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

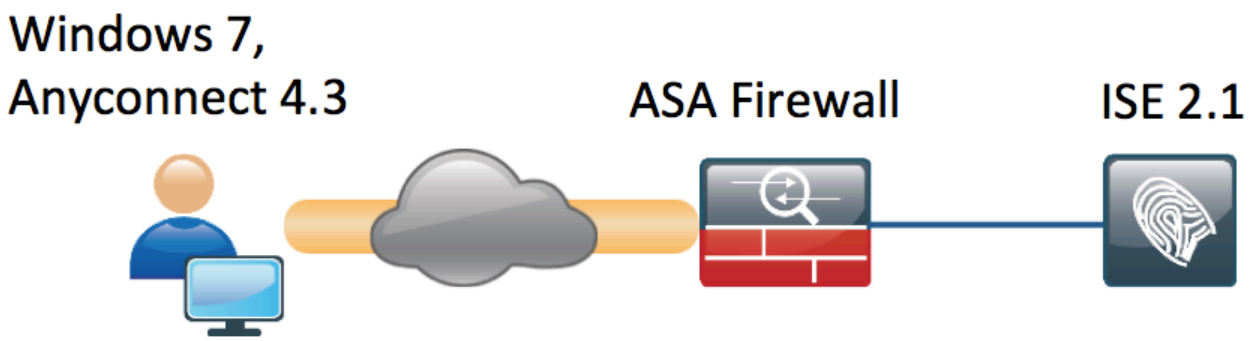
Verwendete Komponenten

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 Laufwerkbuchstaben 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
```

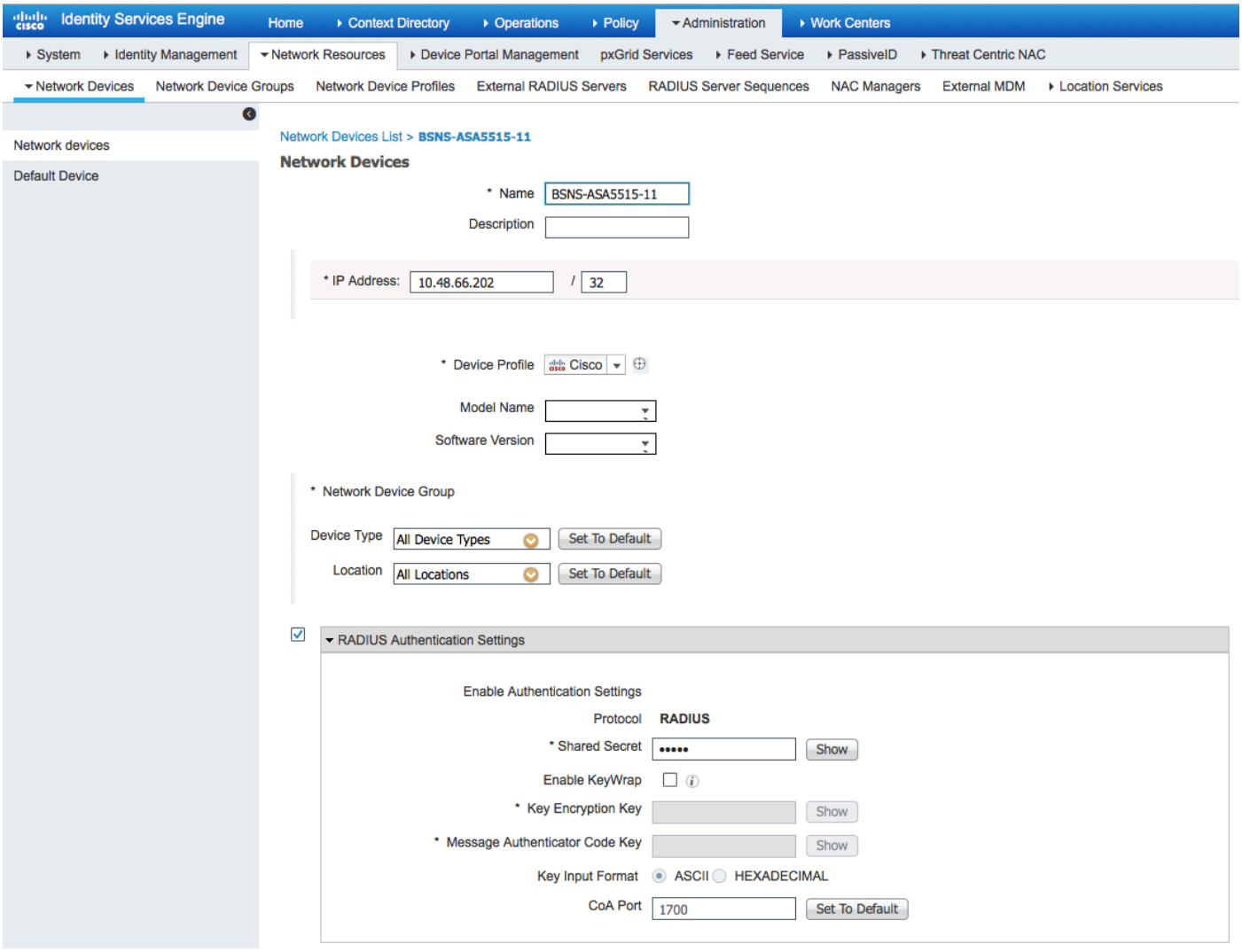
Weitere Informationen finden Sie unter:

[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

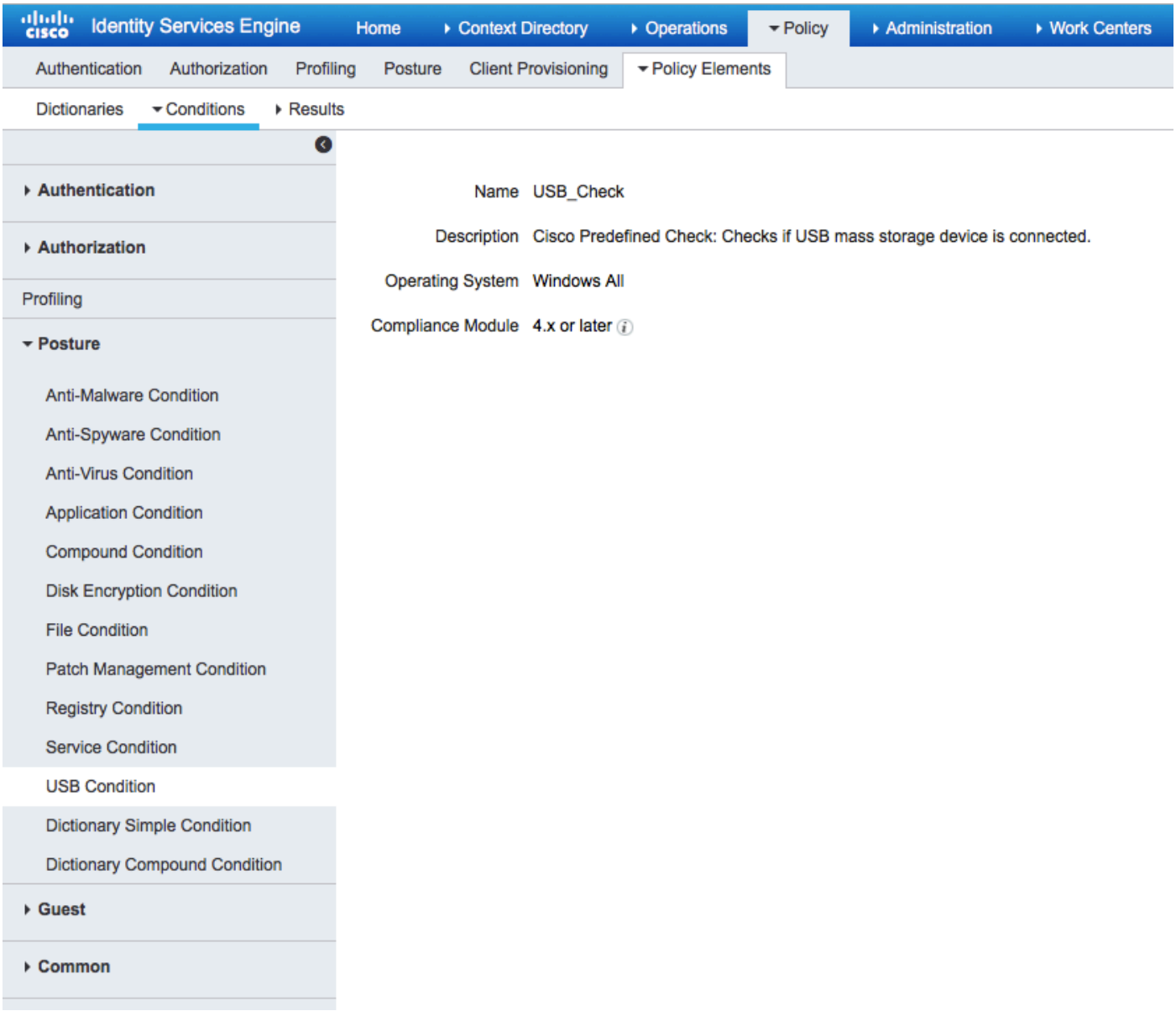


Schritt 2: Konfigurieren der Statusbedingungen und -richtlinien

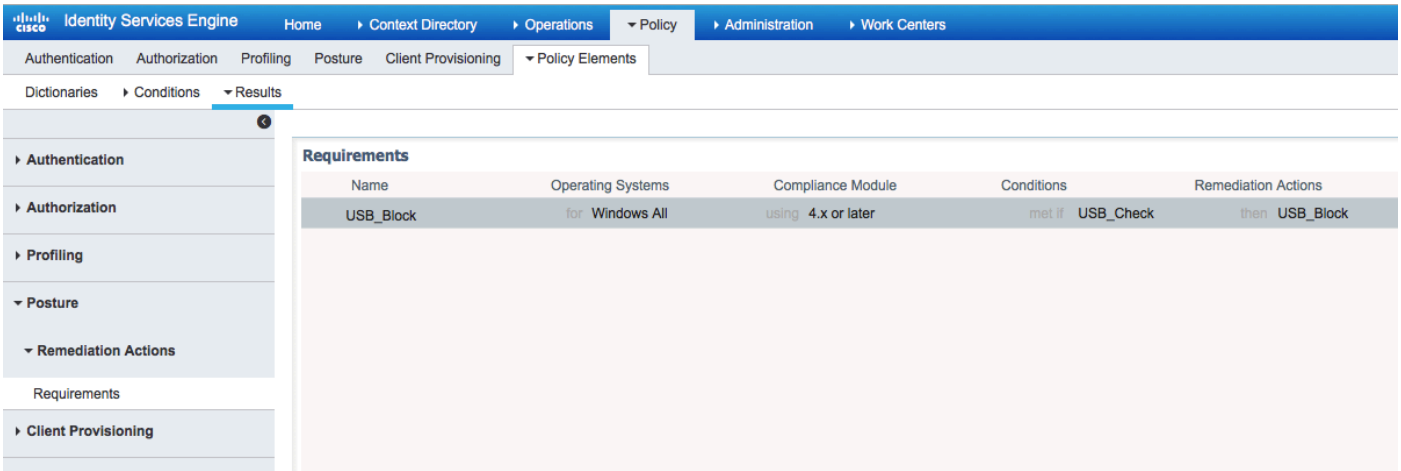
