配置ISE 2.1和AnyConnect 4.3狀態USB檢查

目錄

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)，使其僅在USB大容量儲存裝置斷開連線時提供網路的完全訪問。

必要條件

需求

思科建議您瞭解以下主題：

- 自適應安全裝置(ASA)CLI配置和安全套接字層(SSL)VPN配置的基本知識
- ASA上遠端訪問VPN配置的基本知識
- ISE和狀態服務基礎知識

採用元件

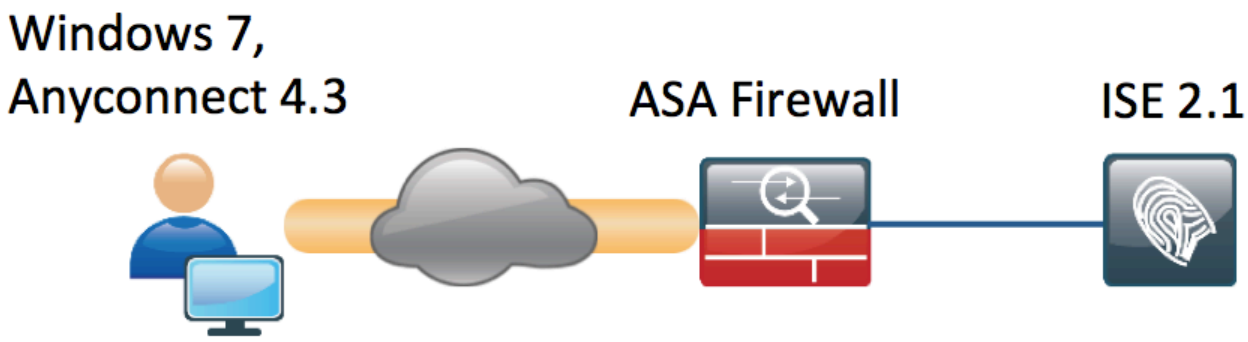
思科身份服務引擎(ISE)版本2.1和AnyConnect安全移動客戶端4.3支援USB大容量儲存檢查和補救。本檔案中的資訊是根據以下軟體版本：

- Cisco ASA軟體版本9.2(4)及更高版本

- 搭載Cisco AnyConnect安全移動客戶端版本4.3及更高版本的Microsoft Windows版本7
- Cisco ISE 2.1版及更高版本

設定

網路圖表



流程如下：

- 使用者尚未連線到VPN，私有USB大容量儲存裝置已插入，且內容可供使用者使用
- 由AnyConnect客戶端發起的VPN會話通過ISE進行身份驗證。終端的狀態未知，規則「Posture_Unknown」被命中，因此會話將重定向到ISE
- USB檢查在AC ISE狀態中引入了一類新的檢查，即只要終端仍位於同一個ISE控制的網路，它們就會持續監控該終端。唯一可用的邏輯補救操作是阻止由其驅動器號標識的USB裝置
- 更新ASA上的VPN會話，刪除重定向ACL並授予完全訪問許可權

VPN會話就是一個例子。狀態功能對於其他型別的訪問也工作正常。

ASA

ASA配置為使用ISE作為AAA伺服器進行遠端SSL VPN訪問。需要設定Radius CoA以及重新導向ACL:

```
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
```

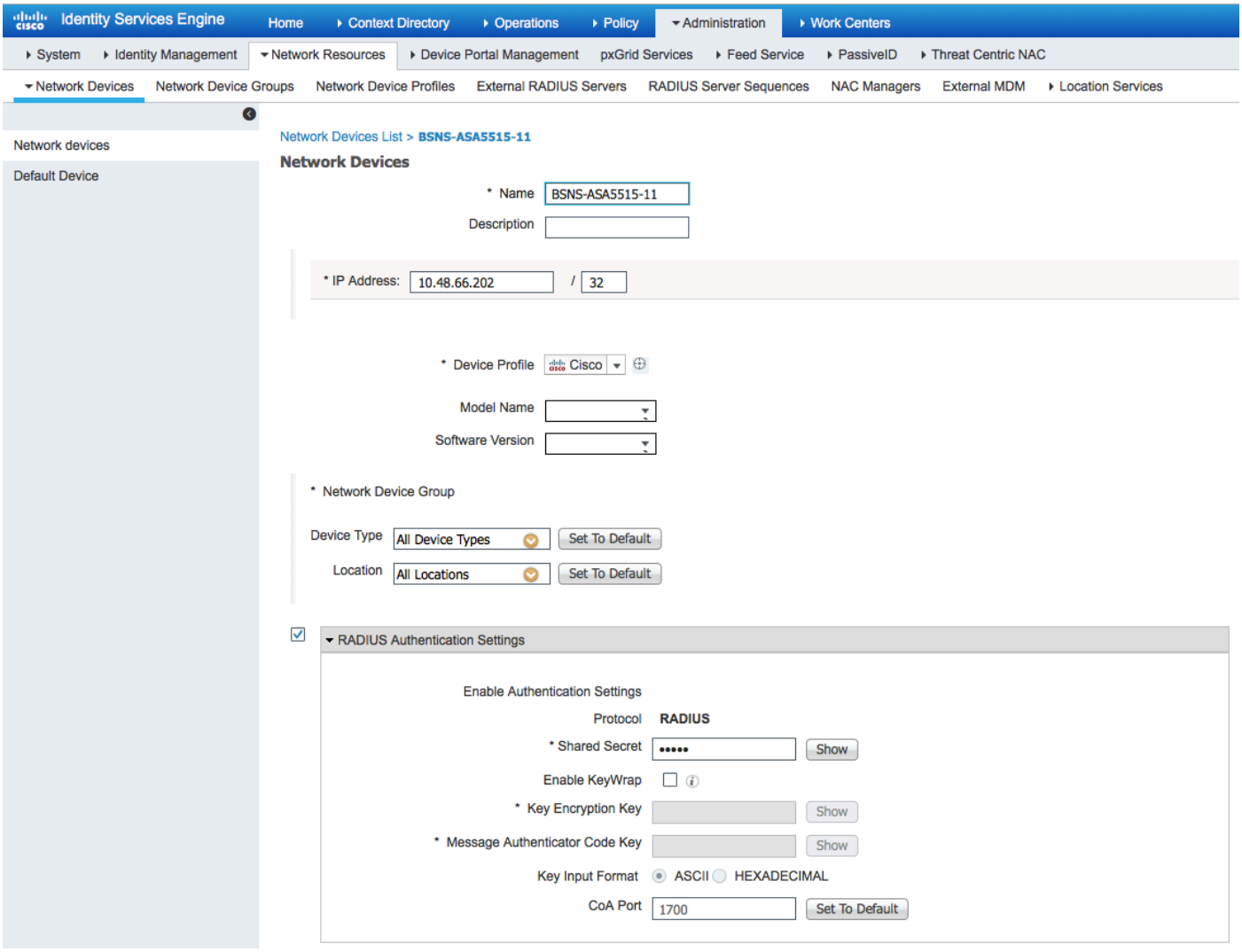
有關詳細資訊，請參閱：

[AnyConnect 4.0與ISE 1.3版整合配置示例]

