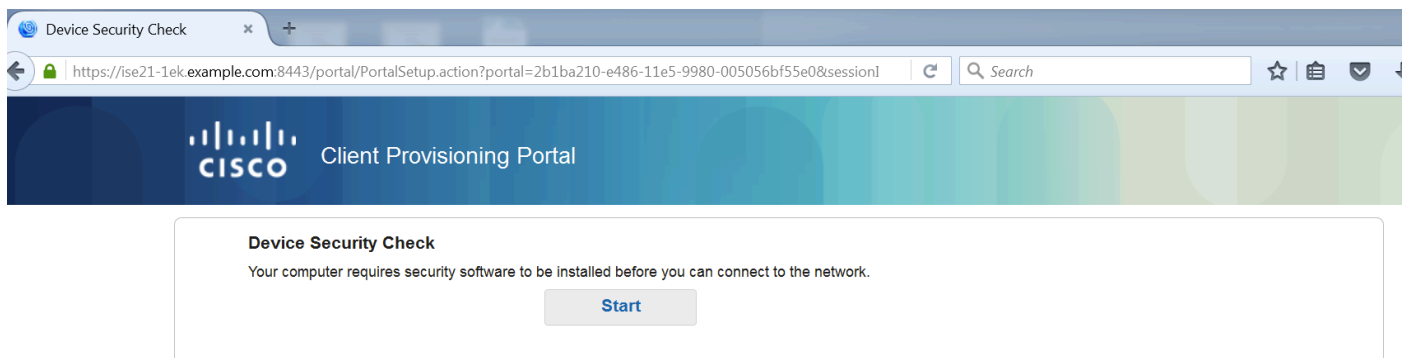
Idle Time Out: 30 Minutes Idle TO Left : 26 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520
Bytes Tx : 1294 Bytes Rx : 16389
Pkts Tx : 10 Pkts Rx : 126
Pkts Tx Drop : 0 Pkts Rx Drop : 0

ISE Posture:

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

クライアントプロビジョニング

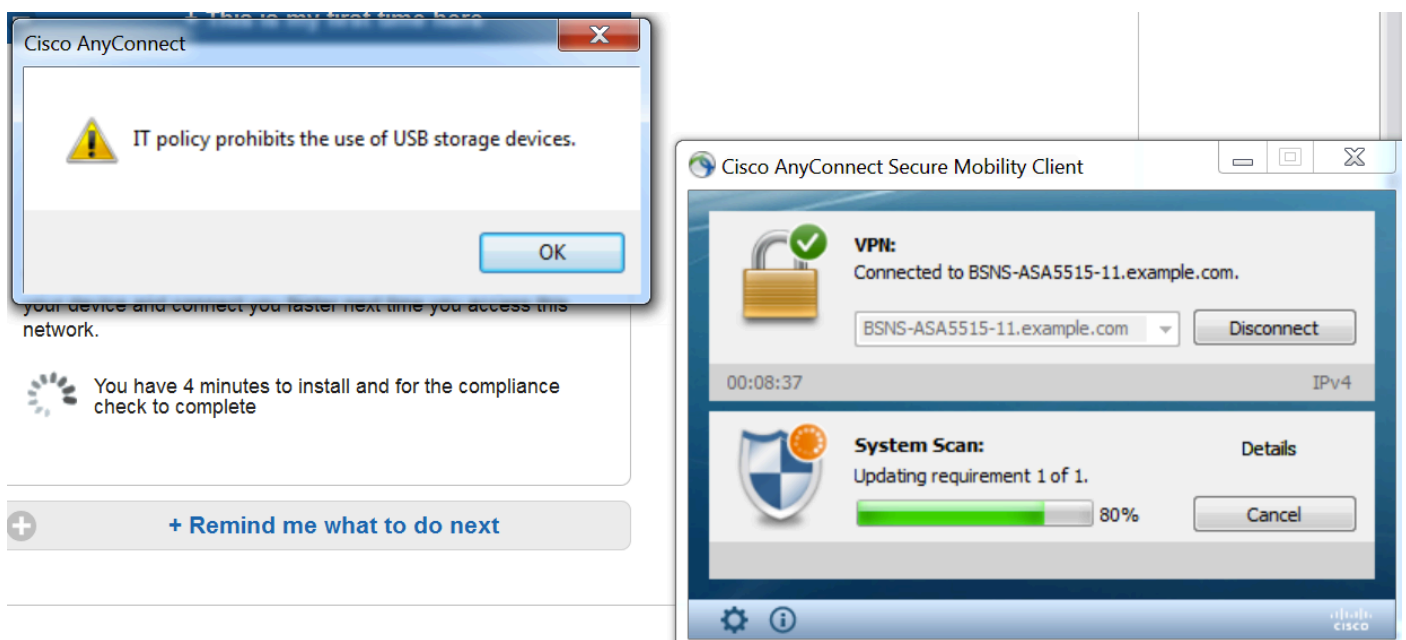
この段階では、エンドポイントの Web ブラウザ トラフィックは ISE にリダイレクトされ、クライアントプロビジョニングが行われます。