Stellen Sie sicher, dass die Statusbedingungen aktualisiert werden: **Verwaltung > System > Einstellungen > Status > Updates > Option Jetzt aktualisieren**.

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

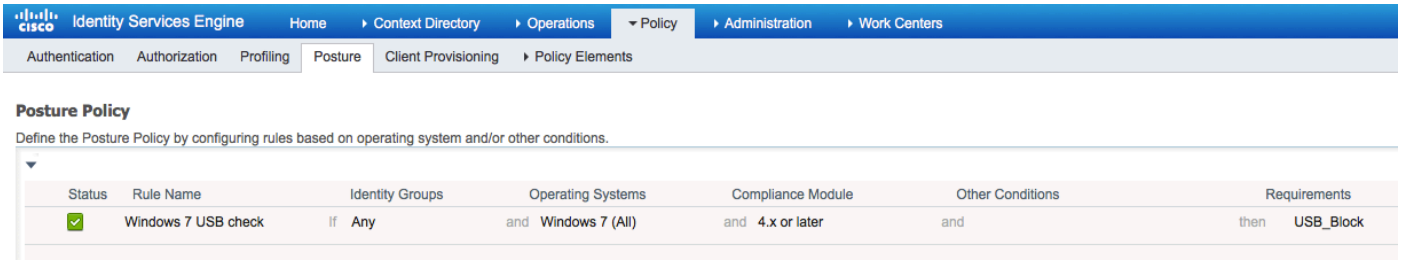
Von **Richtlinien > Richtlinienelemente > Bedingungen > Status > USB-Zustand** überprüfen Sie den vorhandenen Zustand:



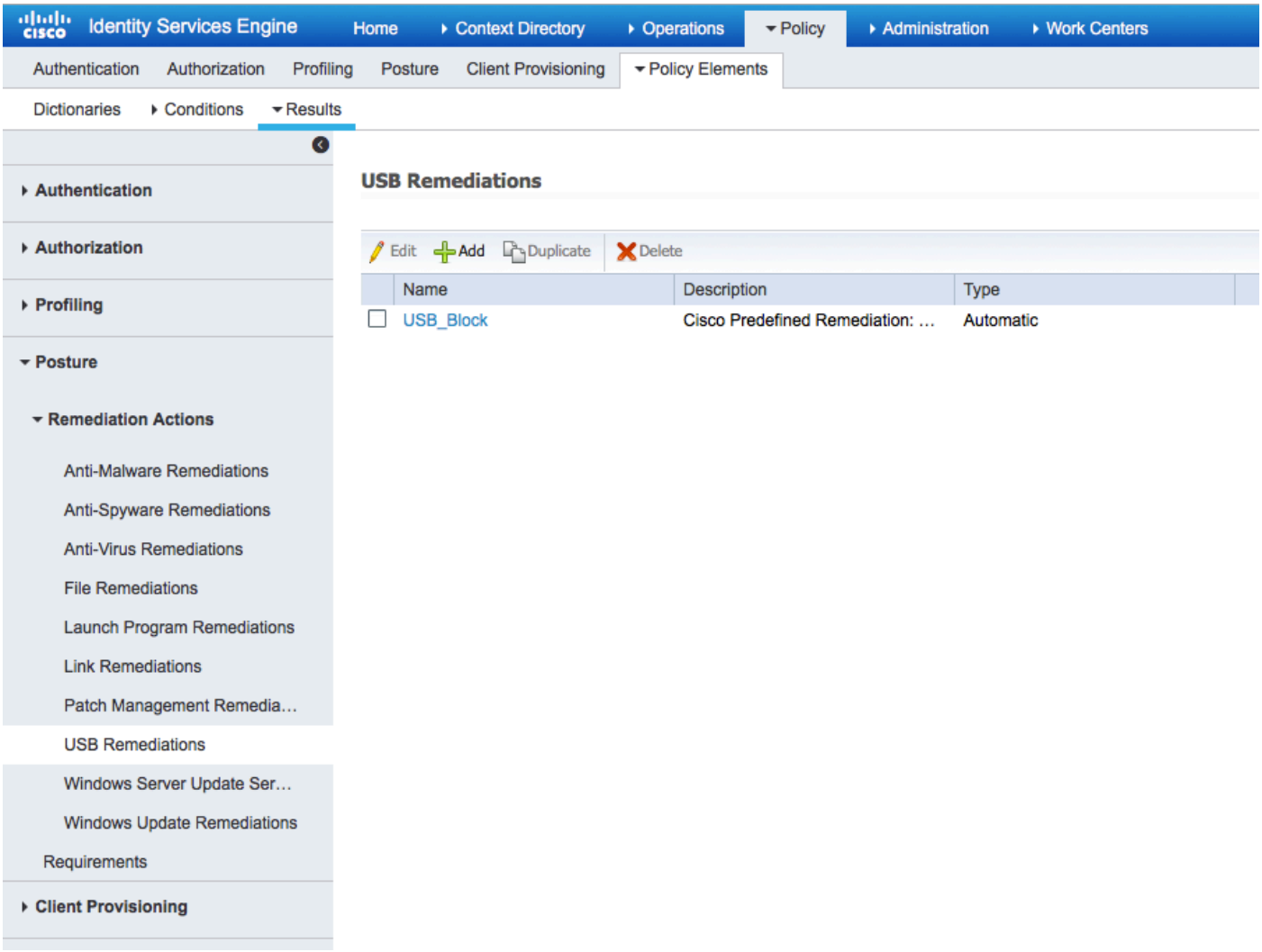
Unter **Richtlinien > Richtlinienelemente > Ergebnisse > Status > Anforderungen** überprüfen Sie die vorkonfigurierte Anforderung, die diese Bedingung verwendet.