ISE

步驟1.配置網路裝置

從**Administration > Network Resources > Network Devices >** add ASA。

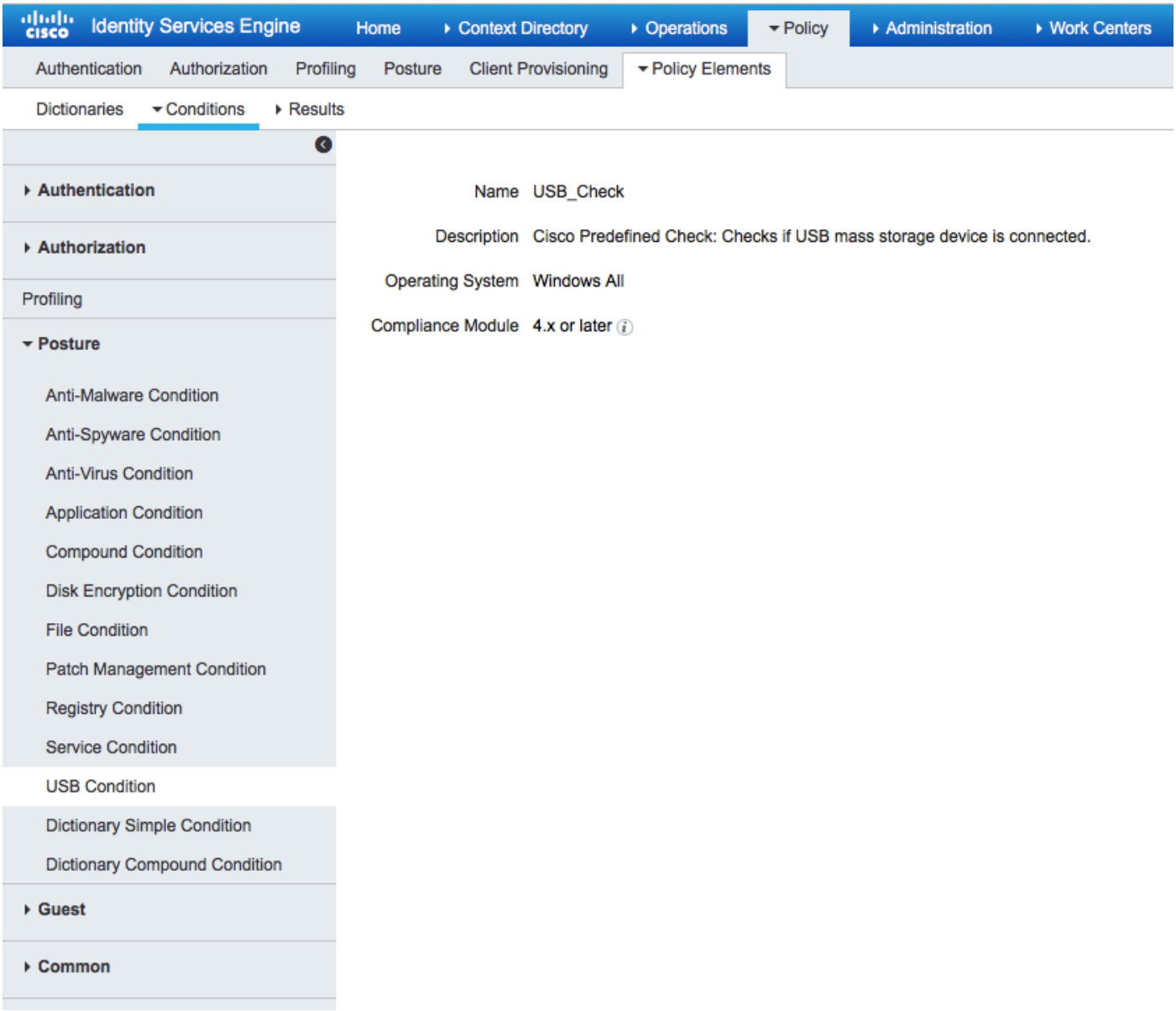


步驟2.配置狀態條件和策略

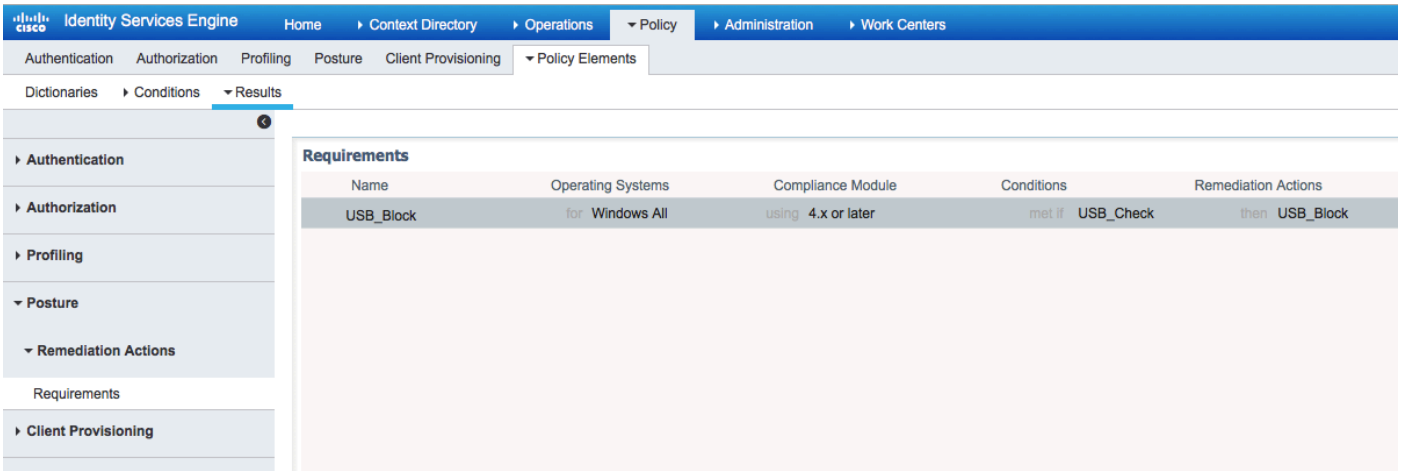
確保狀態條件已更新：**Administration > System > Settings > Posture > Updates > Update now選項**。

ISE 2.1附帶預配置的USB條件，用於檢查USB海量儲存裝置是否已連線。

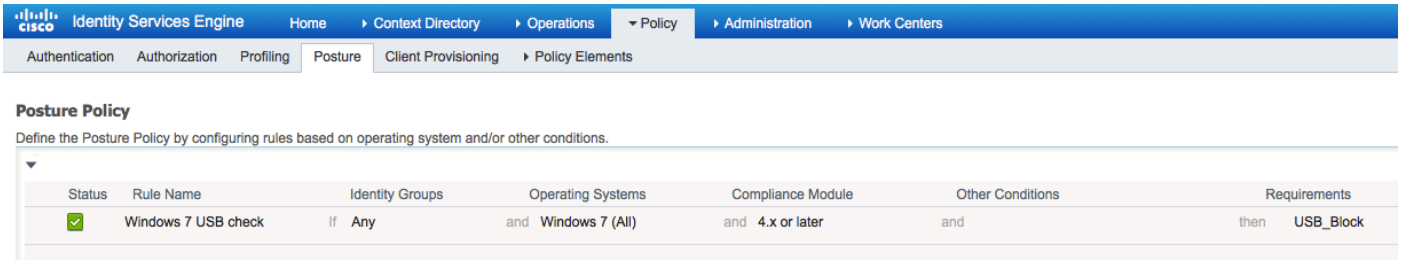
在**Policy > Policy Elements > Conditions > Posture > USB Condition** 中驗證現有條件：



