# ISE 2.0 konfigurieren und AnyConnect 4.2-Posture BitlLocker-Verschlüsselung verschlüsseln

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie die Datenträgerpartition des Endpunkts mithilfe von Microsoft BitLocker verschlüsselt wird und wie die Cisco Identity Services Engine (ISE) so konfiguriert wird, dass der uneingeschränkte Zugriff auf das Netzwerk nur dann gewährleistet wird, wenn die richtige Verschlüsselung konfiguriert ist. Cisco ISE Version 2.0 unterstützt zusammen mit AnyConnect Secure Mobility Client 4.2 die Statusüberprüfung der Festplattenverschlüsselung.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CLI-Konfiguration der Adaptive Security Appliance (ASA) und SSL-VPN-Konfiguration (Secure Socket Layer)

- VPN-Konfiguration für Remote-Zugriff auf der ASA
- ISE und Statusservices

### Verwendete Komponenten

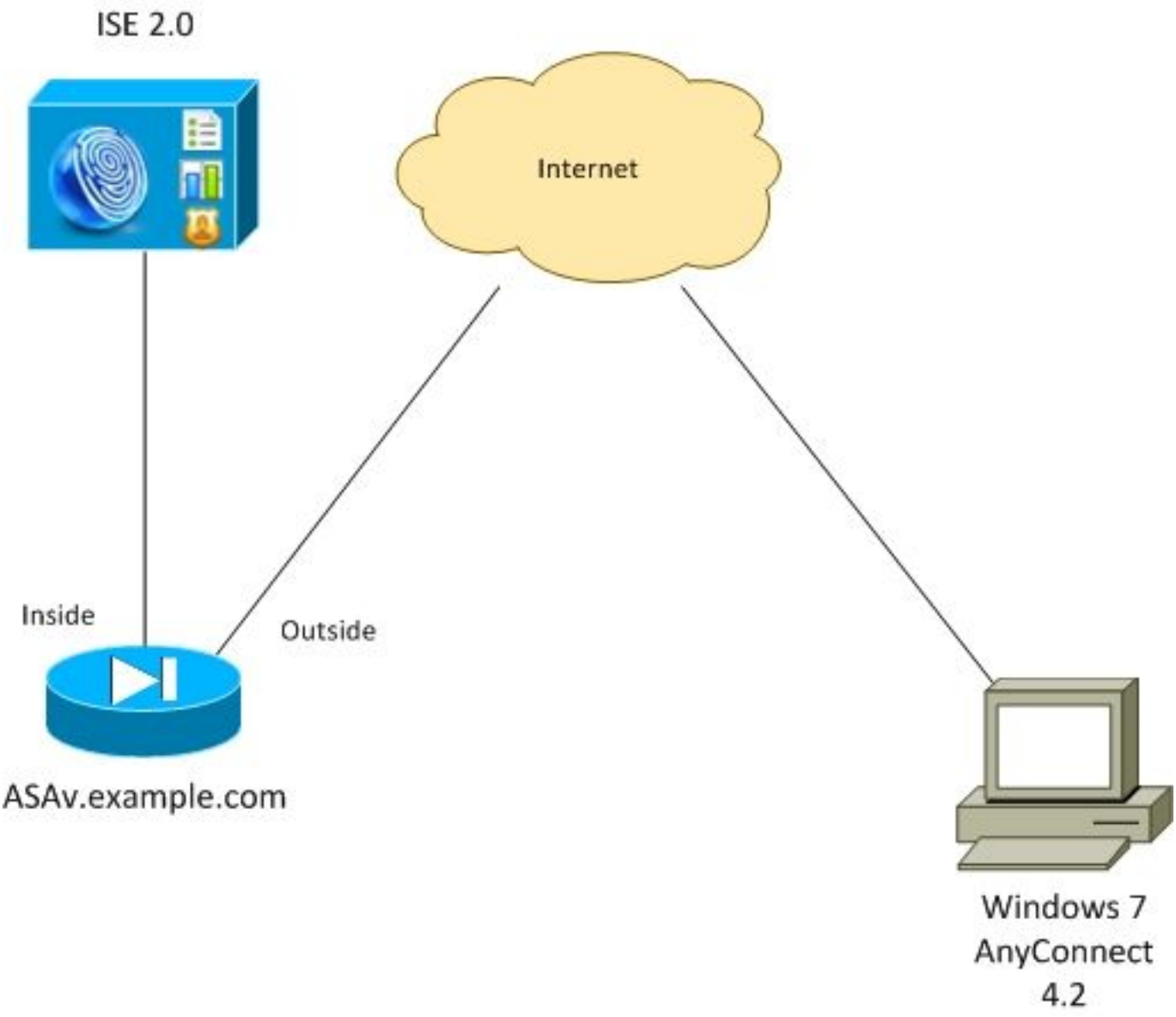
Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco ASA Software Version 9.2.1 oder höher
- Microsoft Windows 7 mit Cisco AnyConnect Secure Mobility Client Version 4.2 und höher
- Cisco ISE, Version 2.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

### Netzwerkdiagramm



Der Ablauf ist wie folgt:

- Vom AnyConnect-Client initiierte VPN-Sitzung wird über ISE authentifiziert. Der Status des Endpunkts ist nicht bekannt, Regel **ASA VPN** ist **unbekannt** wird aufgerufen, und die Sitzung wird zur Bereitstellung an die ISE umgeleitet.
- Benutzer öffnet Webbrowser, HTTP-Datenverkehr wird von ASA an ISE umgeleitet. Die ISE leitet die neueste Version von AnyConnect zusammen mit dem Status- und Compliance-Modul an das Endgerät weiter
- Sobald das Statusmodul ausgeführt wurde, prüft es, ob Partition **E:** ist vollständig mit BitLocker verschlüsselt. Wenn ja, wird der Bericht an die ISE gesendet, die RADIUS Change of Authorization (CoA) ohne Zugriffskontrolllisten (vollständiger Zugriff) auslöst.
- VPN-Sitzung auf ASA wird aktualisiert, ACL umgeleitet und Sitzung ist vollständig zugänglich

Als Beispiel wird eine VPN-Sitzung dargestellt. Die Statusfunktion funktioniert auch für andere Zugriffstypen.

## ASA

Die Konfiguration erfolgt über den Remote-SSL VPN-Zugriff unter Verwendung der ISE als AAA-Server (Authentication, Authorization, and Accounting). Radius CoA muss zusammen mit REDIRECT ACL konfiguriert werden:

```
aaa-server ISE20 protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE20 (inside) host 10.48.17.235
 key cisco

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
 address-pool POOL
authentication-server-group ISE20
 accounting-server-group ISE20
 default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
 group-alias TAC enable

group-policy AllProtocols internal
group-policy AllProtocols attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable

access-list REDIRECT extended deny udp any any eq domain
access-list REDIRECT extended deny ip any host 10.48.17.235
access-list REDIRECT extended deny icmp any any
access-list REDIRECT extended permit tcp any any eq www
```

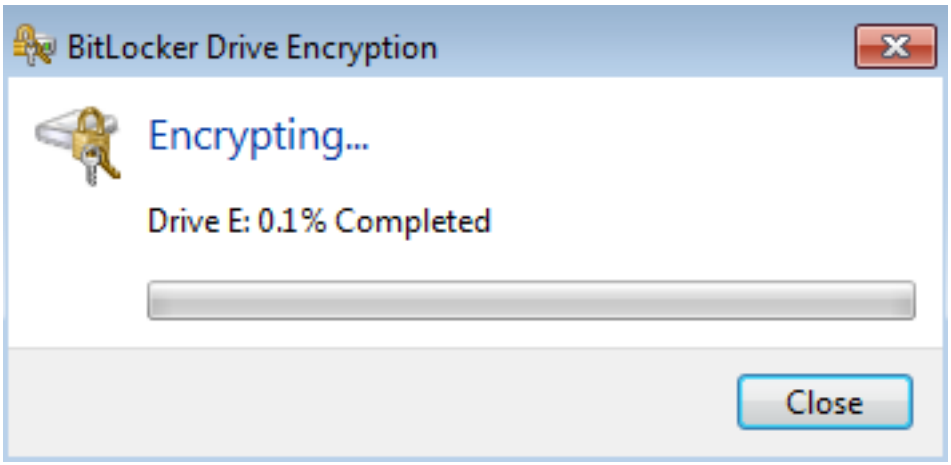
```
ip local pool POOL 172.16.31.10-172.16.31.20 mask 255.255.255.0
```

Weitere Informationen finden Sie unter:

