

# ISE 2.1- und AnyConnect 4.3-Status-USB-Prüfung konfigurieren

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[ASA](#)

[ISE](#)

[Schritt 1: Netzwerkgerät konfigurieren](#)

[Schritt 2: Konfigurieren der Statusbedingungen und -richtlinien](#)

[Schritt 3: Konfiguration von Client-Bereitstellungsressourcen und Richtlinien](#)

[Schritt 4: Autorisierungsregeln konfigurieren](#)

[Überprüfen](#)

[Einrichtung von VPN-Sitzungen](#)

[Einrichtung von VPN-Sitzungen](#)

[Client-Bereitstellung](#)

[Statusprüfung und CoA](#)

[Fehlerbehebung](#)

[Referenzen](#)

## Einführung

In diesem Dokument wird beschrieben, wie die Cisco Identity Services Engine (ISE) so konfiguriert wird, dass der uneingeschränkte Zugriff auf das Netzwerk nur möglich ist, wenn USB-Massenspeichergeräte getrennt werden.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der CLI-Konfiguration der Adaptive Security Appliance (ASA) und der SSL-VPN-Konfiguration (Secure Socket Layer)
- Grundkenntnisse der Remote-Access-VPN-Konfiguration auf der ASA
- Grundkenntnisse der ISE und Statusservices

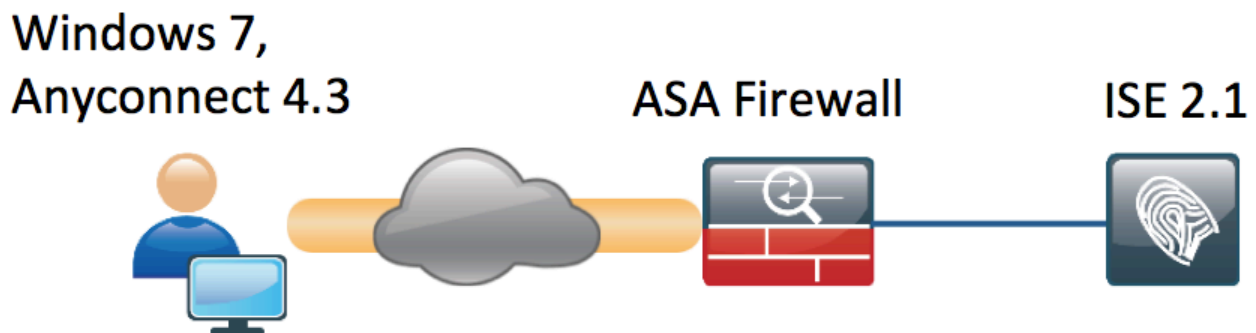
### Verwendete Komponenten

Cisco Identity Services Engine (ISE) Version 2.1 unterstützt zusammen mit AnyConnect Secure Mobility Client 4.3 USB Mass Storage Check und Remediation. Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco ASA Software Version 9.2(4) und höher
- Microsoft Windows 7 mit Cisco AnyConnect Secure Mobility Client Version 4.3 und höher
- Cisco ISE, Version 2.1 und höher

## Konfigurieren

### Netzwerkdiagramm



Der Fluss ist der folgende:

- Der Benutzer ist noch nicht mit dem VPN verbunden, das private USB-Massenspeichergerät ist angeschlossen, und der Benutzer kann Inhalte nutzen.
- Vom AnyConnect-Client initiierte VPN-Sitzung wird über ISE authentifiziert. Der Status des Endpunkts ist nicht bekannt, die Regel "Posture\_Unknown" (Status unbekannt) wird getroffen, und die Sitzung wird an die ISE umgeleitet.
- Die USB-Prüfungen führen eine neue Klasse von Prüfungen des AC ISE-Status ein, da sie den Endpunkt kontinuierlich überwachen, solange er sich im selben ISE-gesteuerten Netzwerk befindet. Die einzige mögliche logische Gegenmaßnahme besteht darin, das/die USB-Gerät(e) zu blockieren, das/die durch den Laufwerksbuchstaben identifiziert wird/werden.
- VPN-Sitzung auf der ASA wird aktualisiert, die Umleitung der ACL wird entfernt und der vollständige Zugriff wird gewährt

Die VPN-Sitzung wurde als Beispiel vorgestellt. Die Statusfunktion funktioniert auch für andere Zugriffstypen gut.