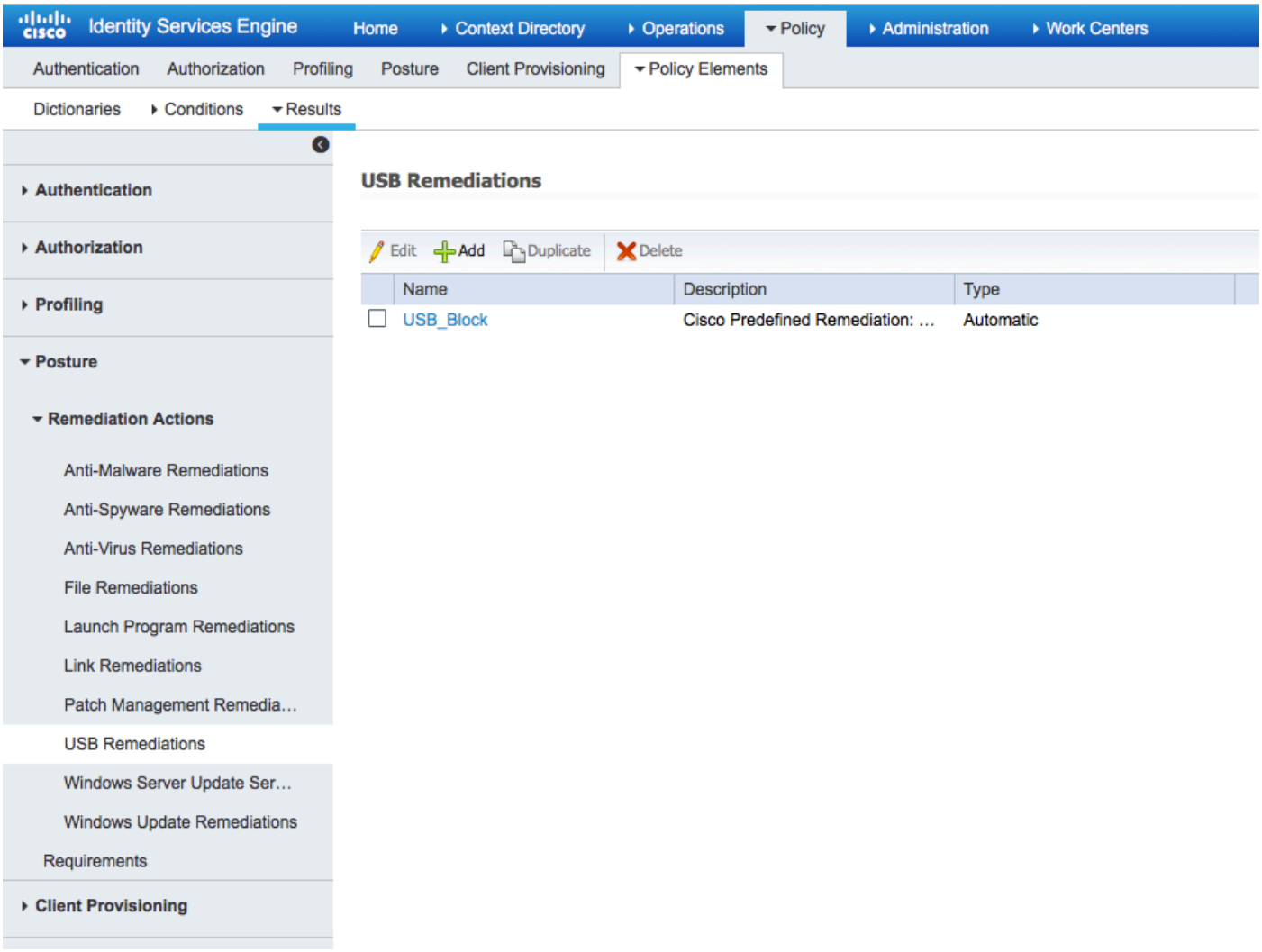
在**Policy > Policy Elements > Results > Posture > Requirements**中，驗證使用該條件的預配置要求。



在**Policy > Posture**中，為所有Windows新增一個條件以使用該要求：

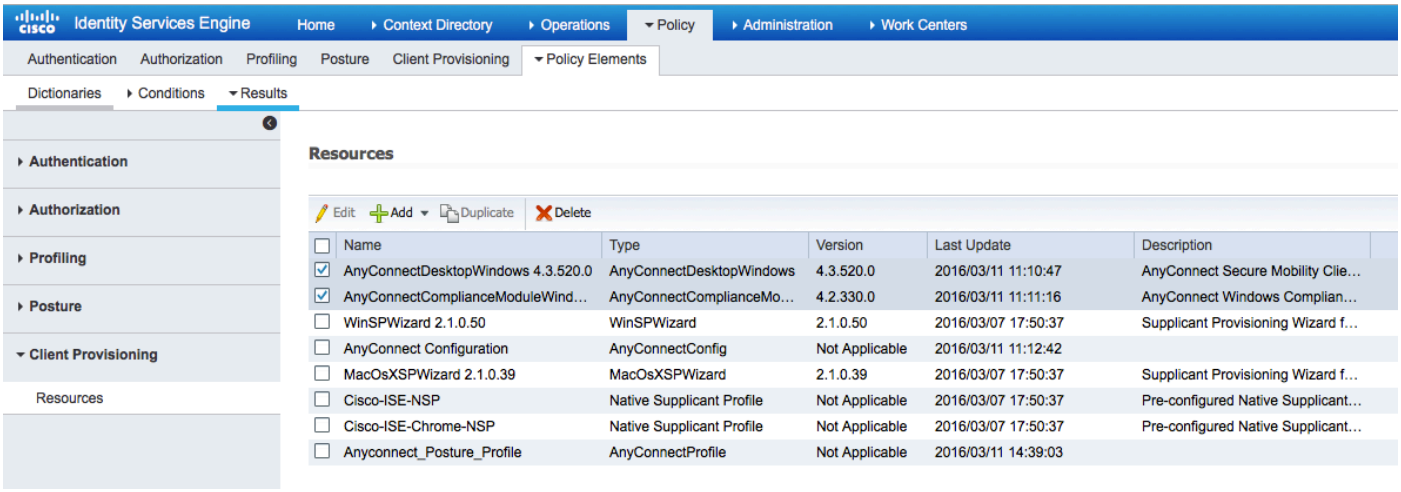


在Policy > Policy Elements > Results > Posture > Remediation Actions > USB Remediations中，驗證預配置的補救操作以阻止USB儲存裝置：