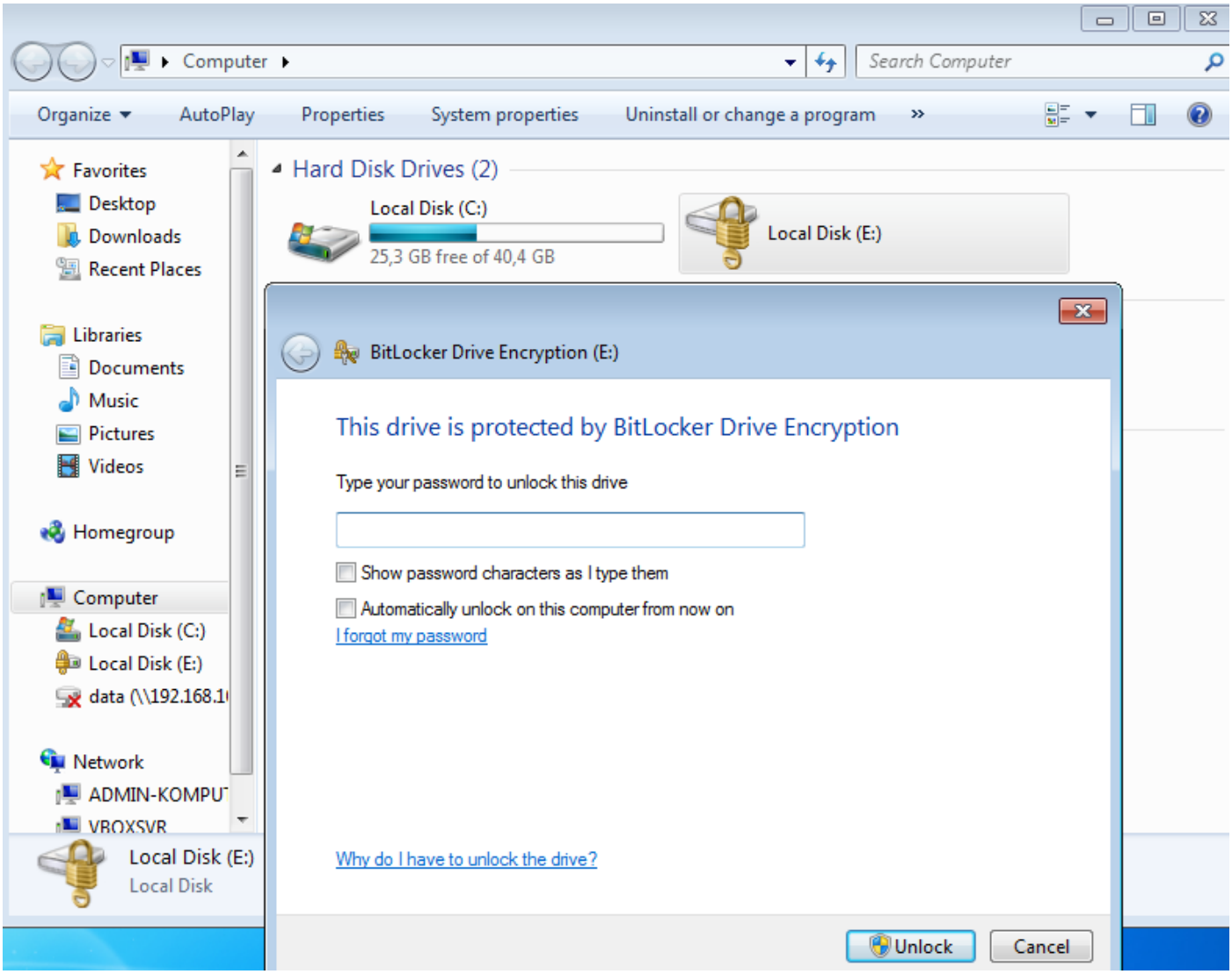
[Konfigurationsbeispiel für die Integration von AnyConnect 4.0 in ISE Version 1.3]

## BitLocker in Windows 7

Navigieren Sie zu **Systemsteuerung > System und Sicherheit > BitLocker-Laufwerkverschlüsselung**, aktivieren Sie **E:** Partitionsverschlüsselung. Schützen Sie es durch ein Passwort (PIN), wie im Bild gezeigt.




Sobald er verschlüsselt ist, mounten Sie ihn (mit dem Passwort) und stellen Sie sicher, dass er wie im Bild gezeigt zugänglich ist.




Weitere Informationen finden Sie in der Microsoft-Dokumentation:

Schrittweise Anleitung zur Windows BitLocker-Laufwerkverschlüsselung

## ISE

### Schritt 1: Netzwerkgerät

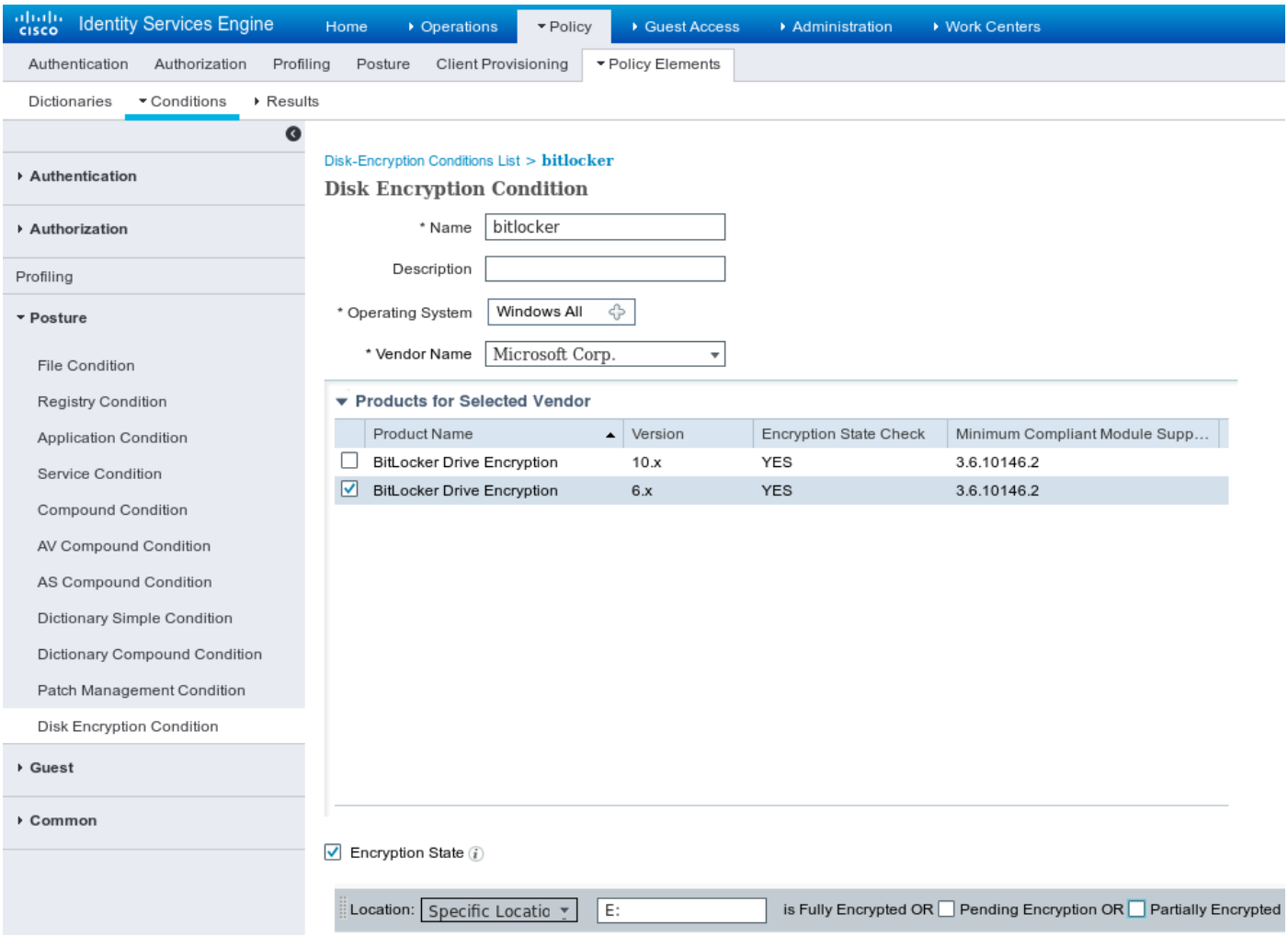
Navigieren Sie zu **Administration > Network Resources > Network Devices**, Add **ASA with Device Type = ASA (ASA mit Gerätetyp hinzufügen)**. Dies wird in den Autorisierungsregeln als Bedingung verwendet, ist jedoch nicht obligatorisch (andere Arten von Bedingungen können verwendet werden).

Gegebenenfalls existiert keine Netzwerkgerätegruppe. Navigieren Sie zum Erstellen zu **Administration > Network Resources > Network Device Groups (Administration > Netzwerkressourcen > Netzwerkgerätegruppen)**.

### Schritt 2: Statusbedingung und Richtlinien

Stellen Sie sicher, dass die Statusbedingungen aktualisiert werden: Navigieren Sie zu **Administration > System > Settings > Posture > Updates > Update Now**.

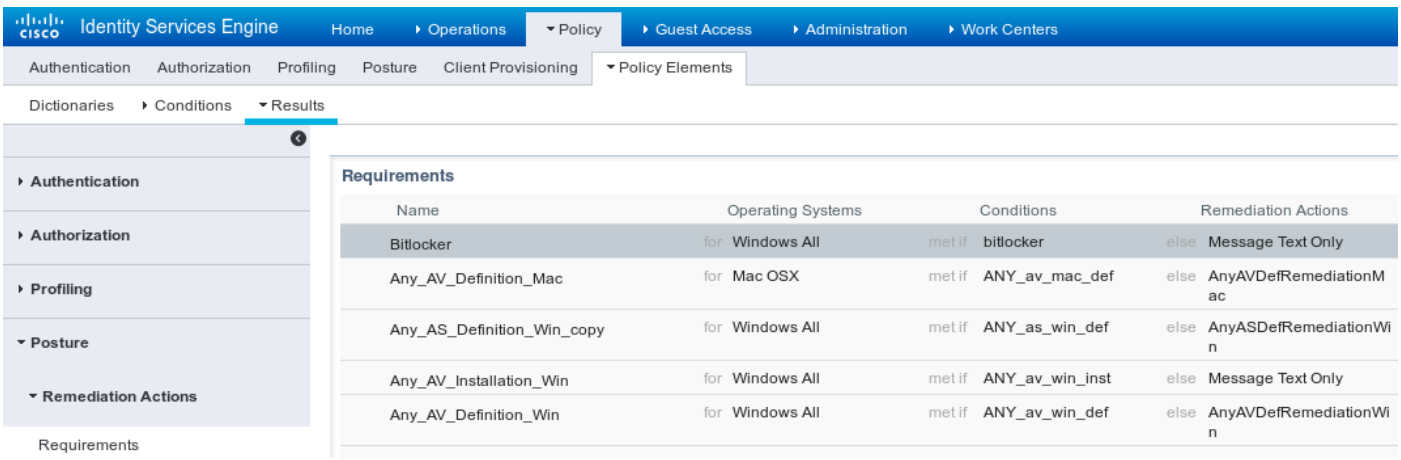
Navigieren Sie zu **Richtlinien > Richtlinienelemente > Bedingungen > Status > Festplattenverschlüsselungsbedingung**, und fügen Sie eine neue Bedingung hinzu, wie im Bild gezeigt.