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

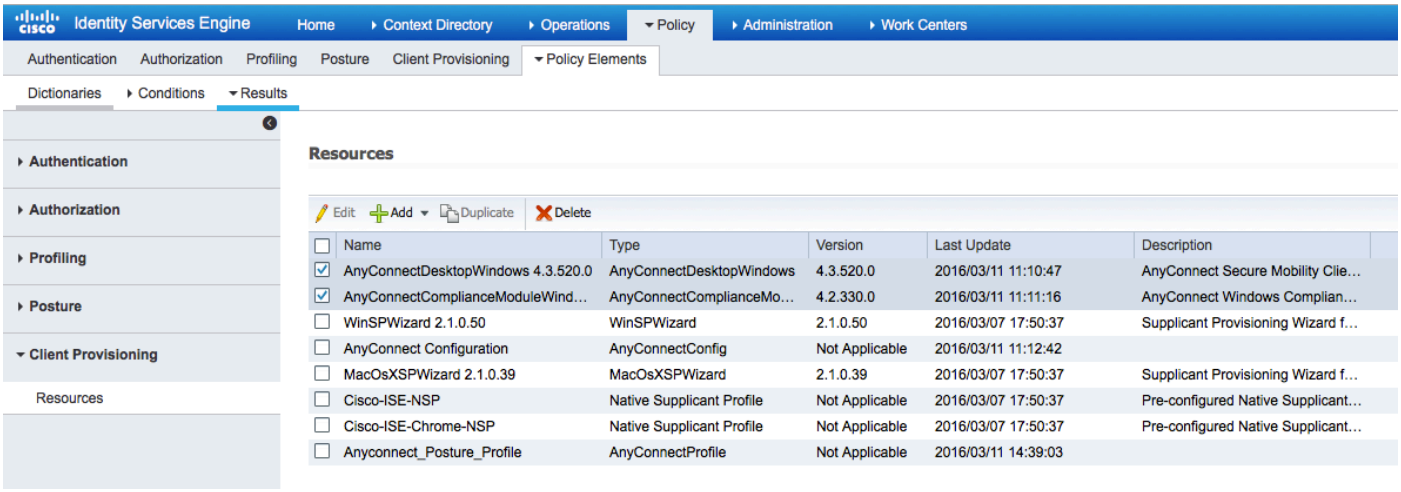


Von **Richtlinien > Richtlinienelemente > Ergebnisse > Status > Remediation Actions > USB Remediations (Aktionen zur Problembehebung > USB-Remediations)** überprüfen Sie vorkonfigurierte Behebungsmaßnahmen, um USB-Speichergeräte zu blockieren:



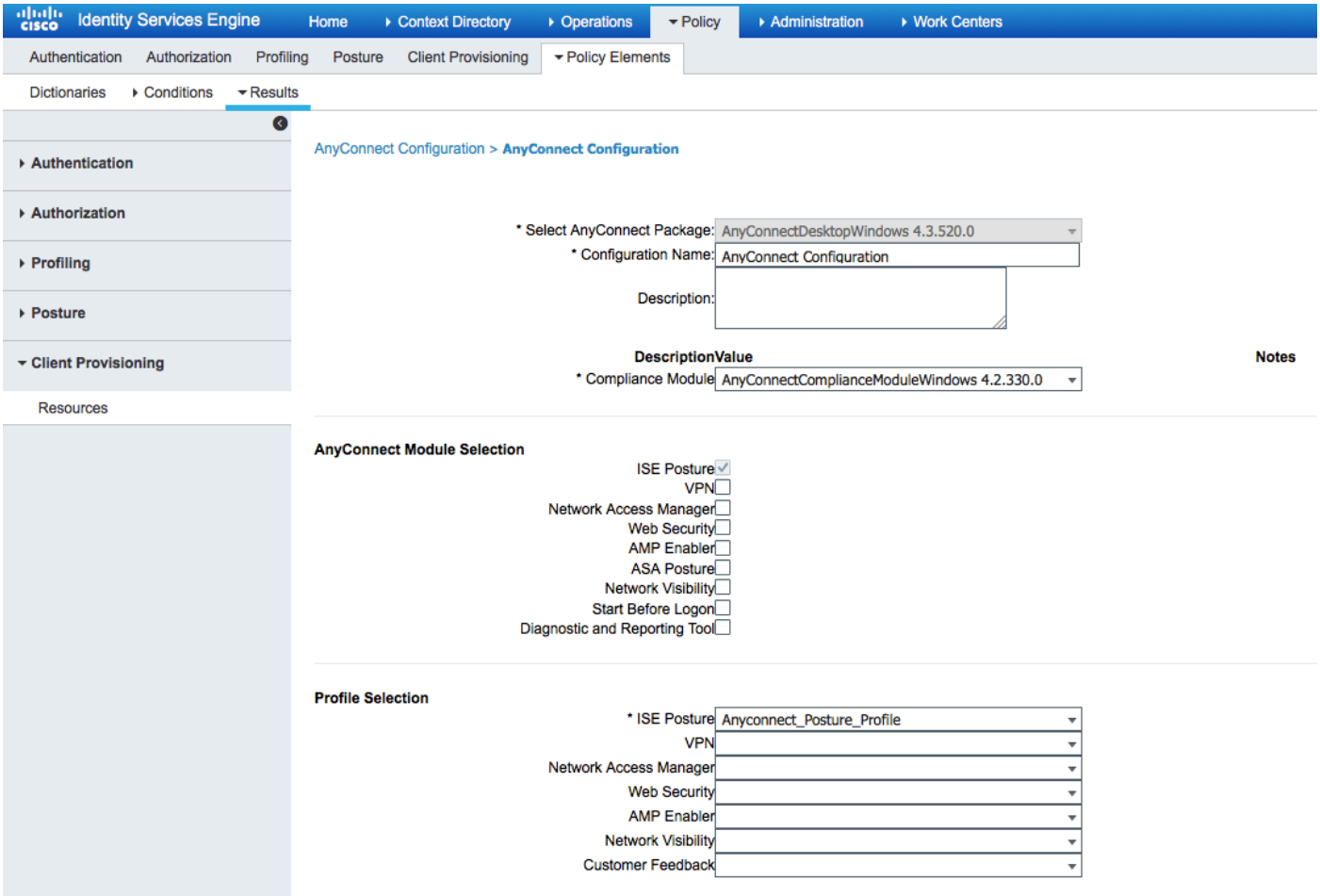
Schritt 3: Konfiguration von Client-Bereitstellungsressourcen und Richtlinien

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

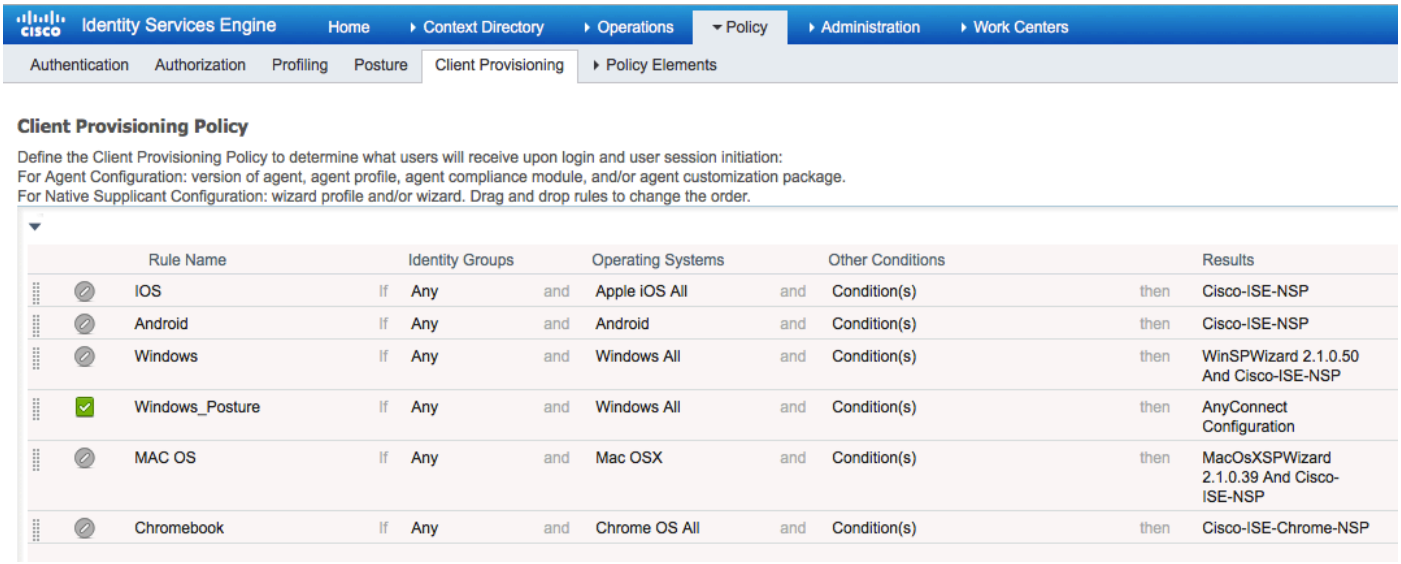