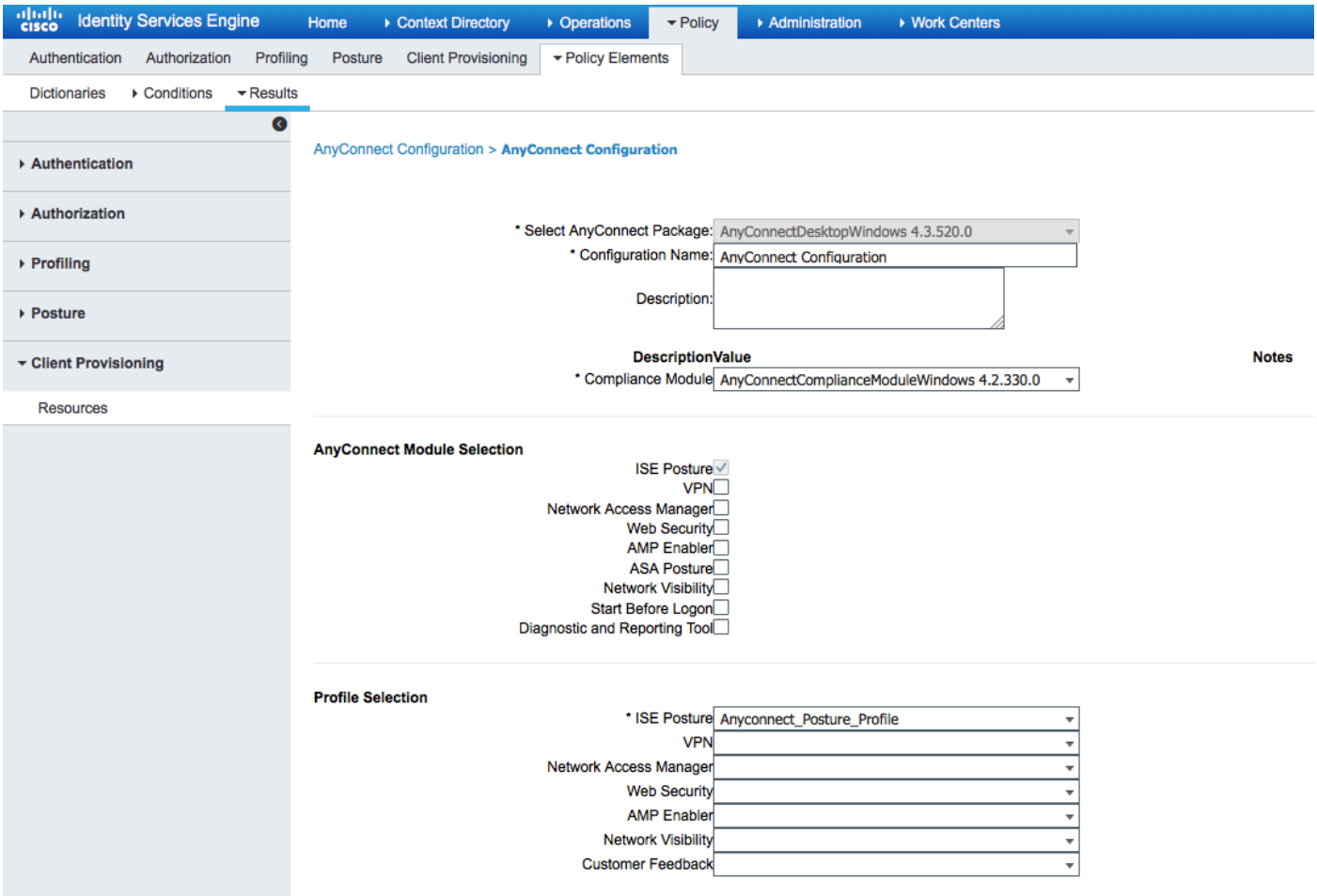
步驟3.配置客戶端調配資源和策略

在Policy > Policy Elements > Client Provisioning > Resources中，從Cisco.com下載合規性模組並手動上傳AnyConnect 4.3軟體包：

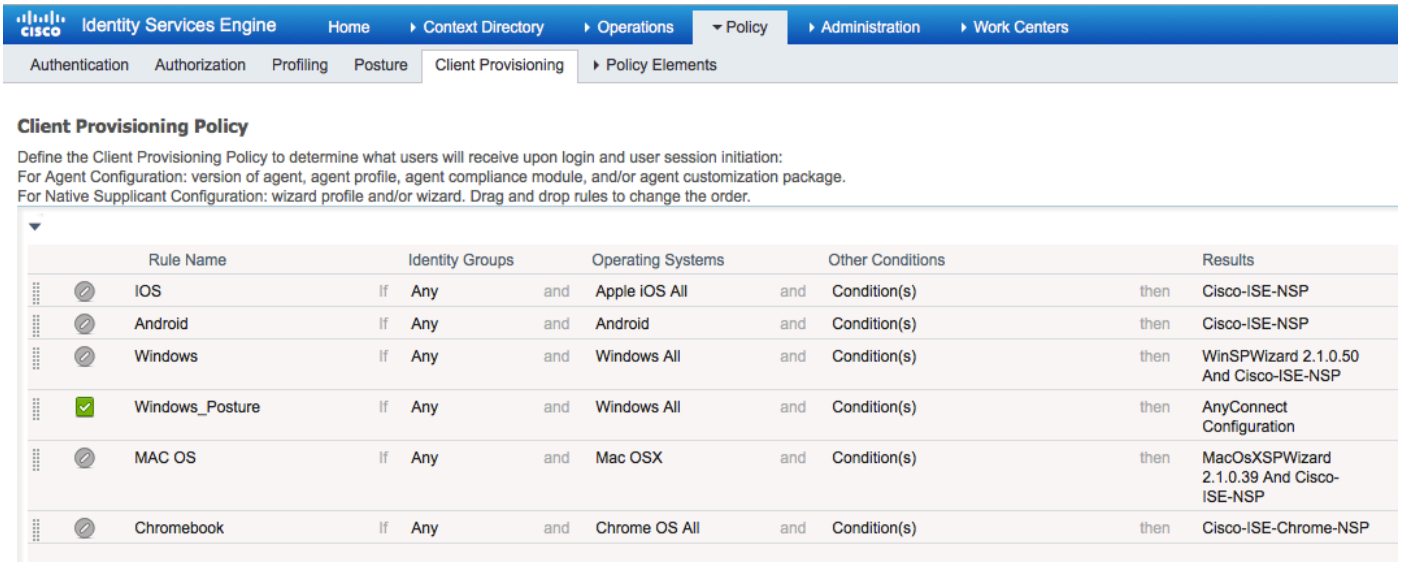


使用**Add > NAC Agent或AnyConnect Posture Profile**建立AnyConnect Posture配置檔案(名稱：*Anyconnect_Posture_Profile*)。

使用**Add > AnyConnect Configuration**新增AnyConnect配置(名稱：AnyConnect配置):

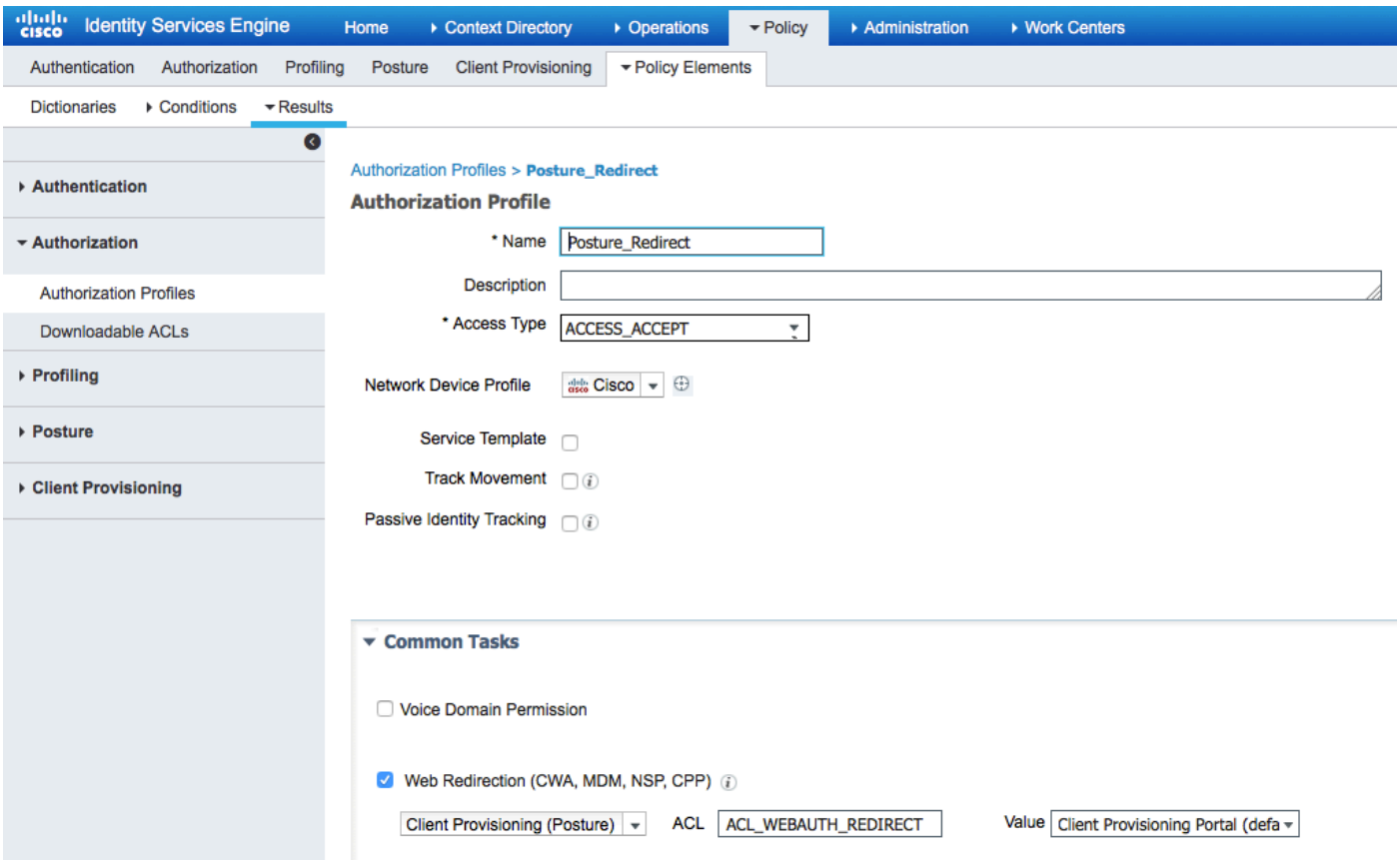


在**Policy > Client Provisioning**中，為Windows建立一個新策略(Windows_Posture)以使用AnyConnect配置：