## ASA

ASA wird für den Remote-SSL VPN-Zugriff mithilfe der ISE als AAA-Server konfiguriert. Radius CoA muss zusammen mit der Umleitungszugriffskontrollliste konfiguriert werden:

```
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
```

Weitere Informationen finden Sie unter:

[Konfigurationsbeispiel für die Integration von AnyConnect 4.0 in ISE Version 1.3](#)

## ISE

### Schritt 1: Netzwerkgerät konfigurieren

Von **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

## Schritt 2: Konfigurieren der Statusbedingungen und -richtlinien

Stellen Sie sicher, dass die Statusbedingungen aktualisiert werden: **Verwaltung > System > Einstellungen > Status > Updates > Option Jetzt aktualisieren.**

ISE 2.1 enthält eine vorkonfigurierte USB-Bedingung, die überprüft, ob ein USB-Massenspeichergerät angeschlossen ist.

Von **Richtlinien > Richtlinienelemente > Bedingungen > Status > USB-Zustand** überprüfen Sie den vorhandenen Zustand:

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 ⓘ

Unter **Richtlinien > Richtlinienelemente > Ergebnisse > Status > Anforderungen** überprüfen Sie die vorkonfigurierte Anforderung, die diese Bedingung verwendet.

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

Fügen Sie unter **Richtlinie > Status** eine Bedingung hinzu, dass alle Windows diese Anforderung verwenden:

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

Von Richtlinien > Richtlinienelemente > Ergebnisse > Status > Remediation Actions > USB Remediations (Aktionen zur Problembehebung > USB-Remediations) überprüfen Sie vorkonfigurierte Behebungsmaßnahmen, um USB-Speichergeräte zu blockieren:

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

### Schritt 3: Konfiguration von Client-Bereitstellungsressourcen und Richtlinien

Von Richtlinien > Richtlinienelemente > Client Provisioning > Ressourcen laden Sie Compliance-Modul von Cisco.com herunter und laden Sie das AnyConnect 4.3-Paket manuell hoch:

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, and Client Provisioning. Under Client Provisioning, the 'Results' tab is active, showing a list of 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	

Erstellen Sie mit **Add > NAC Agent oder AnyConnect Posture Profile** ein AnyConnect-Statusprofil (Name: *AnyConnect\_Posture\_Profile*) mit Standardeinstellungen.

Fügen Sie mithilfe von **Add > AnyConnect Configuration** eine AnyConnect-Konfiguration hinzu (Name: AnyConnect-Konfiguration):

The screenshot shows the 'AnyConnect Configuration' page in Cisco ISE. The breadcrumb navigation is: Home > Context Directory > Operations > Policy > Administration > Work Centers. The main menu is the same as in the previous screenshot. The 'Results' tab is active, showing the configuration details for 'AnyConnect Configuration'.

**AnyConnect Configuration > AnyConnect Configuration**

- \* Select AnyConnect Package: AnyConnectDesktopWindows 4.3.520.0
- \* Configuration Name: AnyConnect Configuration
- Description: [Empty text box]
- DescriptionValue
- \* 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 menu]
- Network Access Manager: [Dropdown menu]
- Web Security: [Dropdown menu]
- AMP Enabler: [Dropdown menu]
- Network Visibility: [Dropdown menu]
- Customer Feedback: [Dropdown menu]

Erstellen Sie unter **Richtlinie > Client Provisioning** eine neue Richtlinie (Windows\_Posture) für Windows, um die AnyConnect-Konfiguration zu verwenden:

### 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

## Schritt 4: Autorisierungsregeln konfigurieren

Von **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung** Autorisierungsprofil hinzufügen (Name: Posture\_Redirect), die zu einem Standard-Client-Bereitstellungsportal umgeleitet wird:

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:

Description:

\* Access Type:

Network Device Profile:

Service Template:

Track Movement:

Passive Identity Tracking:

---

### Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL:  Value:

Hinweis: ACL WEBAUTH REDIRECT ACL ist auf ASA definiert.