Erstellen Sie mit **Add > NAC Agent oder AnyConnect Posture Profile** ein AnyConnect-Statusprofil (Name: *AnyConnect_Posture_Profile*) mit Standardeinstellungen.

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

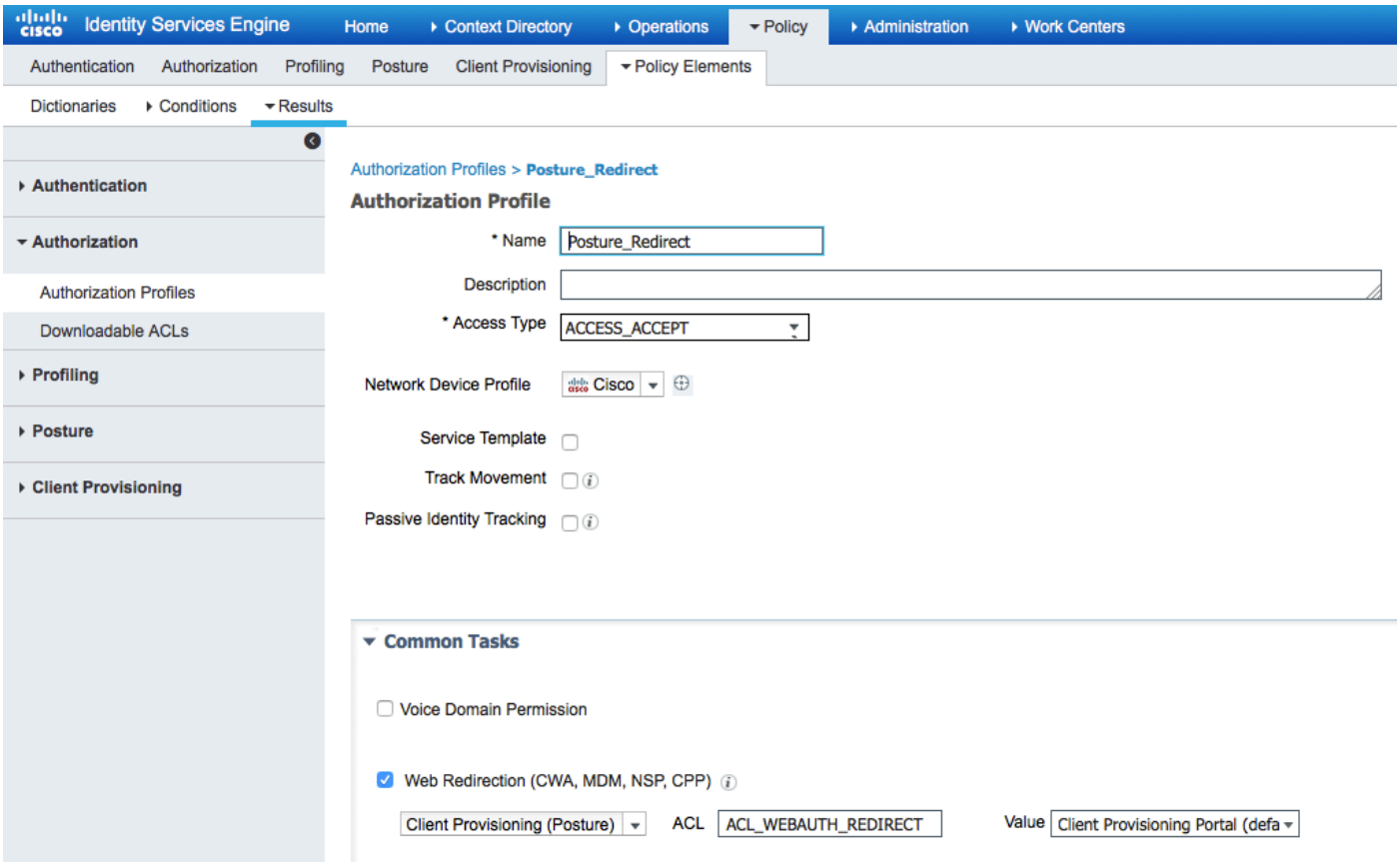


Erstellen Sie unter **Richtlinie > Client Provisioning** eine neue Richtlinie (Windows_Posture) für Windows, um die AnyConnect-Konfiguration zu verwenden:



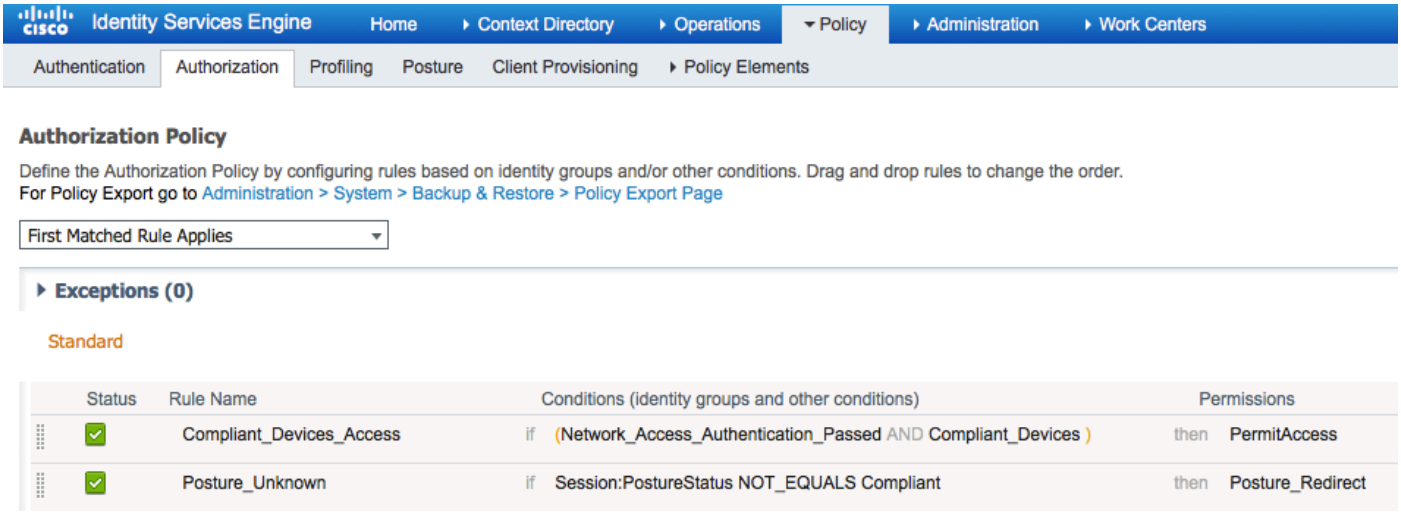
Schritt 4: Autorisierungsregeln konfigurieren

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