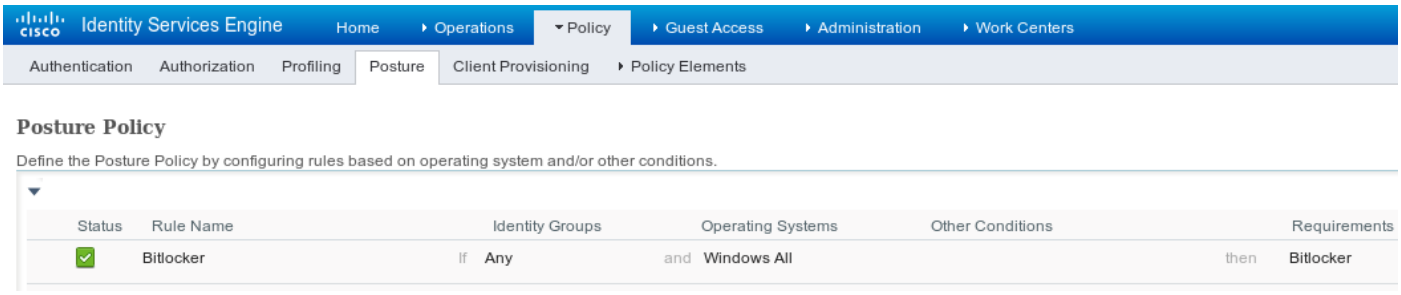

Diese Bedingung überprüft, ob BitLocker für Windows 7 installiert ist und ob **E:** Partition ist vollständig verschlüsselt.

> **Hinweis**: BitLocker ist eine Verschlüsselung auf Festplattenebene und unterstützt keine spezifische Location mit Pfadargument, sondern nur Laufwerkbuchstaben.

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Status > Anforderungen**, um eine neue Anforderung zu erstellen, die die im Bild dargestellte Bedingung verwendet.

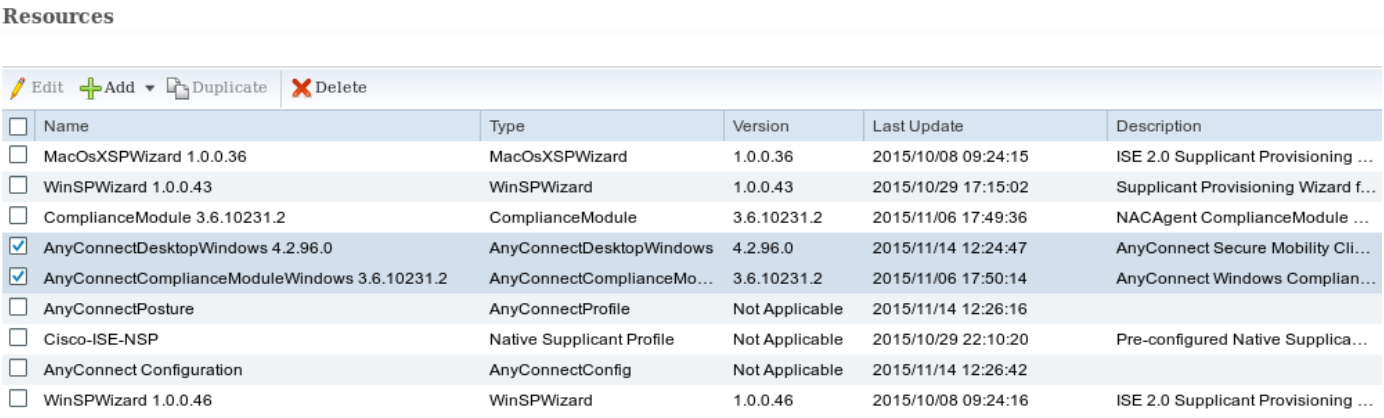


Navigieren Sie zu **Richtlinie > Status**, und fügen Sie eine Bedingung für alle Windows hinzu, um die Anforderung wie im Bild gezeigt zu verwenden.



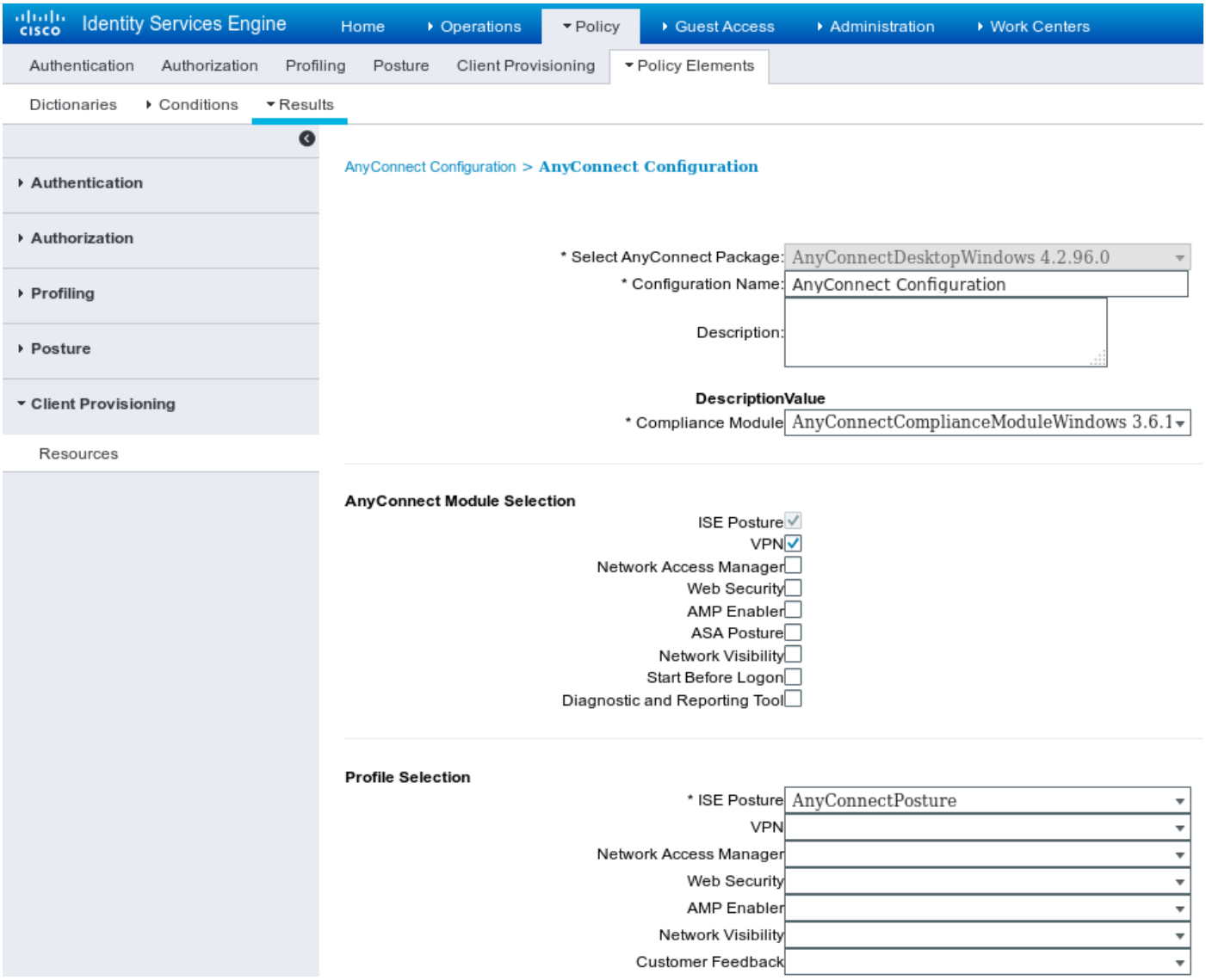

## Schritt 3: Ressourcen und Richtlinien für die Client-Bereitstellung

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Client Provisioning > Resources**, laden Sie das **Compliance Module** von Cisco.com herunter, und laden Sie das **AnyConnect 4.2-Paket manuell hoch,** wie im Bild gezeigt.

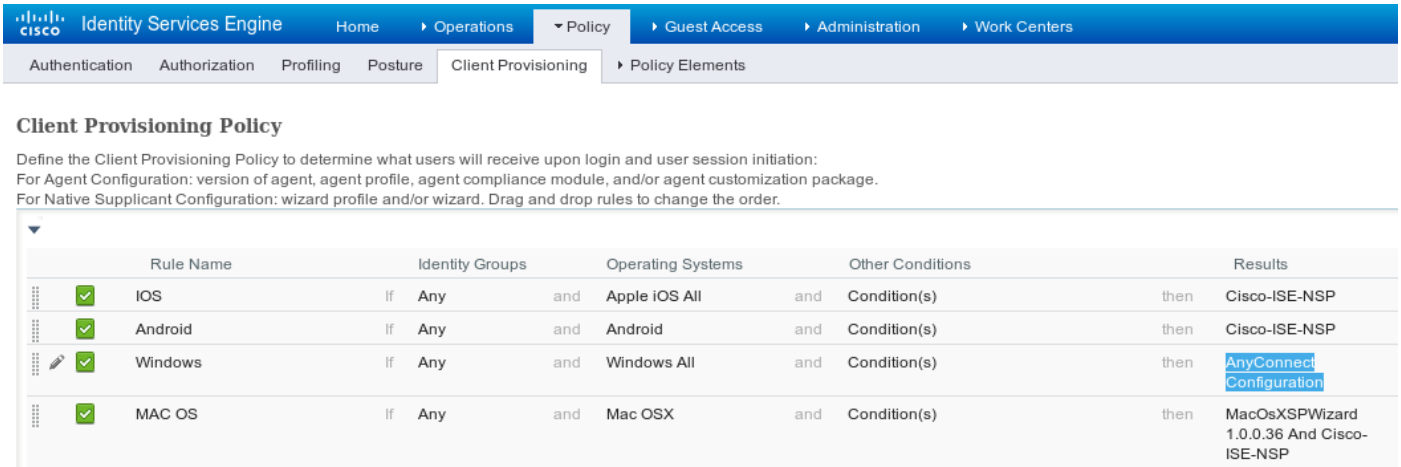



Navigieren Sie zu **Add > NAC Agent oder AnyConnect Posture Profile**, und erstellen Sie ein AnyConnect-Statusprofil (Name: **AnyConnectPosture**) mit Standardeinstellungen.