Erstellen Sie unter **Richtlinien > Autorisierung** eine Autorisierungsregel für die Umleitung. Eine Autorisierungsregel für konforme Geräte ist auf der ISE vorkonfiguriert:



### 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

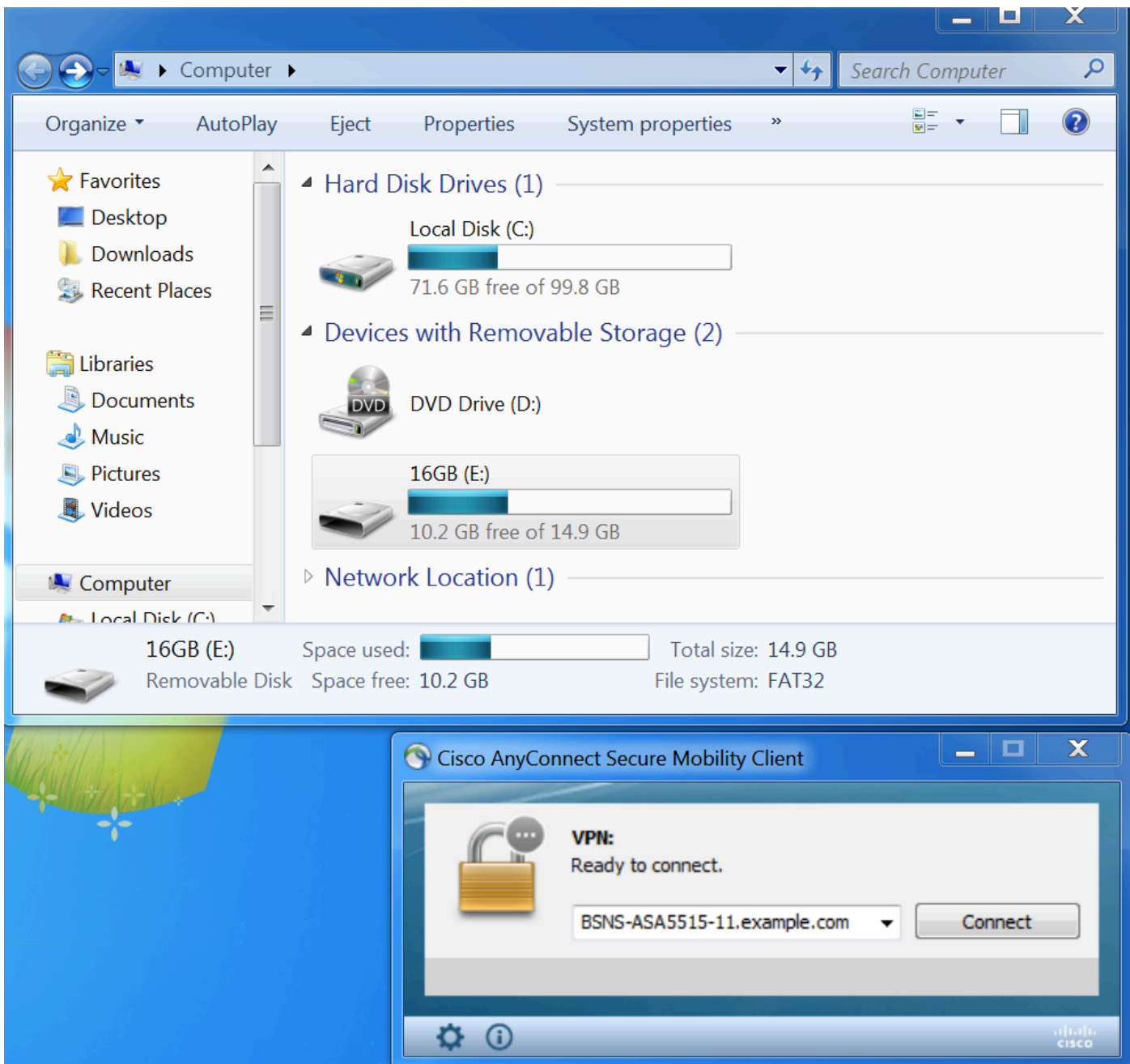
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices )	then PermitAccess
✔	Posture_Unknown	if Session:PostureStatus NOT_EQUALS Compliant	then Posture_Redirect

Wenn der Endpunkt den Vorgaben entspricht, wird umfassender Zugriff bereitgestellt. Wenn der Status unbekannt oder nicht konform ist, wird eine Umleitung für die Client-Bereitstellung zurückgegeben.