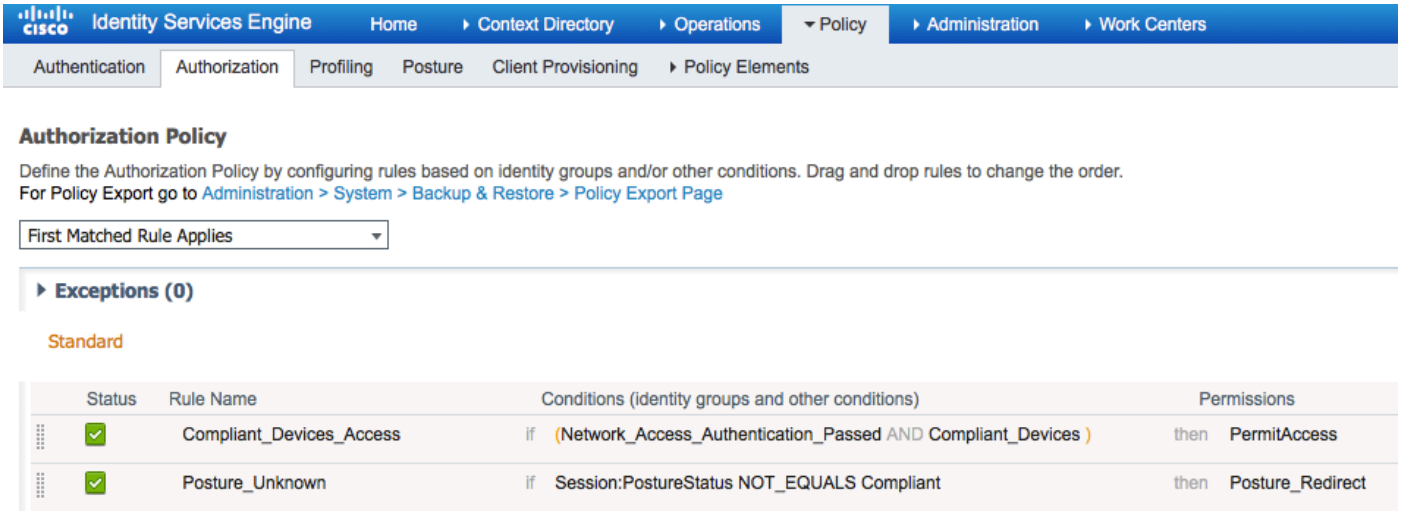
步驟4.配置授權規則

在**Policy > Policy Elements > Results > Authorization**中新增授權配置檔案(名稱：Posture_Redirect)，重定向到預設客戶端調配門戶：