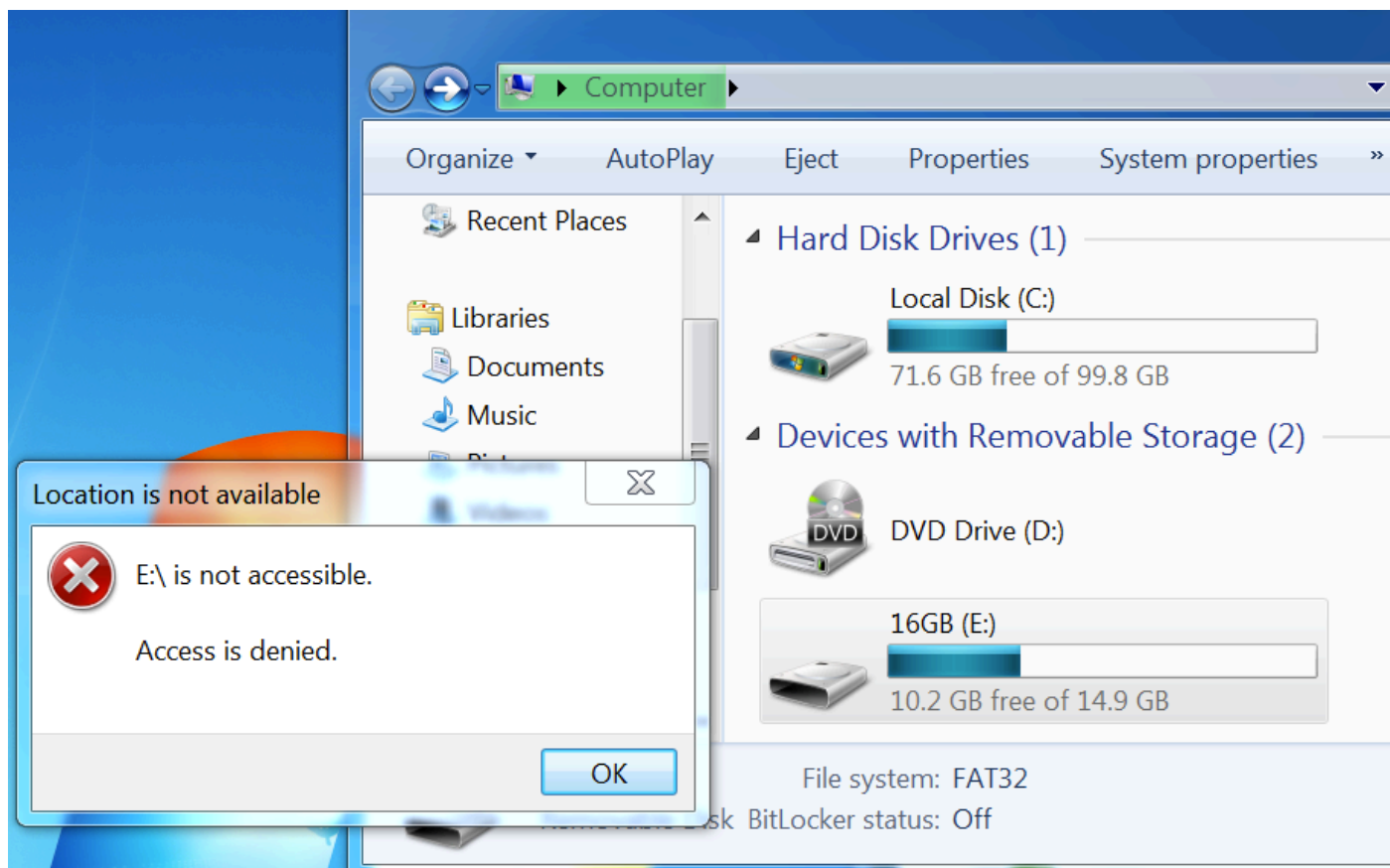
必要に応じて、AnyConnect とともに、ポスチャおよびコンプライアンス モジュールが更新されます。