## Überprüfen

### Einrichtung von VPN-Sitzungen

USB-Gerät angeschlossen, und der Inhalt ist für den Benutzer verfügbar.



## Einrichtung von VPN-Sitzungen

Während der Authentifizierung gibt die ISE im Rahmen des Status\_Redirect Authorization Profile (Status\_Redirect-Autorisierungsprofils) die Umleitungsliste zurück und leitet die URL um.

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

Nach Einrichtung der VPN-Sitzung wird der ASA-Datenverkehr vom Client entsprechend der

## Umleitungsliste umgeleitet:

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

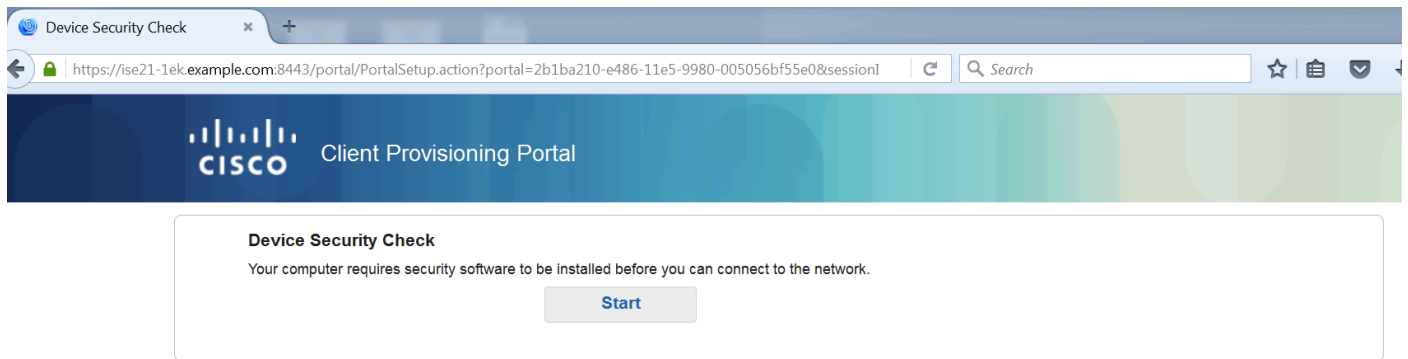
Idle Time Out: 30 Minutes                      Idle TO Left : 26 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.00520  
Bytes Tx : 1294                                      Bytes Rx : 16389  
Pkts Tx : 10                       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

## Client-Bereitstellung

In dieser Phase wird der Webbrowser-Datenverkehr des Endgeräts zur Client-Bereitstellung an die ISE umgeleitet:



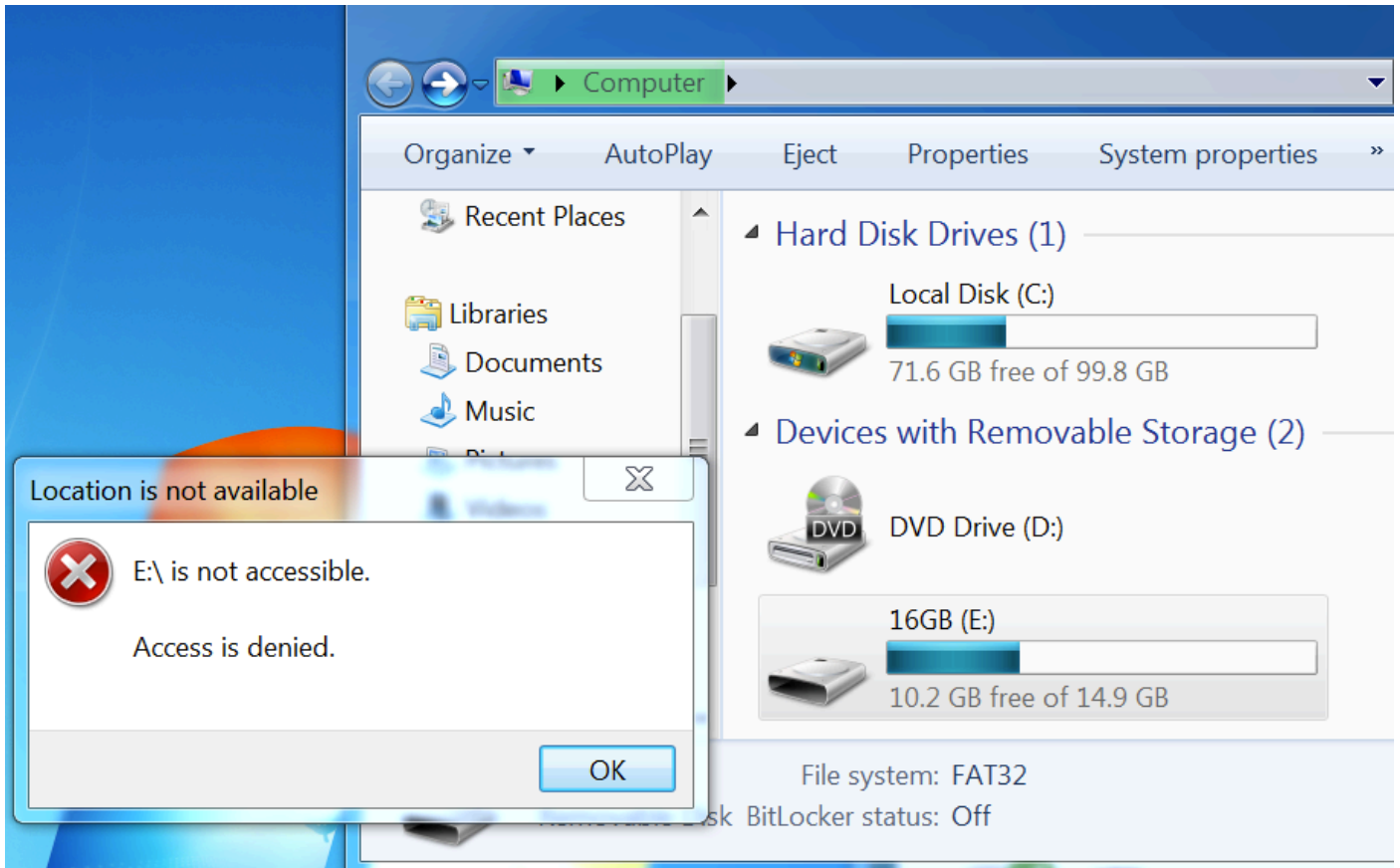
Bei Bedarf wird AnyConnect zusammen mit dem Status- und Compliance-Modul aktualisiert.