附註：ACL_WEBAUTH_REDIRECT ACL是在ASA上定義的。

從**Policy > Authorization**為重定向建立授權規則。在ISE上預配置合規裝置的授權規則：

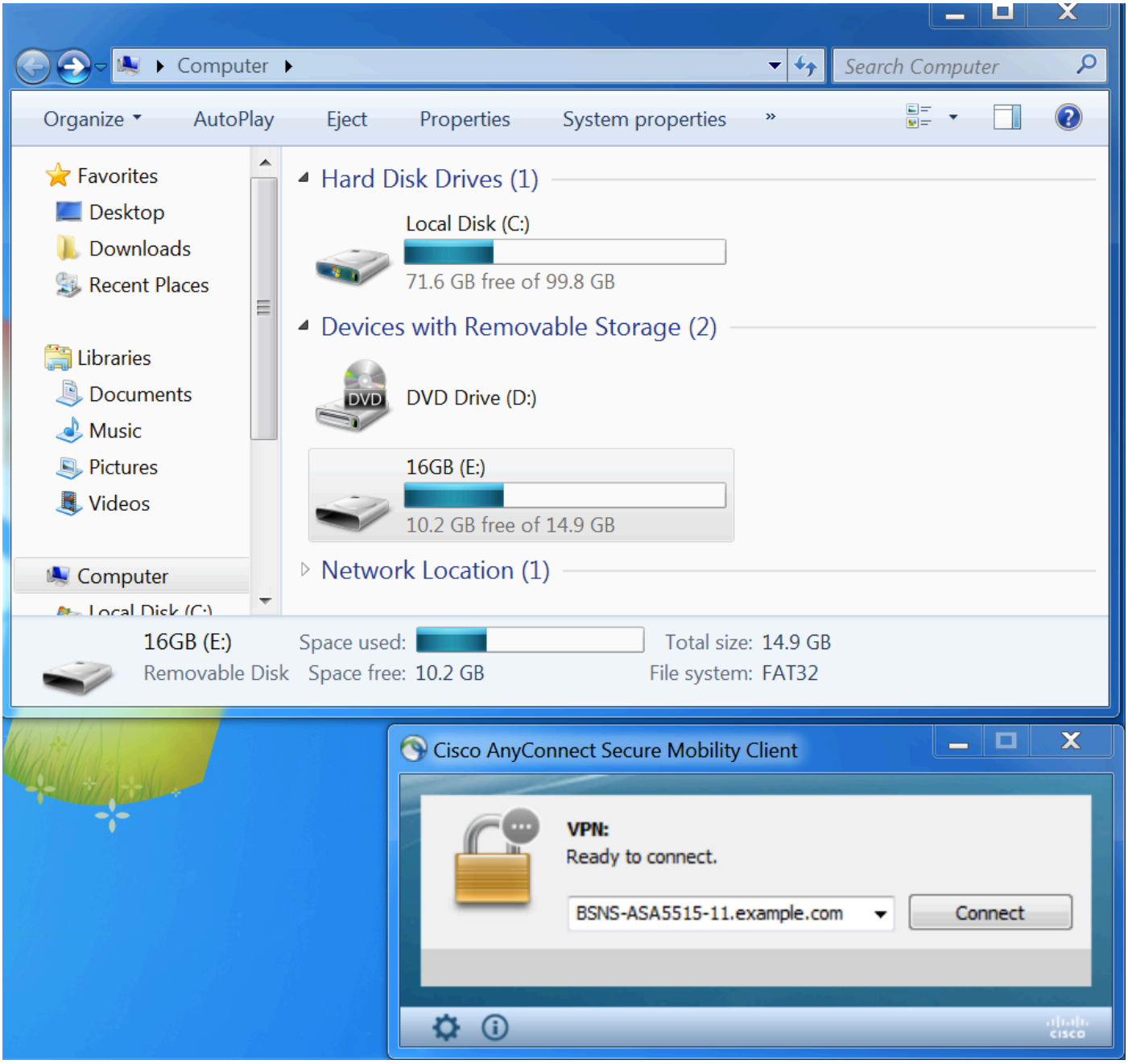


如果終端符合要求，則提供完全訪問。如果狀態未知或不相容，將返回客戶端預配的重定向。

驗證

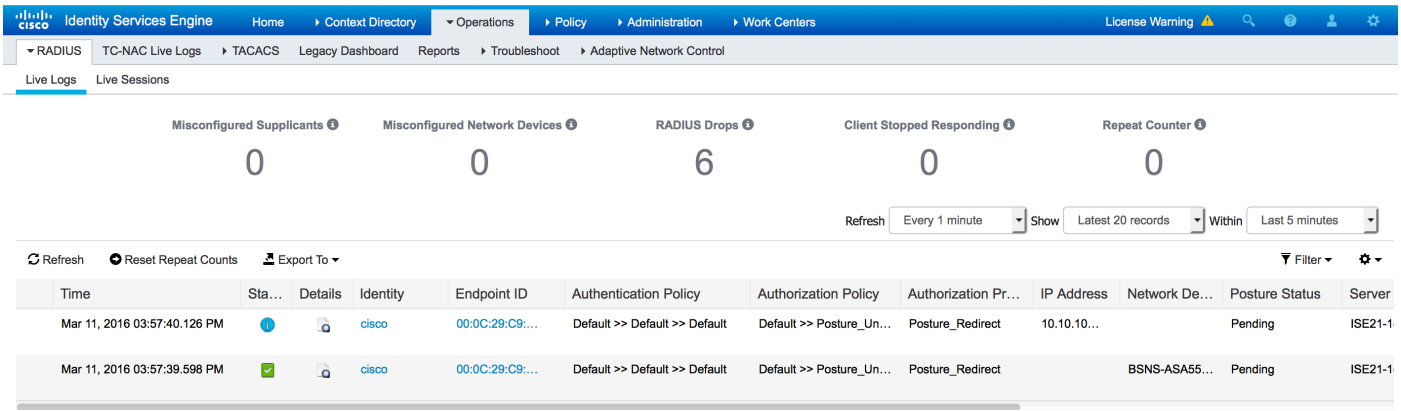
建立VPN會話之前

已插入USB裝置，其內容可供使用者使用。



VPN會話建立

在身份驗證期間，ISE將返回重定向訪問清單和重定向url，作為Posture_Redirect授權配置檔案的一部分



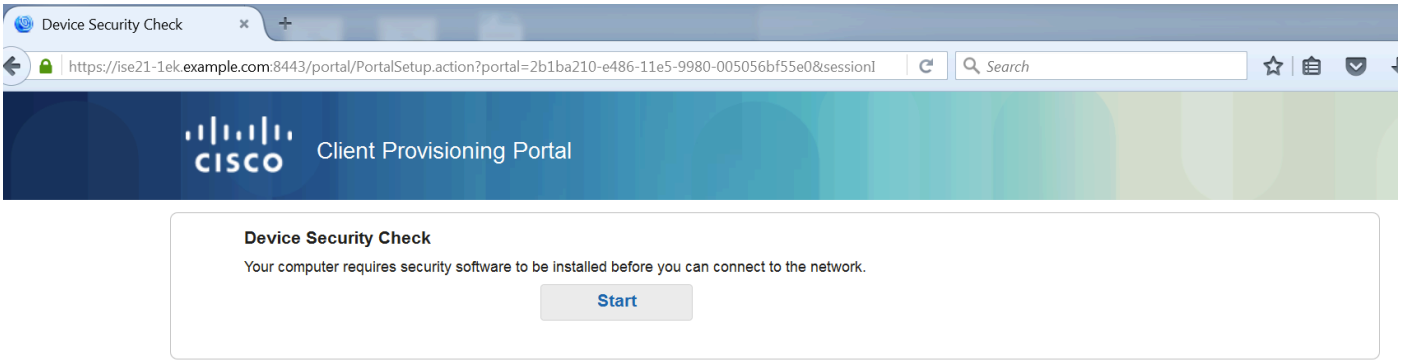
建立VPN會話後，來自客戶端的ASA流量將根據重定向訪問清單進行重定向：

```
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
```