ポスチャのチェックと CoA

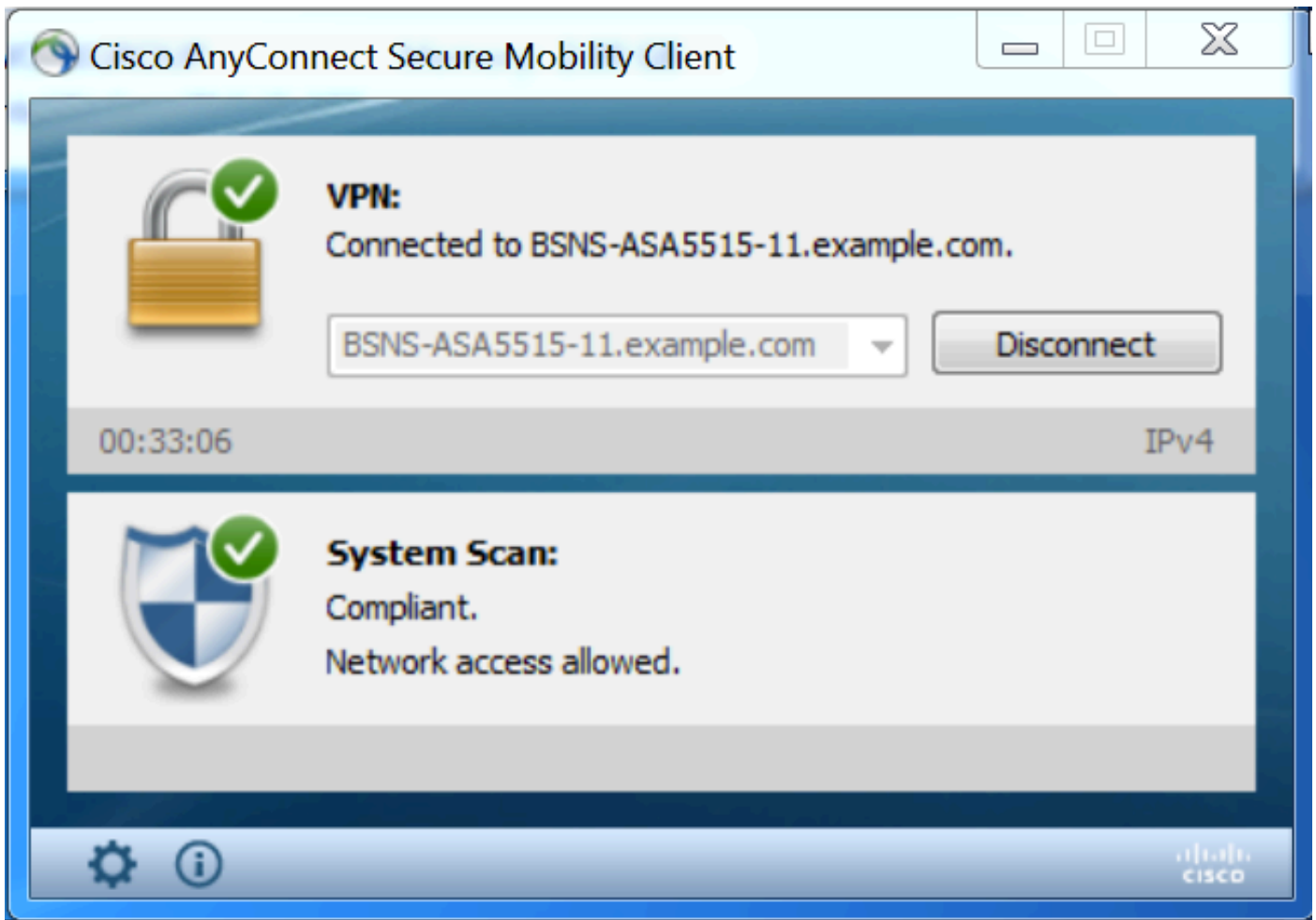
ポスチャ モジュールが実行され、ISE が検出され (enroll.cisco.com での処理が正常に行われるために DNS A レコードが必要になる場合があります)、ポスチャ条件がダウンロードおよびチェックされます。USB デバイスをブロックする新たな OPSWAT v4 アクションが使用されます。設定したメッセージがユーザに表示されます。



ユーザがこのメッセージを確認すると、ユーザはこの USB デバイスを使用できなくなります。



ASA はリダイレクション ACL を削除し、フル アクセスを許可します。適合していることが AnyConnect によって報告されます。



また、ISE の詳細レポートでは、要求される条件を満たしたエンドポイントを確認できます。

条件別のポスチャ アセスメント :

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

エンドポイント別のポスチャ アセスメント :

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

Favorites

ISE Reports

- ▶ Audit
10 reports
- ▶ Device Administration
4 reports
- ▶ Diagnostics
10 reports
- ▼ Endpoints and Users
- Authentication Summary
- Client Provisioning
- Current Active Sessions
- External Mobile Device Management
- Manual Certificate Provisioning
- PassiveID
- Posture Assessment by Condition
- Posture Assessment by Endpoint

Time Range: Today

Run

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

エンドポイントの詳細レポート :

Posture More Detail Assessment

Time Range: From 03/11/2016 12:00:00.000 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 MAC 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		

トラブルシューティング

ISE では不適合条件の詳細を確認できます。これに従い、適切なアクションを実行する必要があります。

参考資料

- [セキュリティ アプライアンスのユーザ承認用の外部サーバの設定](#)
- [Cisco ASA シリーズ VPN CLI 構成ガイド 9.1](#)
- [Cisco Identity Services Engine 管理者ガイド リリース 2.0](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)