Navigieren Sie zu **Add > AnyConnect Configuration**, und fügen Sie das AnyConnect-Profil hinzu (Name: **AnyConnect-Konfiguration**), wie im Bild gezeigt.

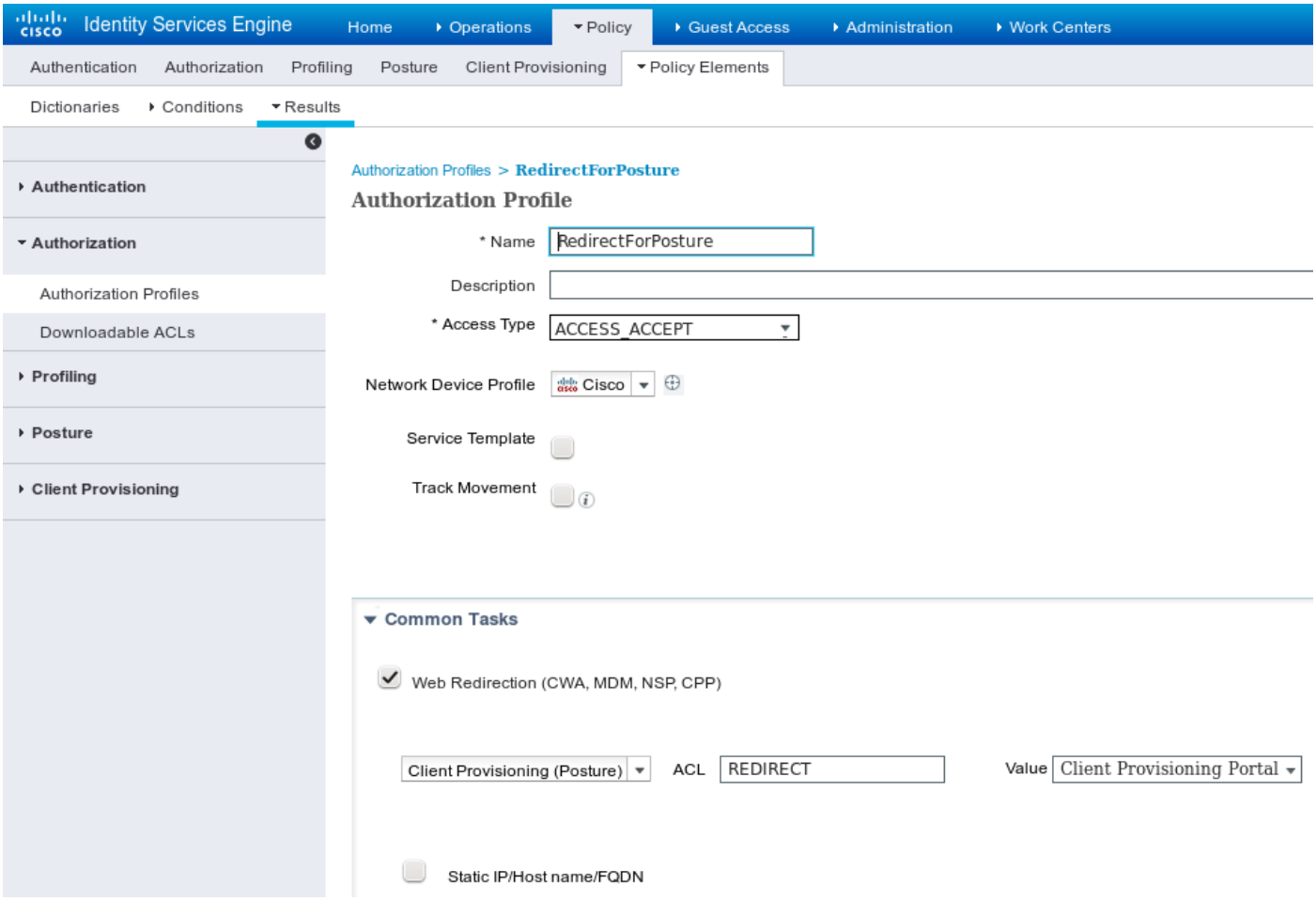



Navigieren Sie zu **Richtlinie > Client Provisioning**, und ändern Sie die Standardrichtlinie für Windows, um das konfigurierte AnyConnect-Profil zu verwenden, wie im Bild gezeigt.



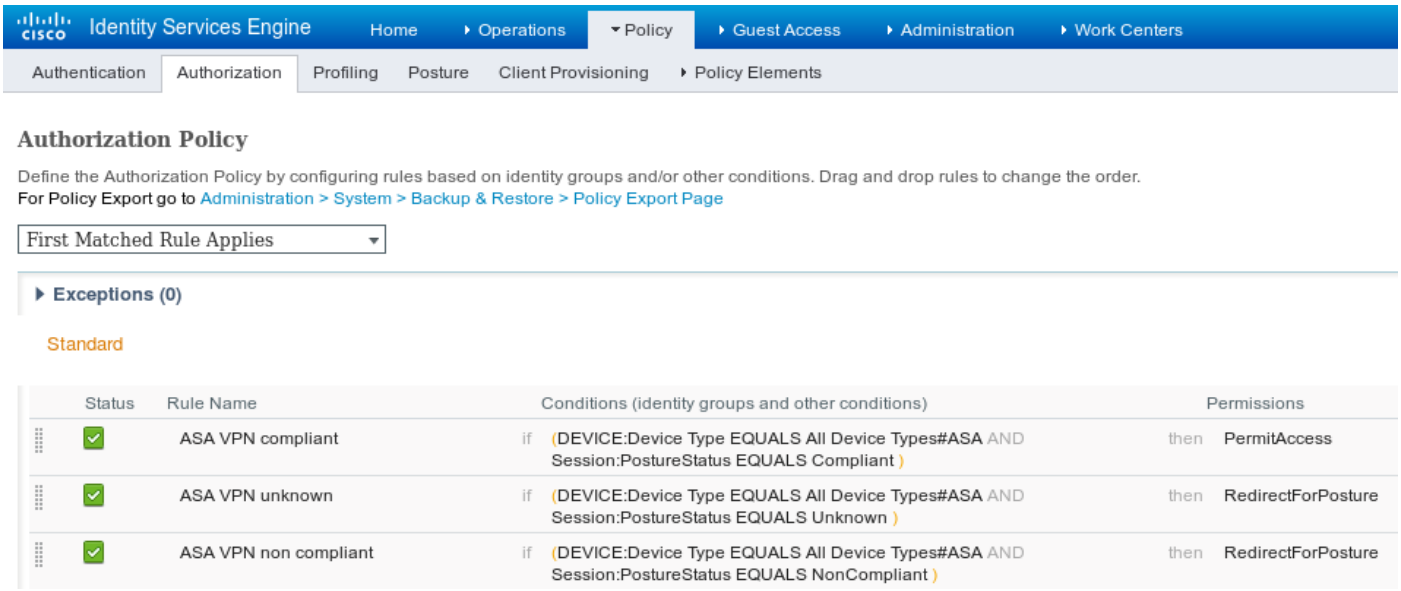

## Schritt 4: Autorisierungsregeln

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung**, und fügen Sie das Autorisierungsprofil hinzu (Name: **RedirectForPosture**), die zu einem Standard-Client-Bereitstellungsportal umleitet, wie im Bild gezeigt.




**REDIRECT** ACL ist auf ASA definiert.

Navigieren Sie zu **Richtlinien > Autorisierung**, und erstellen Sie 3 Autorisierungsregeln, wie im Bild gezeigt.



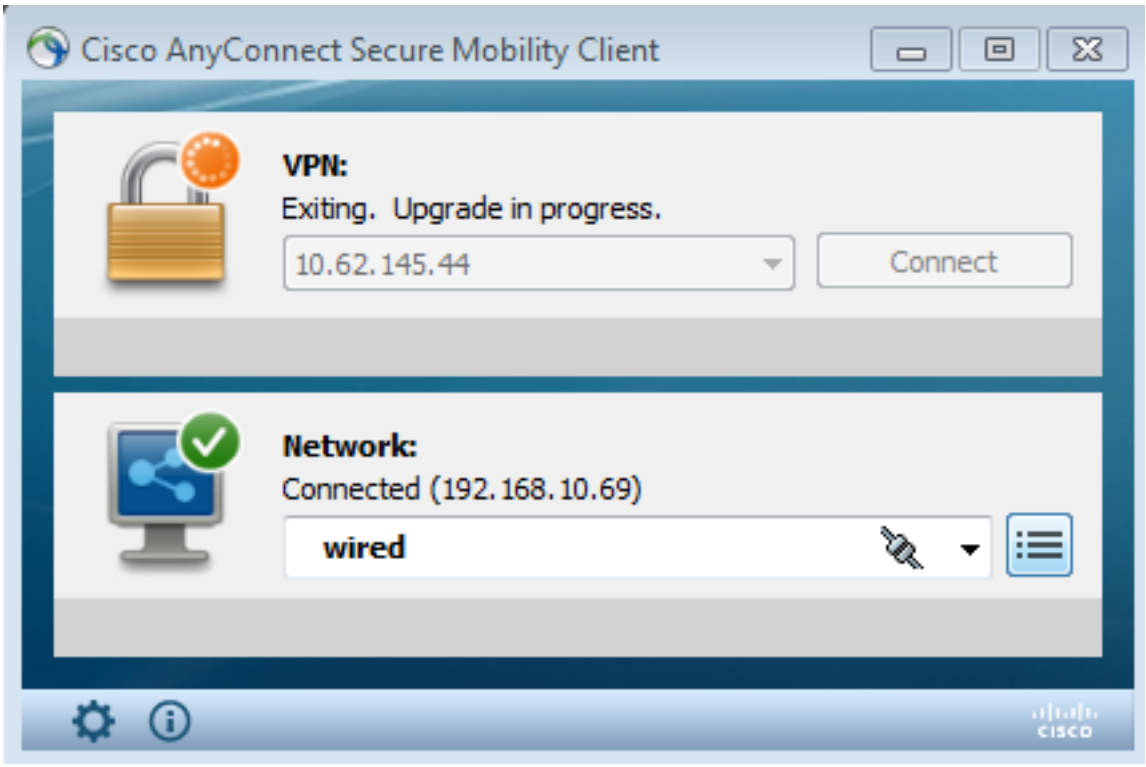

Wenn der Endpunkt den Vorgaben entspricht, wird umfassender Zugriff bereitgestellt. Wenn der Status unbekannt oder nicht konform ist, wird eine Umleitung für die Client-Bereitstellung zurückgegeben.