客戶端調配

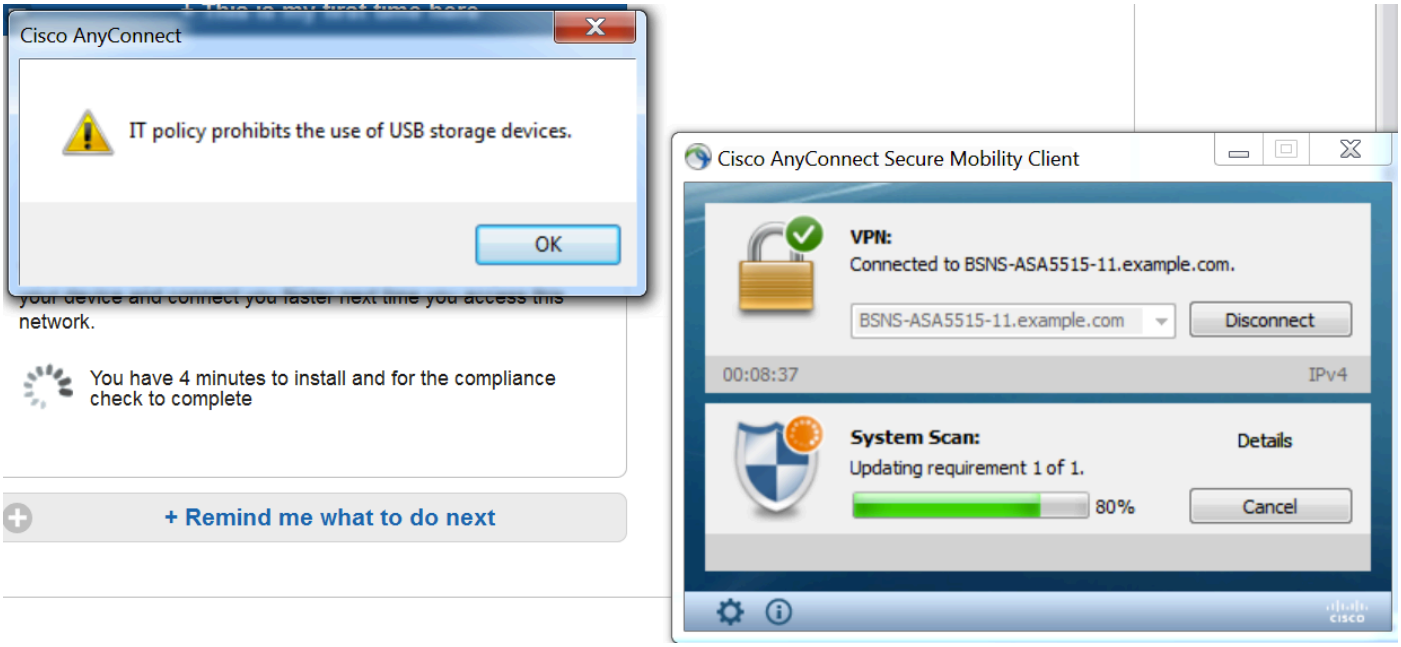
在此階段，終端Web瀏覽器流量重定向到ISE進行客戶端調配：



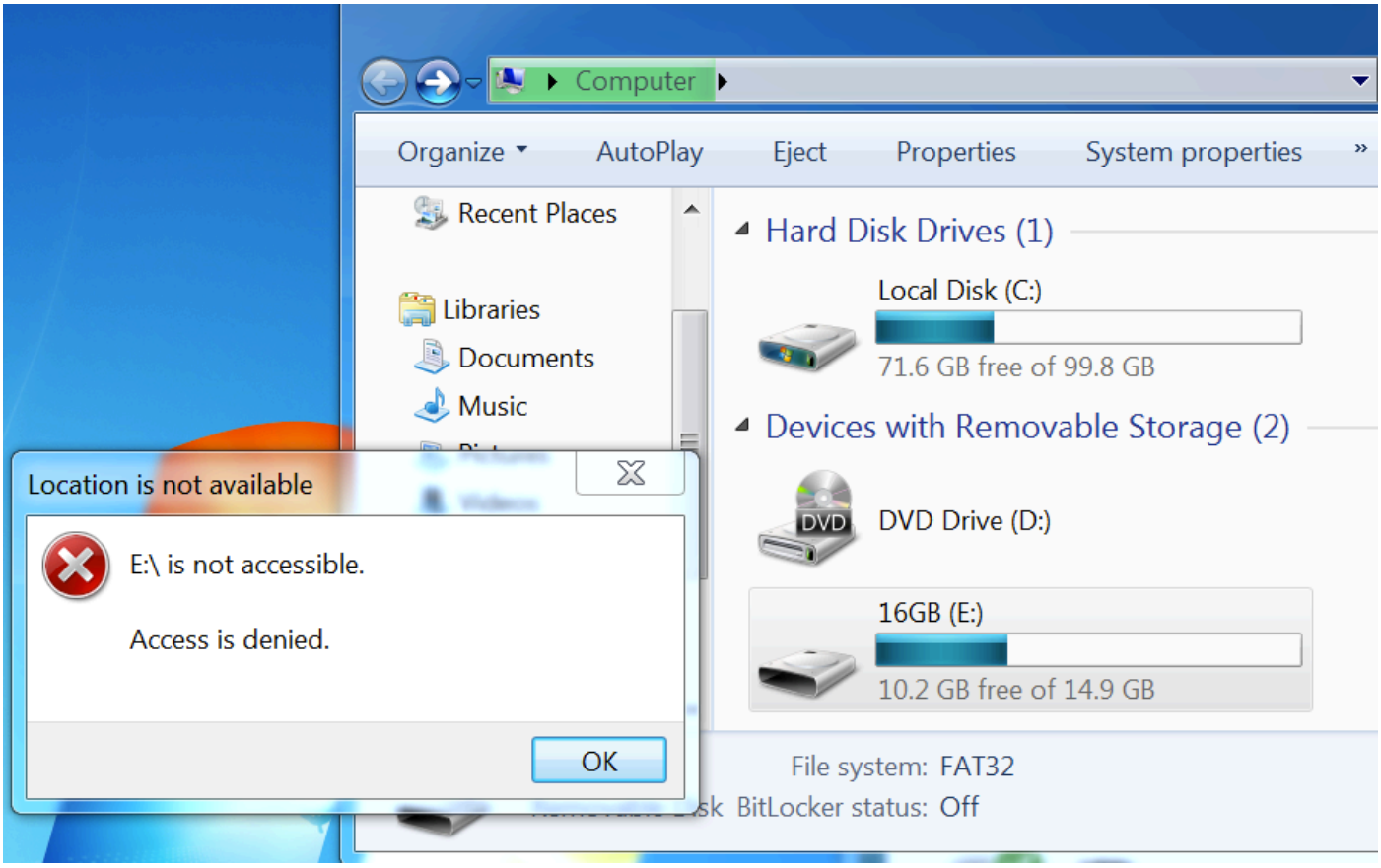
如果需要，會更新AnyConnect以及Posture and Compliance模組。

狀況檢查和CoA

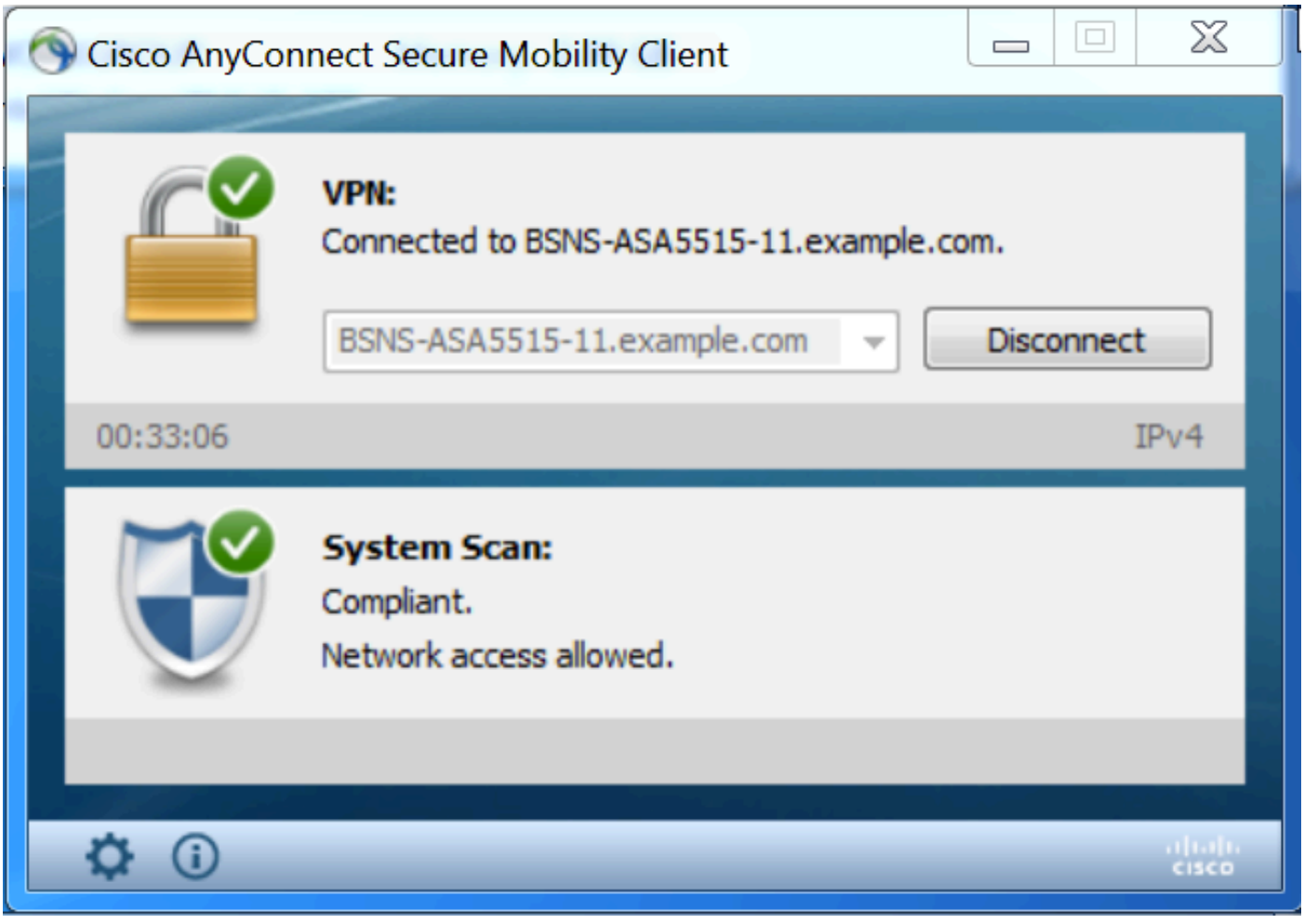
執行狀態模組，發現ISE(可能需要enroll.cisco.com的DNS A記錄才能成功)、下載並檢查狀態條件、新的OPSWAT v4阻止USB裝置操作。將為使用者顯示配置消息：