## Statusprüfung und CoA

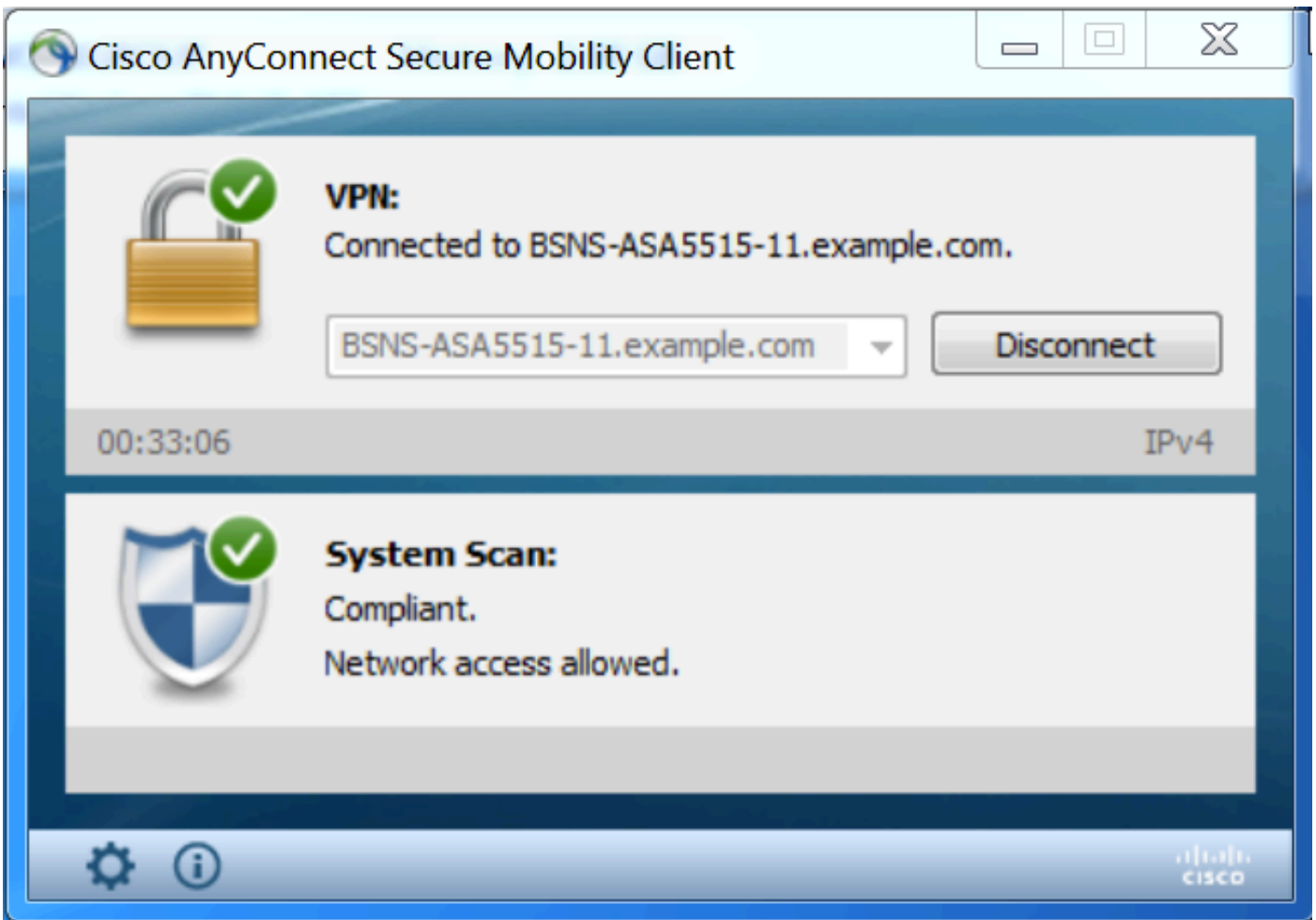
Statusmodul wird ausgeführt, ISE wird ermittelt (es kann erforderlich sein, dass DNS A-Eintrag für enroll.cisco.com vorhanden ist, um erfolgreich zu sein), Statusbedingungen heruntergeladen und überprüft, neue OPSWAT v4-Block USB-Geräteaktion. Die konfigurierte Nachricht wird für den Benutzer angezeigt:



Sobald die Meldung bestätigt wurde, ist das USB-Gerät für den Benutzer nicht mehr verfügbar:



ASA entfernt Umleitungszugriffskontrolllisten, die vollständigen Zugriff ermöglichen. AnyConnect meldet Compliance:



Darüber hinaus können detaillierte Berichte zur ISE bestätigen, dass die erforderlichen Bedingungen erfüllt wurden.

Statusüberprüfung nach Bedingung:

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
    - Filters
    - \* Time Range Today
    - Run

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

Statusüberprüfung nach Endpunkt:

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

## Details zum Endpunktbericht:

**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		

## Fehlerbehebung

Die ISE kann Einzelheiten zu den ausgefallenen Bedingungen mitteilen. Daher sollten entsprechende Maßnahmen ergriffen werden.

## Referenzen

- [Konfigurieren eines externen Servers für die Benutzerautorisierung der Sicherheitsappliance](#)
- [Konfigurationsleitfaden für die CLI der Cisco ASA-Serie 9.1](#)
- [Administratoranleitung für Cisco Identity Services Engine, Version 2.0](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)