# Überprüfen

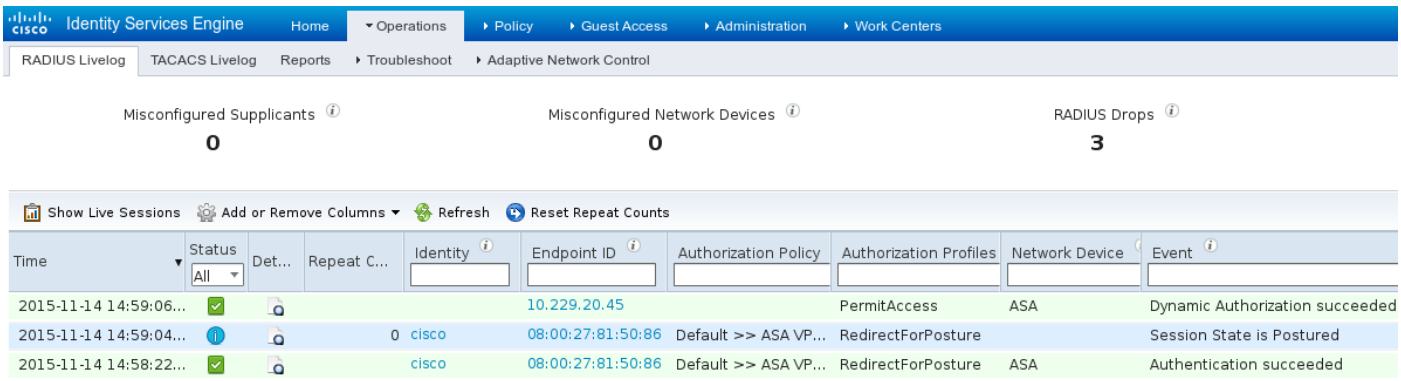
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

### Schritt 1: Einrichtung von VPN-Sitzungen

Nach Einrichtung der VPN-Sitzung möchte ASA möglicherweise ein Upgrade der AnyConnect-Module durchführen, wie im Bild gezeigt.




Auf der ISE wird die letzte Regel getroffen, sodass **RedirectForPosture**-Berechtigungen wie im Bild gezeigt zurückgegeben werden.



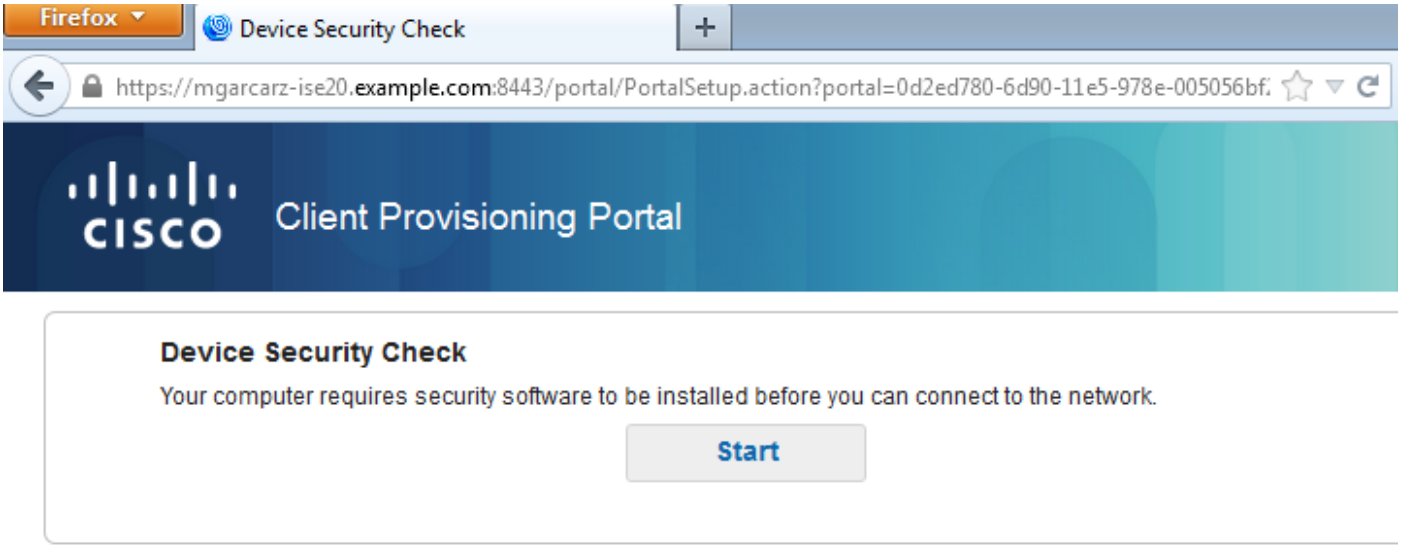

Nach Abschluss der VPN-Sitzung meldet die ASA, dass die Umleitung erfolgen muss:

```
ASAv# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 32
Assigned IP  : 172.16.31.10           Public IP    : 10.61.90.226
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
```

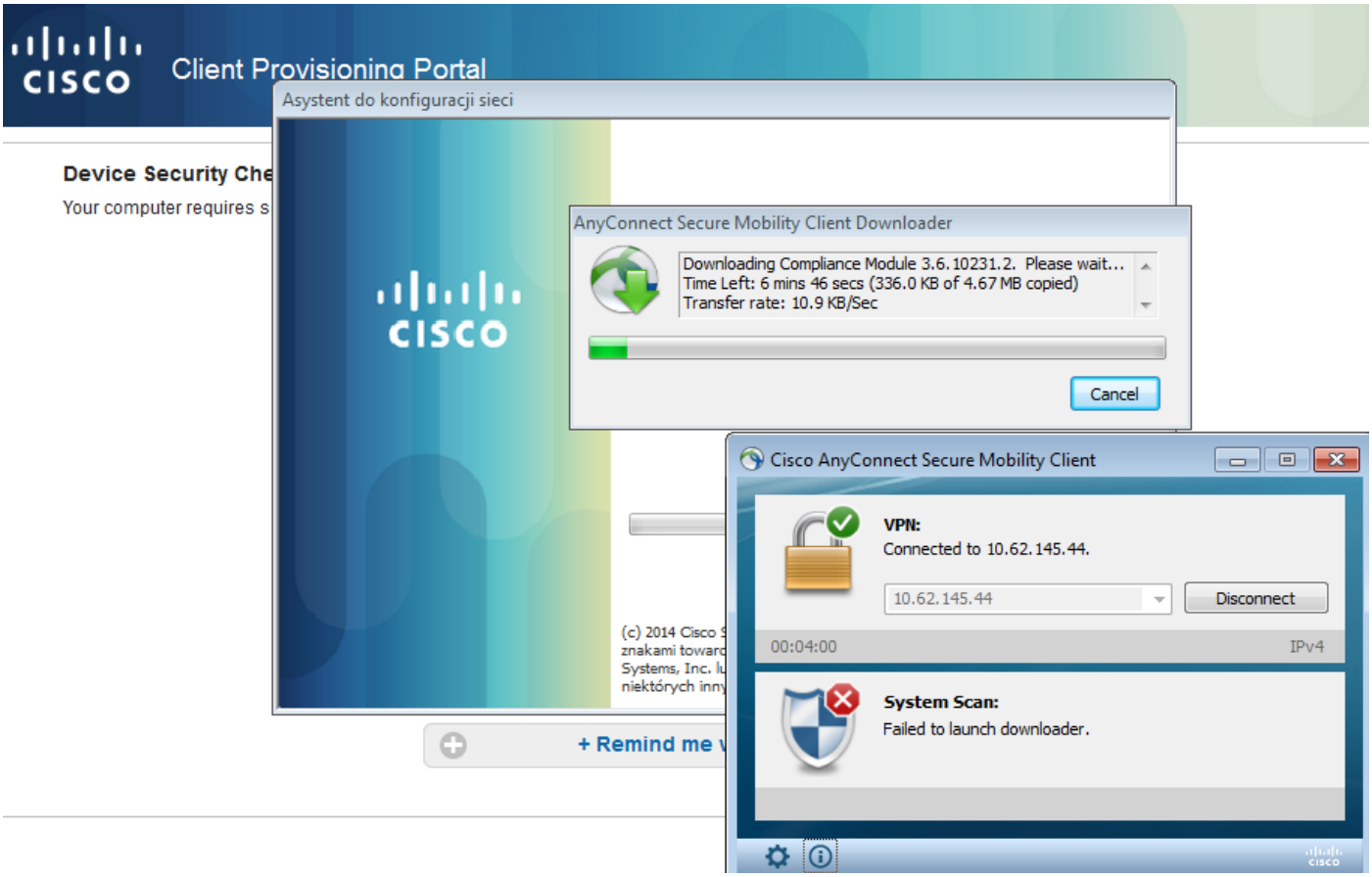
```
Bytes Tx     : 53201                  Bytes Rx     : 122712
Pkts Tx      : 134                    Pkts Rx      : 557
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : AllProtocols           Tunnel Group : TAC
Login Time   : 21:29:50 UTC Sat Nov 14 2015
Duration     : 0h:56m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801010002000056647a7ce
Security Grp : none

<some output omitted for clarity>

ISE Posture:
  Redirect URL : https://mgarcarz-
ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-00505...
  Redirect ACL : REDIRECT
```

### Schritt 2: Client-Bereitstellung

In diesem Stadium wird der Endpunkt-Webbrowser-Datenverkehr zur Client-Bereitstellung an die ISE umgeleitet, wie im Bild gezeigt.