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:

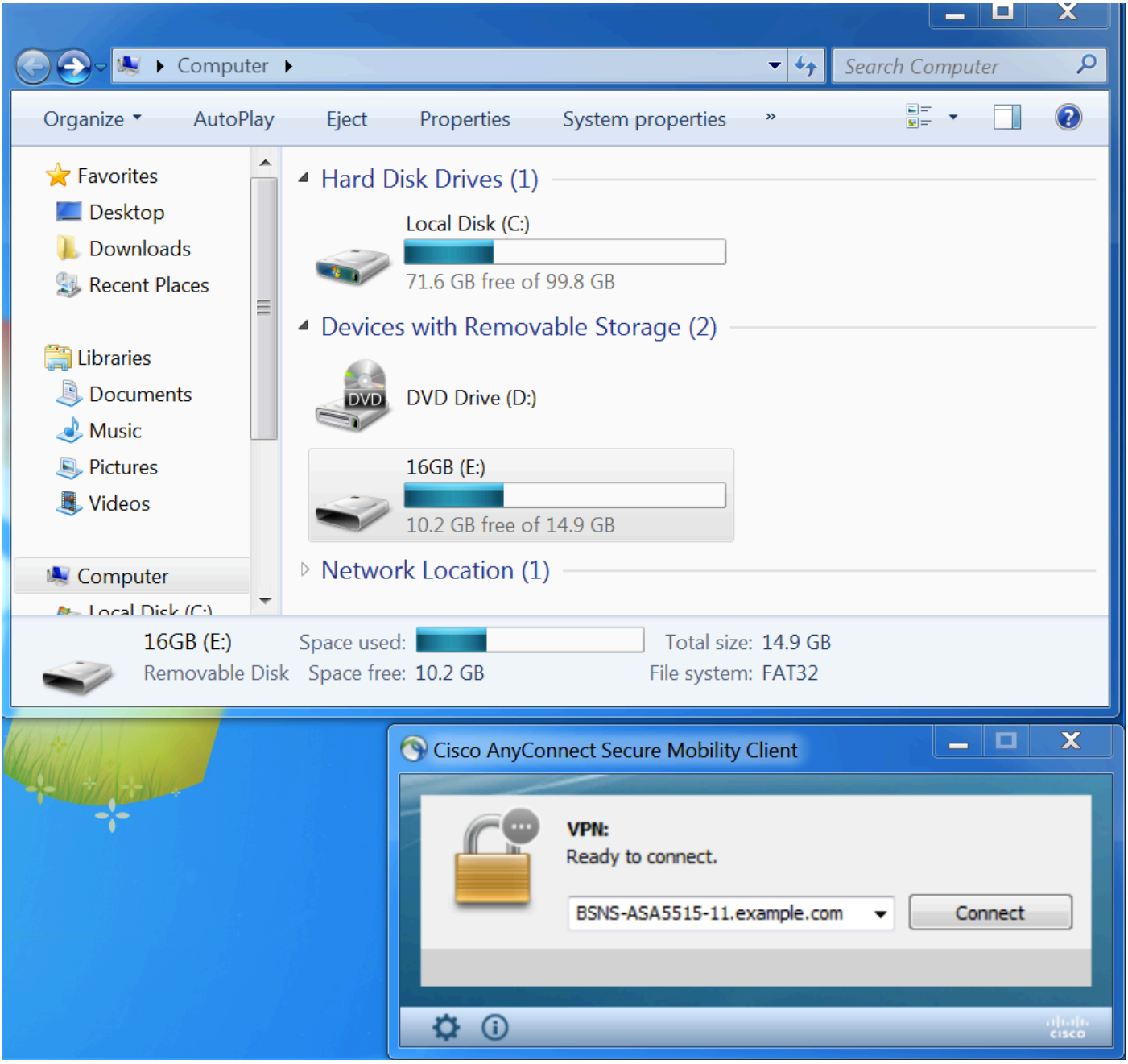


Wenn der Endpunkt den Vorgaben entspricht, wird umfassender Zugriff bereitgestellt. Wenn der Status unbekannt oder nicht konform ist, wird eine Umleitung für die Client-Bereitstellung zurückgegeben.

Überprüfen

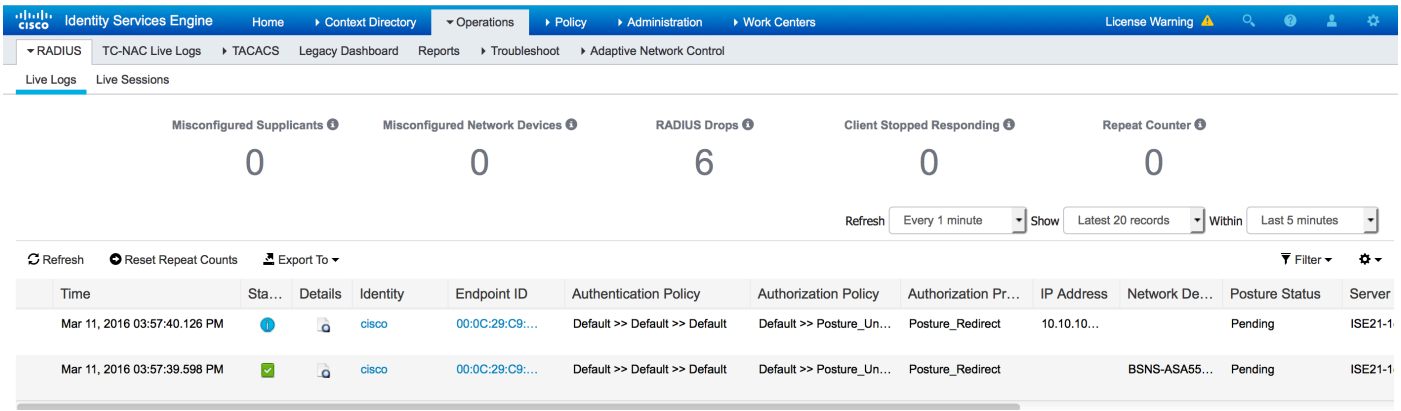
Einrichtung von VPN-Sitzungen

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.



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

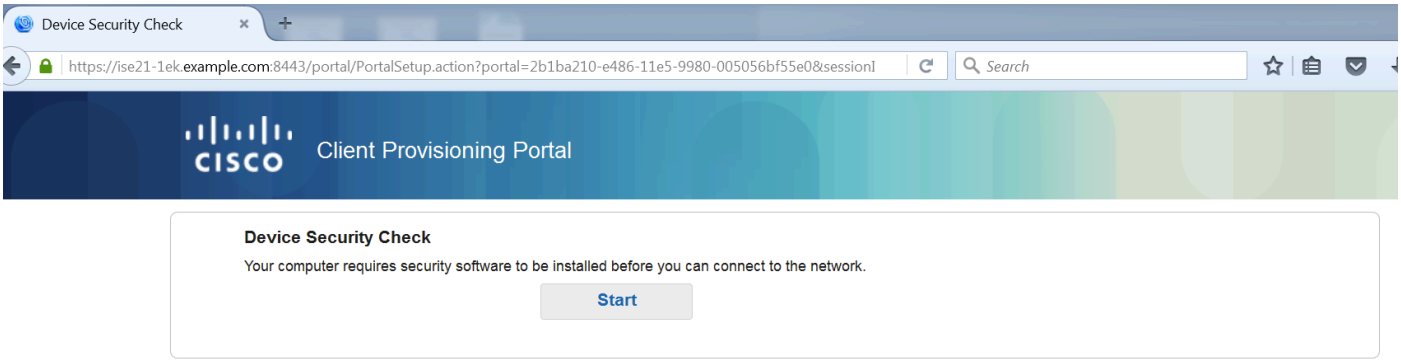
Umleitungsliste umgeleitet:

```
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

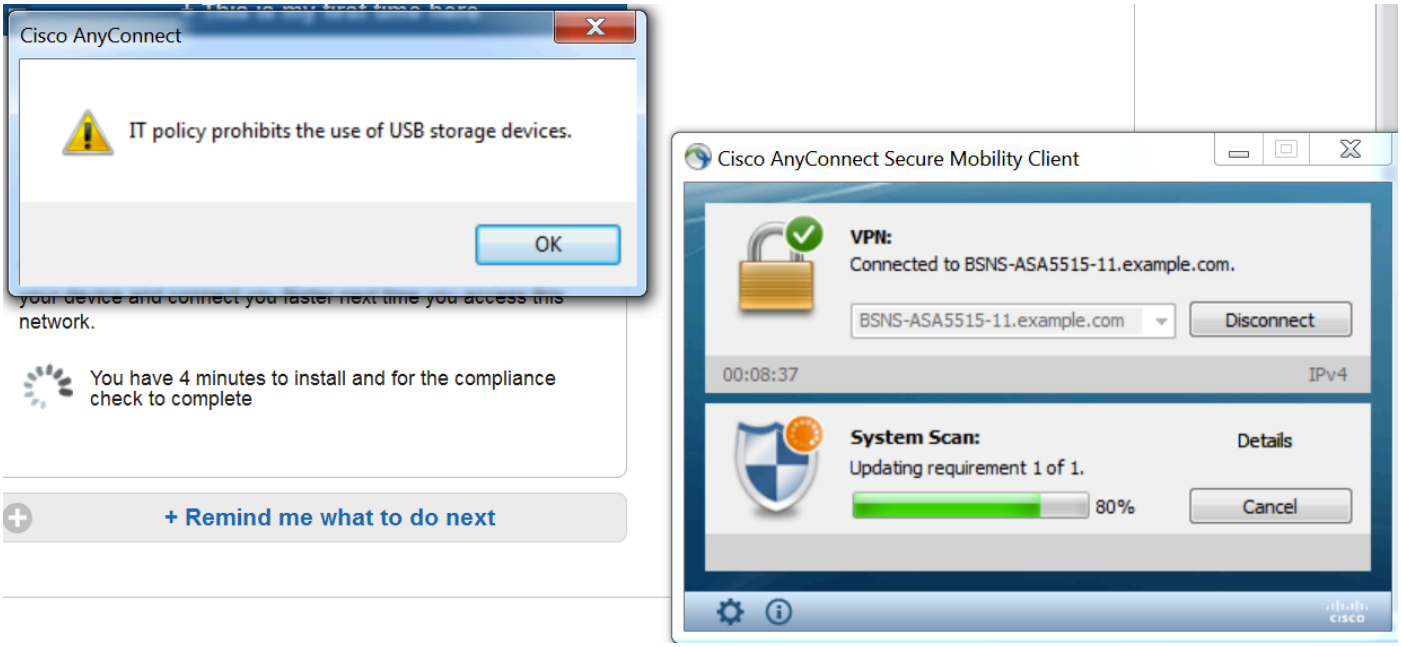
In dieser Phase wird der Webbrowser-Datenverkehr des Endgeräts zur Client-Bereitstellung an die ISE umgeleitet:



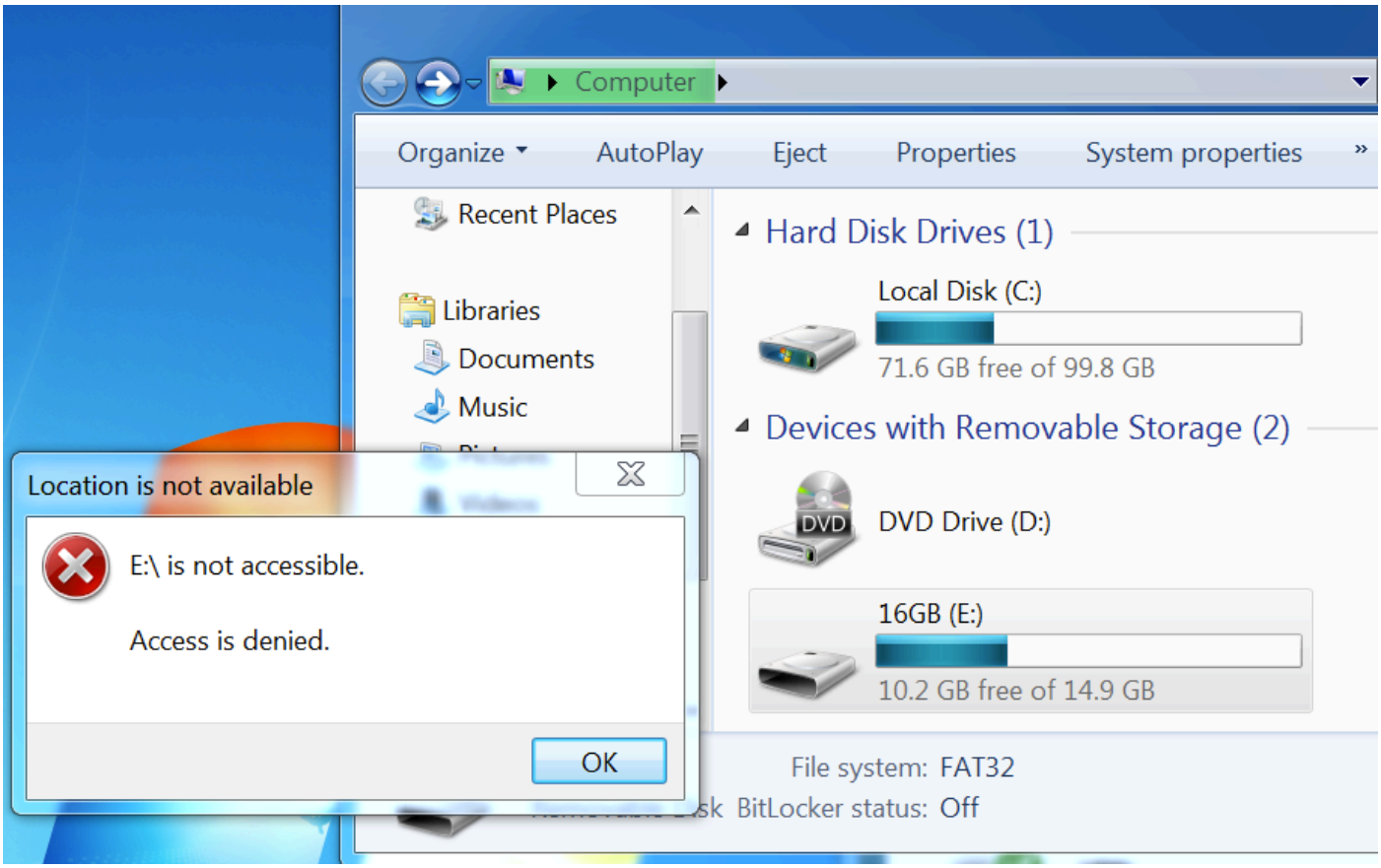
Bei Bedarf wird AnyConnect zusammen mit dem Status- und Compliance-Modul aktualisiert.

Statusprüfung und CoA

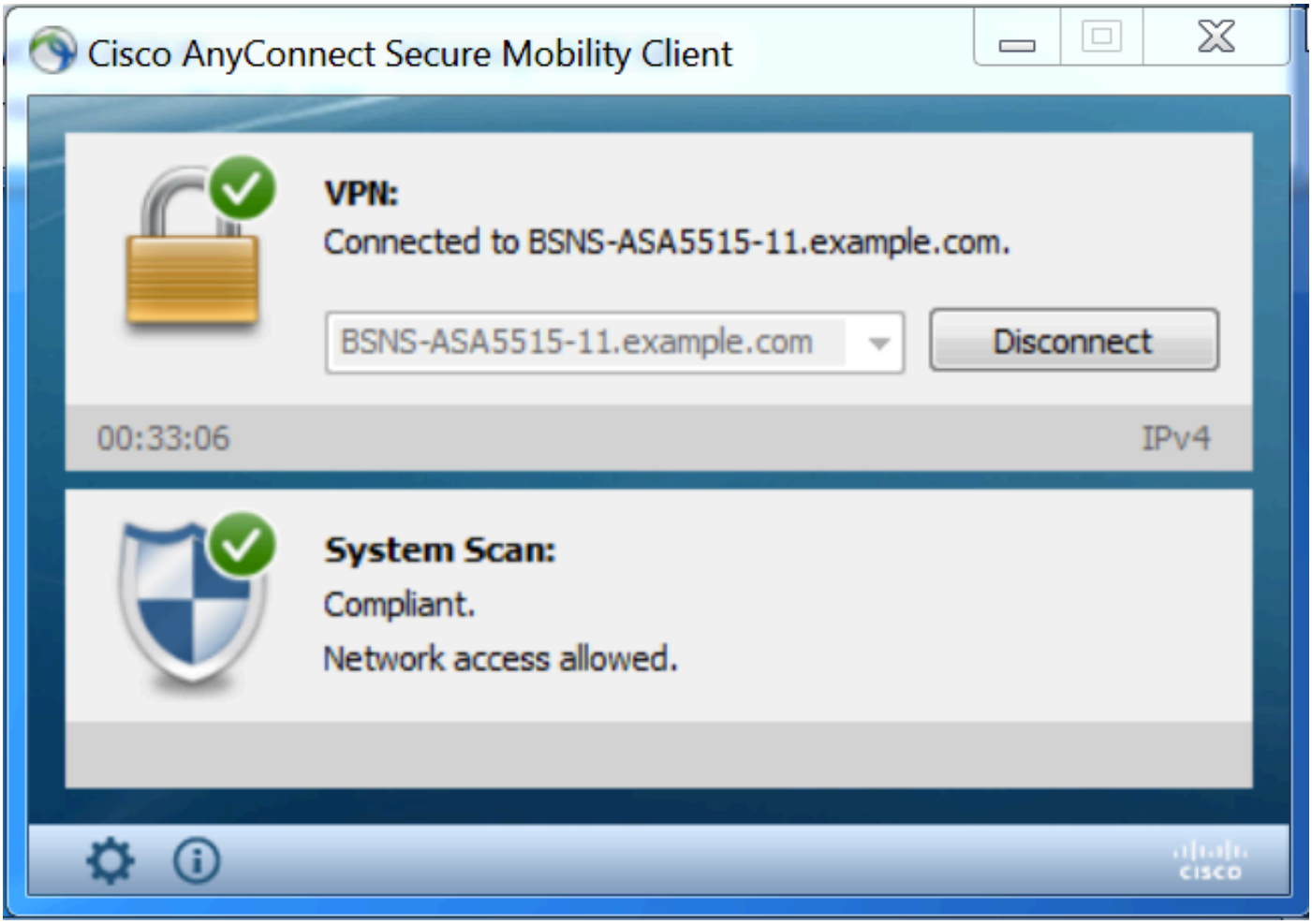
Statusmodul wird ausgeführt, ISE wird ermittelt (es kann erforderlich sein, dass DNS A-Eintrag für enroll.cisco.com vorhanden ist, um erfolgreich zu sein), Statusbedingungen heruntergeladen und überprüft, neue OPSWAT v4-Block USB-Geräteaktion. Die konfigurierte Nachricht wird für den Benutzer angezeigt:



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

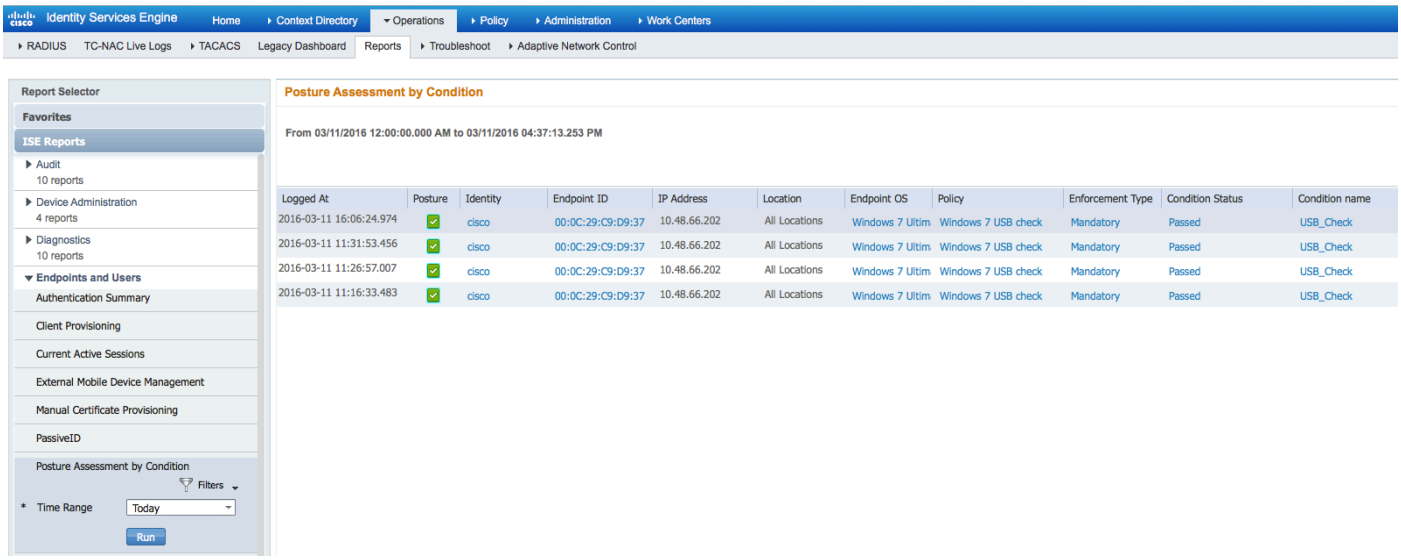


ASA entfernt Umleitungszugriffskontrolllisten, die vollständigen Zugriff ermöglichen. AnyConnect meldet Compliance:

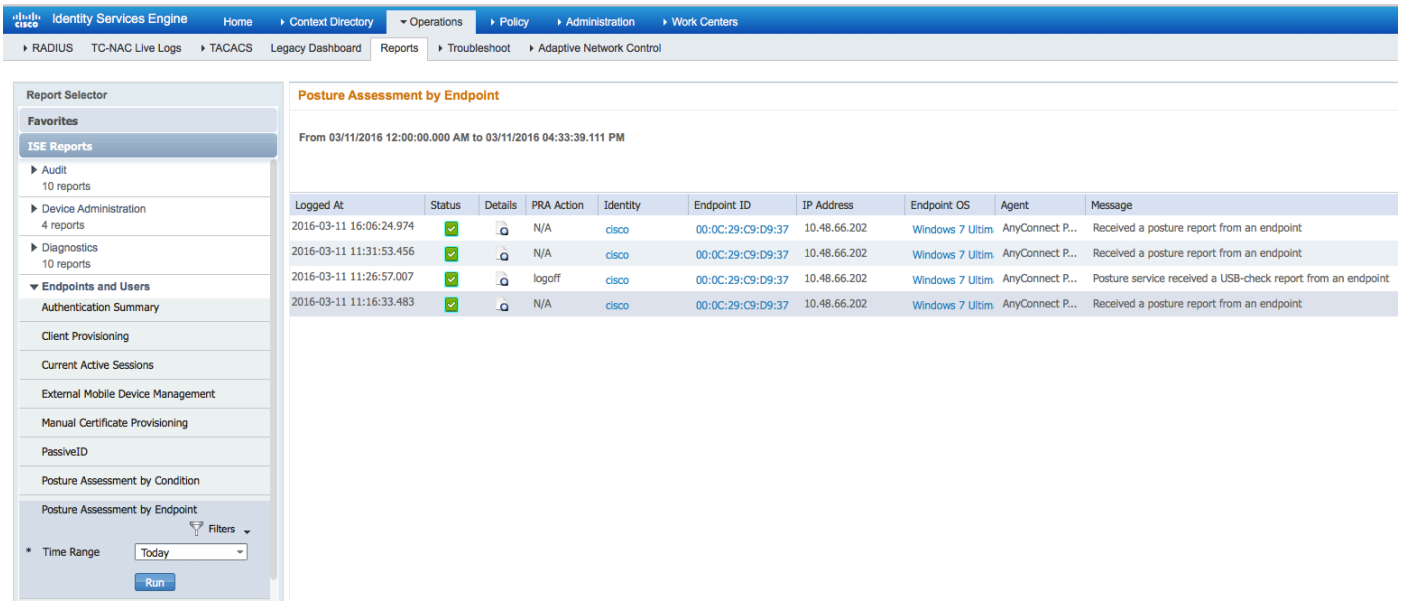


Darüber hinaus können detaillierte Berichte zur ISE bestätigen, dass die erforderlichen Bedingungen erfüllt wurden.

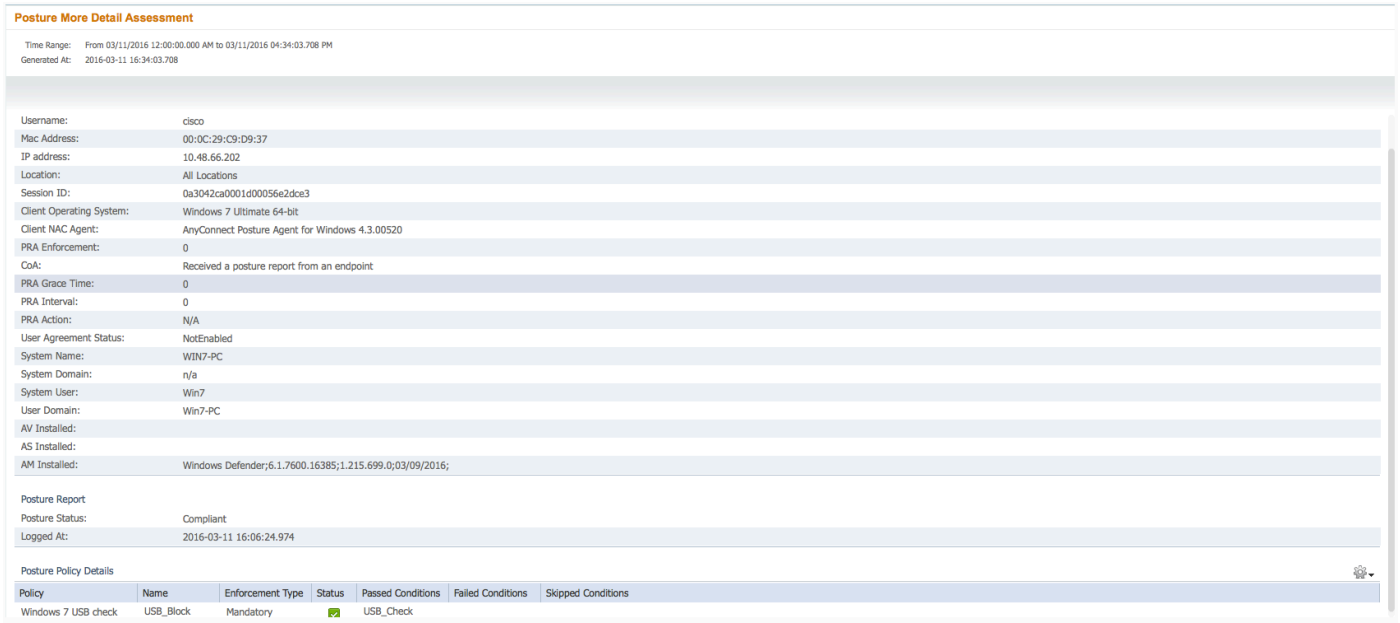
Statusüberprüfung nach Bedingung:



Statusüberprüfung nach Endpunkt:



Details zum Endpunktbericht:



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