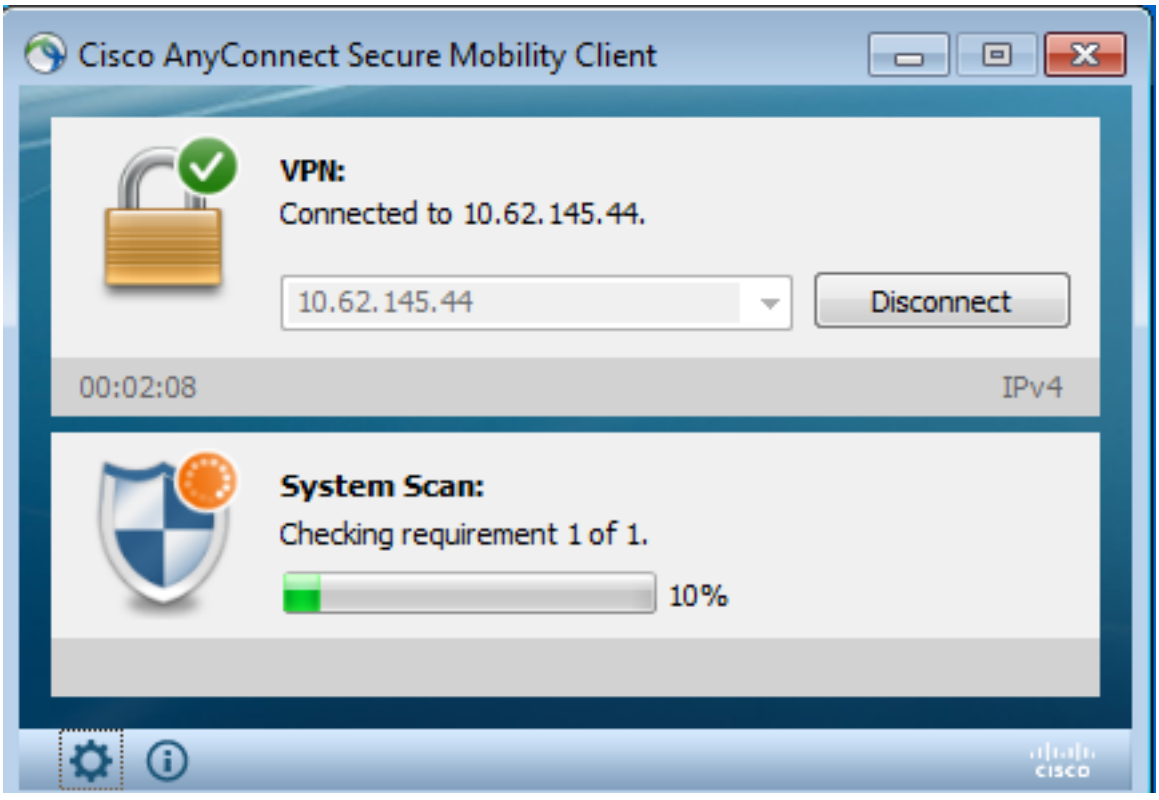



Bei Bedarf wird AnyConnect zusammen mit dem Status- und Compliance-Modul aktualisiert, wie im Bild gezeigt.



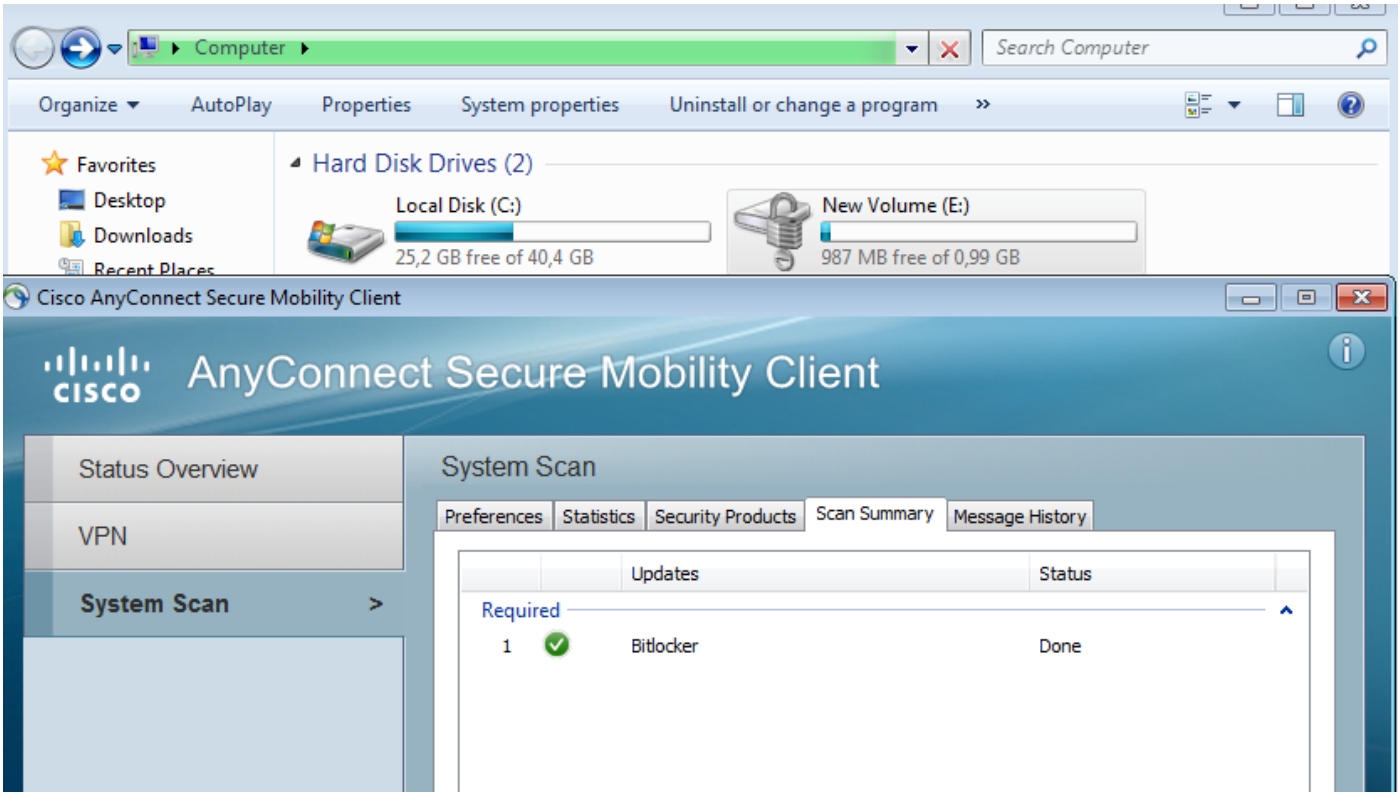

### Schritt 3: Statusprüfung und CoA

Statusmodul wird ausgeführt, ISE wird ermittelt (es kann erforderlich sein, dass DNS A-Eintrag für enroll.cisco.com vorhanden ist, um erfolgreich zu sein), und die Statusbedingungen werden wie im Bild gezeigt heruntergeladen und überprüft.

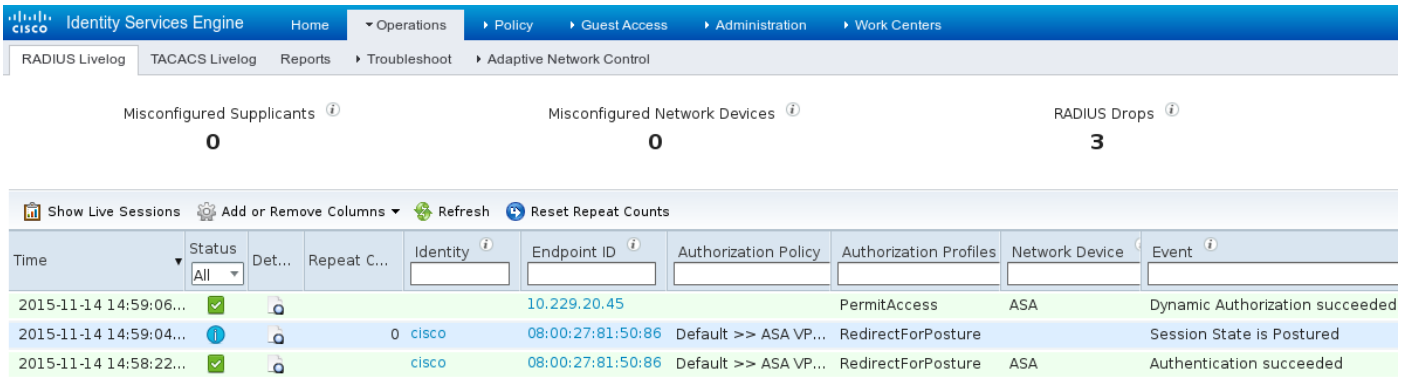



Sobald bestätigt ist, dass **E:** -Partition vollständig mit BitLocker verschlüsselt ist, wird der richtige

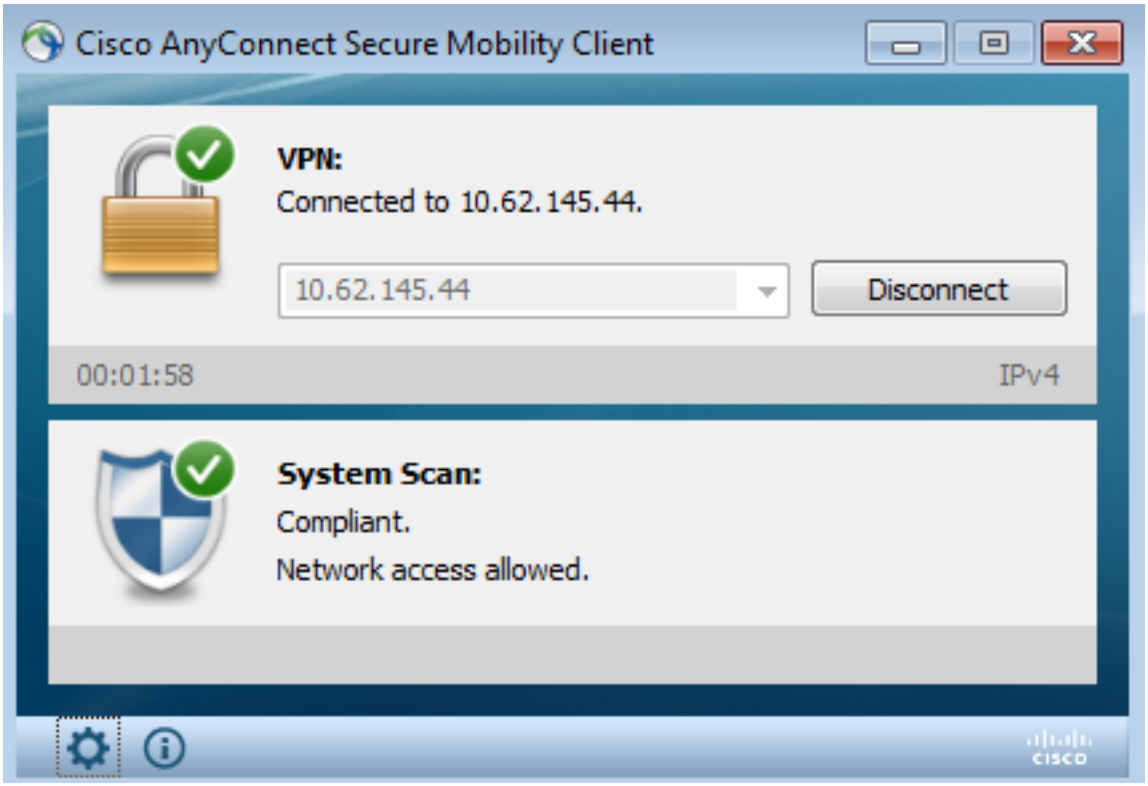
Bericht wie im Bild gezeigt an die ISE gesendet.



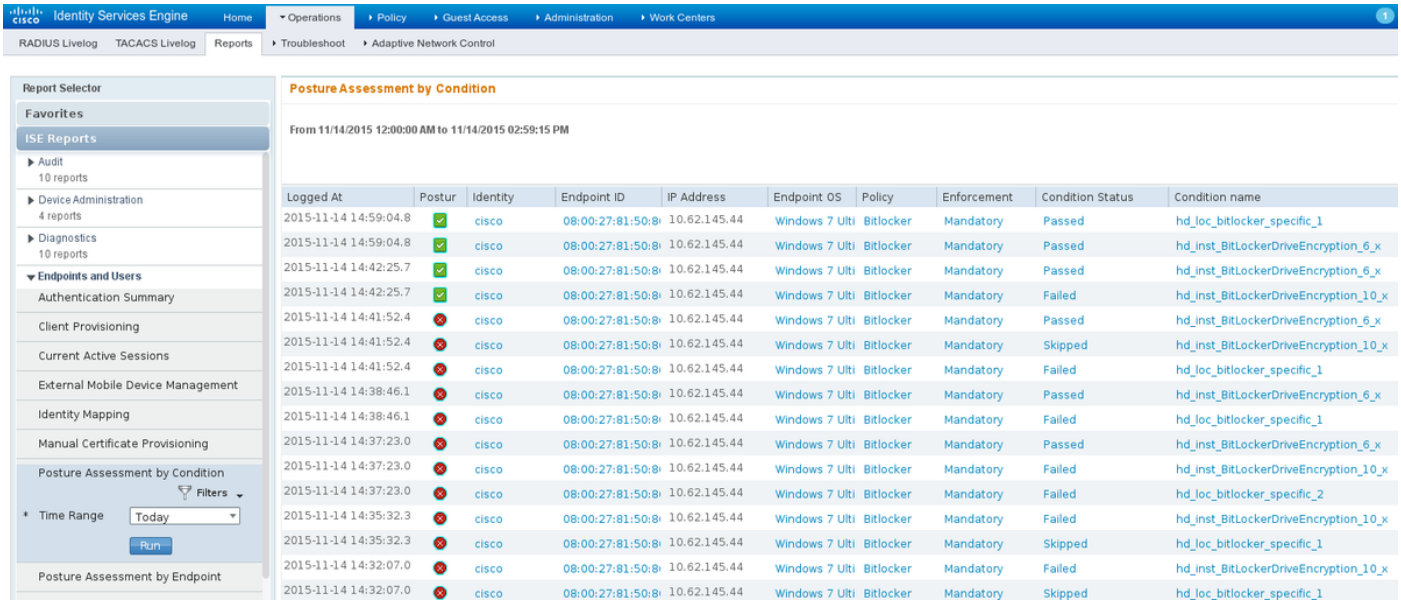

Dies veranlasst CoA zur erneuten Autorisierung der VPN-Sitzung, wie im Bild gezeigt.




ASA entfernt die Umleitungszugriffskontrollliste, die uneingeschränkten Zugriff bietet. AnyConnect meldet die Compliance, wie im Bild gezeigt.




Darüber hinaus können detaillierte Berichte zur ISE bestätigen, dass beide Bedingungen erfüllt sind (**Statusüberprüfung nach Bedingung** ist der neue ISE 2.0-Bericht, der alle Bedingungen anzeigt). Die erste Bedingung (**hd_inst_BitLockerDriveEncryption_6_x**) prüft die Installation/den Prozess, die zweite (**hd_loc_bitlocker_specific_1**) prüft, ob ein bestimmter Speicherort (E:), wie im Bild gezeigt, vollständig verschlüsselt ist.




Der Bericht ISE **Posture Assesment by Endpoint** bestätigt, dass alle Bedingungen erfüllt sind (siehe Bild).

## Posture More Detail Assessment

Time Range: From 11/14/2015 12:00:00 AM to 11/14/2015 11:42:08 PM
Generated At: 2015-11-14 23:42:08.257

### Client Details

| | |
|---|---|
| Username: | cisco |
| Mac Address: | 08:00:27:81:50:86 |
| IP address: | 10.62.145.44 |
| Session ID: | c0a8010100001700056473ebe |
| Client Operating System: | Windows 7 Ultimate 64-bit |
| Client NAC Agent: | AnyConnect Posture Agent for Windows 4.2.00096 |
| 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: | ADMIN-KOMPUTER |
| System Domain: | n/a |
| System User: | admin |
| User Domain: | admin-Komputer |
| AV Installed: | |
| AS Installed: | Windows Defender;6.1.7600.16385;1.141.3676.0;01/11/2013; |

### Posture Report

| | |
|---|---|
| Posture Status: | Compliant |
| Logged At: | 2015-11-14 14:59:04.827 |

Dasselbe kann von ise-psc.log Debug bestätigt werden. Statusanfrage bei ISE und Antwort:

```
2015-11-14 14:59:01,963 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::c0a8010100001700056473ebe:::- Received posture
request [parameters: reqtype=validate, userip=10.62.145.44, clientmac=08-00-27-81-50-86,
os=WINDOWS, osVerison=1.2.1.6.1.1, architecture=9, provider=Device Filter, state=, ops=1,
avpid=, avvname=Microsoft Corp.:!:::!:::!:, avpname=Windows Defender:!:::!:::!:,
avpversion=6.1.7600.16385:!:::!:::!:, avpfeature=AS:!:::!:::!:, userAgent=Mozilla/4.0 (compatible;
WINDOWS; 1.2.1.6.1.1; AnyConnect Posture Agent v.4.2.00096), session_id=c0a8010100001700056473ebe
2015-11-14 14:59:01,963 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8010100001700056473ebe:::- Creating a new
session info for mac 08-00-27-81-50-86
2015-11-14 14:59:01,963 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8010100001700056473ebe:::- Turning on
enryption for endpoint with mac 08-00-27-81-50-86 and os WINDOWS, osVersion=1.2.1.6.1.1
2015-11-14 14:59:01,974 DEBUG  [portal-http-service28][]
```

```
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco:c0a801010001700056473ebe:::- Agent criteria
for rule [Name=bitlocker, Description=, Operating Systems=[Windows All],
Vendor=com.cisco.cpm.posture.edf.AVASVendor@96b084e, Check Type=Installation, Allow older def
date=0, Days Allowed=Undefined, Product Name=[com.cisco.cpm.posture.edf.AVASProduct@44870fea]] -
  (  ( (hd_inst_BitLockerDriveEncryption_6_x) )  & (hd_loc_bitlocker_specific_1) )
```

Die Antwort auf die Schwachstellenanforderung (Bedingung + Problembehebung) ist im XML-Format:

```
2015-11-14 14:59:02,052 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
 <version>2</version>
 <encryption>0</encryption>
 <package>
   <id>10</id>




   <version/>




    <type>3</type>
   <optional>0</optional>
   <action>3</action>
   <check>
     <id>hd_loc_bitlocker_specific_1</id>
     <category>10</category>
     <type>1002</type>
     <param>180</param>









     <value_type>2</value_type>
   </check>
   <check>




     <category>10</category>
     <type>1001</type>
```

```
     <param>180</param>
     <operation>regex match</operation>
     <value>^6\..+$|^6$</value>
     <value_type>3</value_type>
   </check>
   <criteria>( (  ( (hd_inst_BitLockerDriveEncryption_6_x) )  &amp;
(hd_loc_bitlocker_specific_1) ) )</criteria>
 </package>
</cleanmachines>
```

Nachdem der verschlüsselte Bericht von der ISE empfangen wurde:

```
2015-11-14 14:59:04,816 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Decrypting
report
2015-11-14 14:59:04,817 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Decrypted
report [[
<report><version>1000</version><encryption>0</encryption><key></key><os_type>WINDOWS</os_type><o
sversion>1.2.1.6.1.1</osversion><build_number>7600</build_number><architecture>9</architecture><
user_name>[device-filter-AC]</user_name><agent>x.y.z.d-todo</agent><sys_name>ADMIN-
KOMPUTER</sys_name><sys_user>admin</sys_user><sys_domain>n/a</sys_domain><sys_user_domain>admin-
Komputer</sys_user_domain><av><av_vendor_name>Microsoft
Corp.</av_vendor_name><av_prod_name>Windows
Defender</av_prod_name><av_prod_version>6.1.7600.16385</av_prod_version><av_def_version>1.141.36
76.0</av_def_version><av_def_date>01/11/2013</av_def_date><av_prod_features>AS</av_prod_features
></av><package><id>10</id><status>1</status><check><chk_id>hd_loc_bitlocker_specific_1</chk_id>
```

```
</check><check><chk_id>hd_inst_BitLockerDriveEncryption_6_x</chk_id><chk_status>1></check></pack
age></report> ]]
```

Station ist als konform markiert und ISE sendet CoA:

```
2015-11-14 14:59:04,823 INFO   [portal-http-service28][]
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a801010001700056473ebe:::- Posture state is
compliant for endpoint with mac 08-00-27-81-50-86
2015-11-14 14:59:06,825 DEBUG  [pool-5399-thread-1][] cisco.cpm.posture.runtime.PostureCoA -
:cisco:c0a801010000f0005647358b:::- Posture CoA is triggered for endpoint [08-00-27-81-50-86]
with session [c0a801010001700056473ebe
```

Die endgültige Konfiguration wird außerdem von der ISE gesendet:

```
2015-11-14 14:59:04,827 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Sending
response to endpoint 08-00-27-81-50-86 http response [[ <!--X-Perfigo-DM-Error=0--><!--error=0--
><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--><!--X-Perfigo-Auto-Close-Login-
Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--><!--user role=--><!--X-Perfigo-OrigRole=--
><!--X-Perfigo-UserKey=dummykey--><!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-
Perfigo-Session=--><!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter--><!--X-
Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4--><!--X-Perfigo-DHCP-Renew-Delay=1--
><!--X-Perfigo-Client-MAC=08:00:27:81:50:86--> ]]
```

Diese Schritte können auch vom Client aus bestätigt werden (AnyConnect DART):

```
Date         : 11/14/2015
Time         : 14:58:41
Type         : Warning
Source       : acvpnui

Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344
No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[Scanning system ... ]
```

```
****************************************

Date         : 11/14/2015
Time         : 14:58:43
Type         : Warning
Source       : acvpnui

Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344
No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[Checking requirement 1 of 1. ]

****************************************

Date         : 11/14/2015
Time         : 14:58:46
Type         : Warning
Source       : acvpnui

Description : Function: CNacApiShim::PostureNotification
File: .\NacShim.cpp
Line: 461
Clearing Posture List.
```

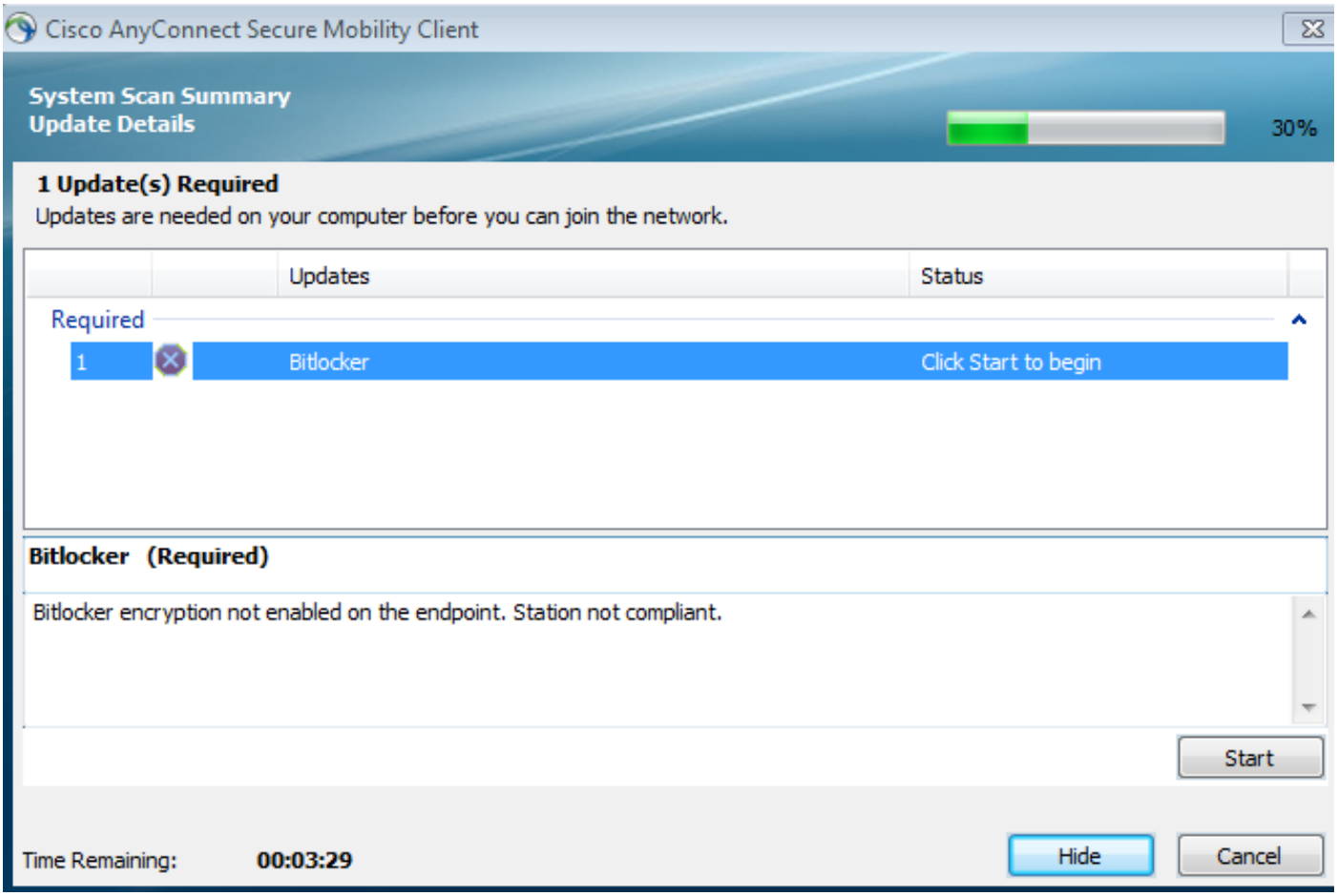
Für eine erfolgreiche Sitzung meldet AnyConnect UI System Scan / Message History:

```
     14:41:59    Searching for policy server.
    14:42:03    Checking for product updates...
    14:42:03    The AnyConnect Downloader is performing update checks...
    14:42:04    Checking for profile updates...
    14:42:04    Checking for product updates...
    14:42:04    Checking for customization updates...
    14:42:04    Performing any required updates...
    14:42:04    The AnyConnect Downloader updates have been completed.
    14:42:03    Update complete.
    14:42:03    Scanning system ...
    14:42:05    Checking requirement 1 of 1.
    14:42:05    Updating network settings.
    14:42:10    Compliant.
```

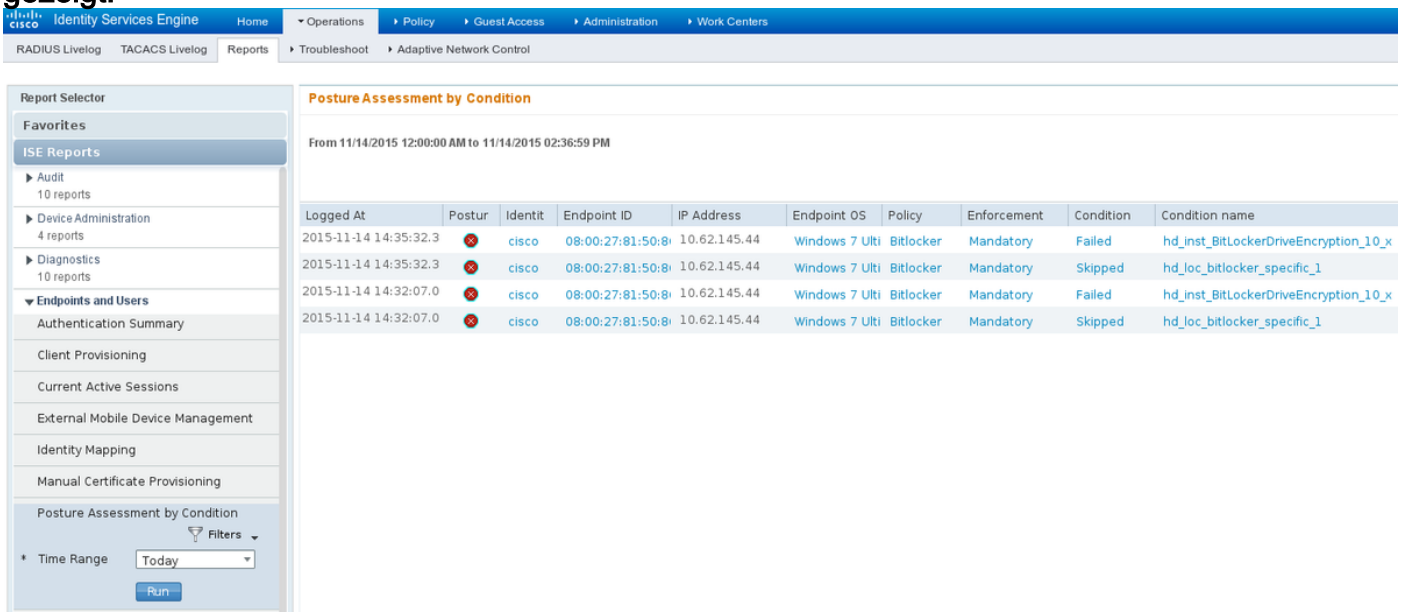
## BugCSCux15941 - ISE 2.0- und AC4.2-Posture-Bitlocker-Verschlüsselung mit fehlgeschlagener Location (char \ / nicht unterstützt)

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.Wenn der Endpunkt nicht den Vorgaben entspricht, wird er von der AnyConnect-Benutzeroberfläche gemeldet (ebenfalls konfigurierte Problembehebung wird ausgeführt), wie im Bild
gezeigt.




Die ISE kann Details zu den fehlerhaften Bedingungen bereitstellen, wie im Bild gezeigt.




Dasselbe kann über die CLI-Protokolle überprüft werden (Beispiele der Protokolle im Abschnitt Überprüfen).

## Zugehörige Informationen

- 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