確認消息後，使用者無法再使用USB裝置：

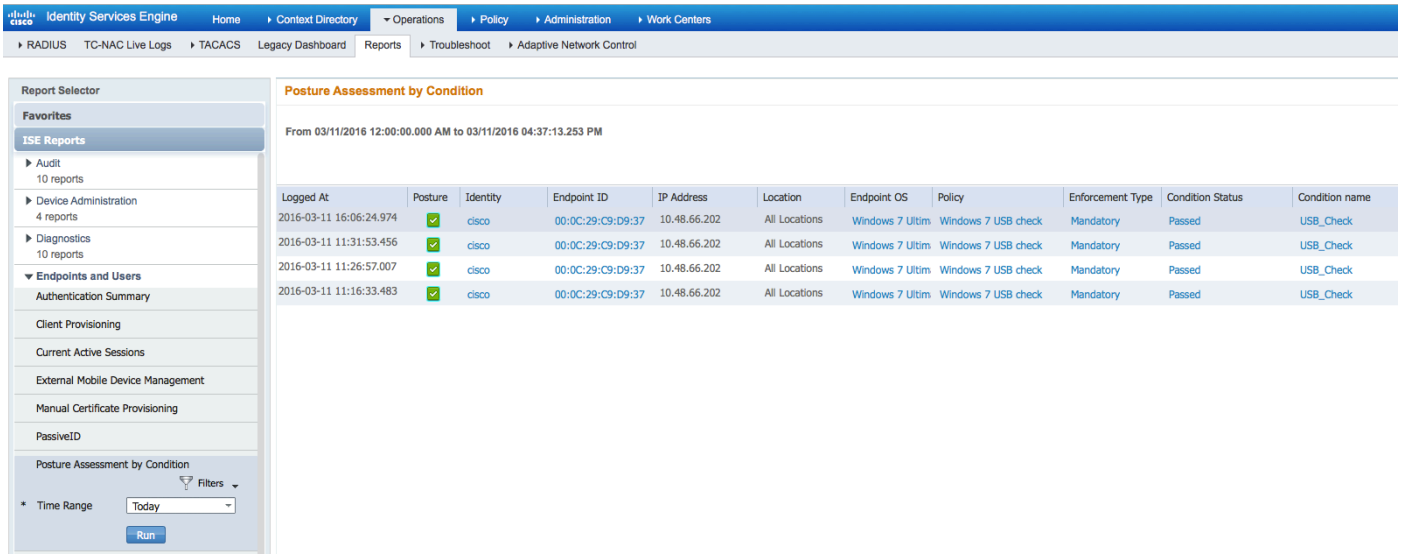


ASA刪除提供完全訪問許可權的重定向ACL。AnyConnect報告合規性：

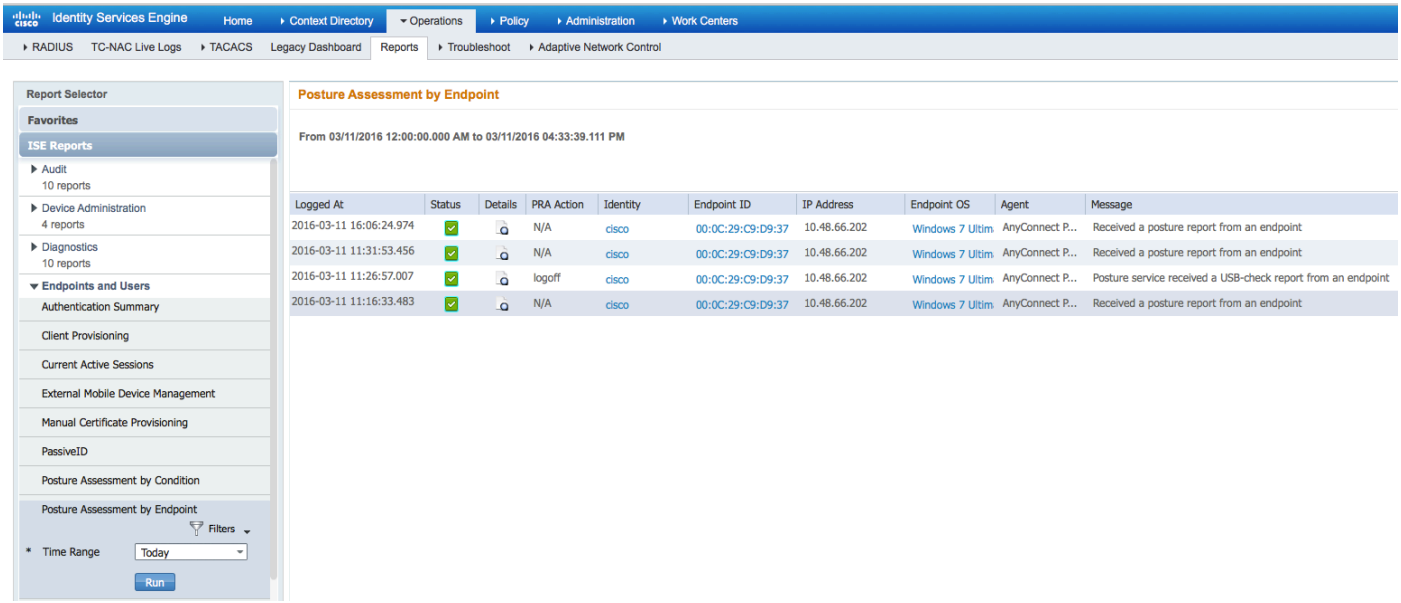


此外，有關ISE的詳細報告可以確認通過所需的條件。

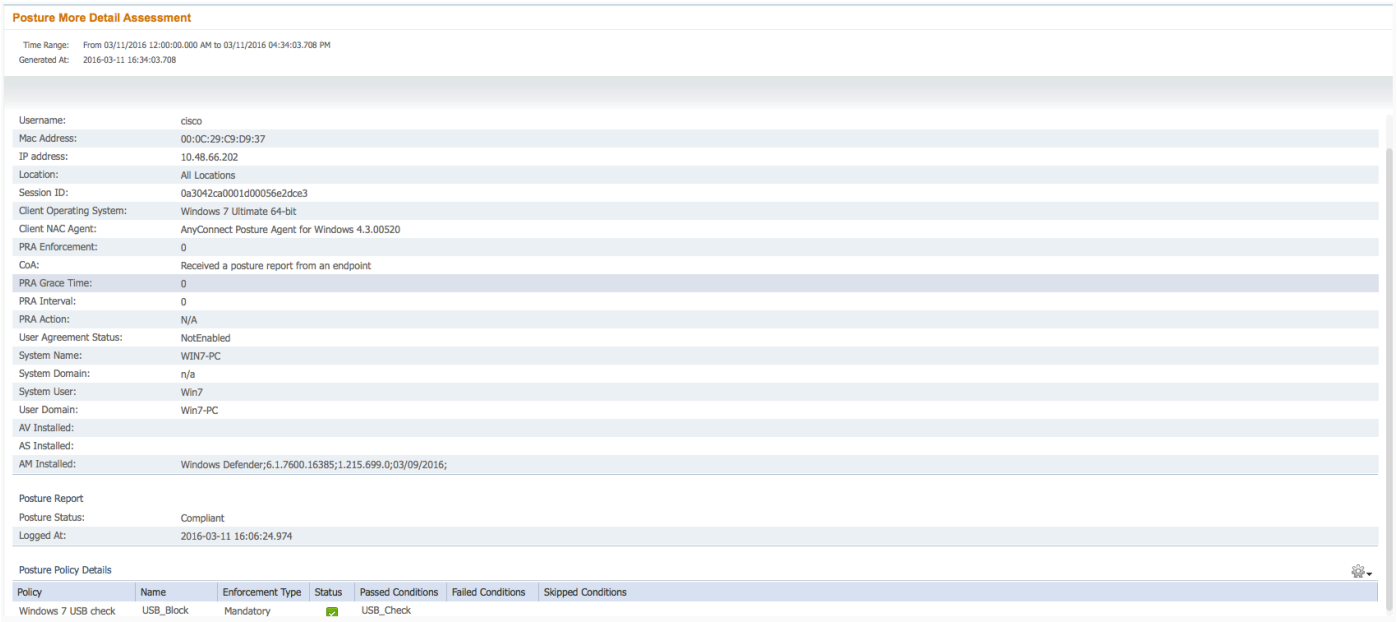
按條件進行的狀態評估：



終端安全評估：



終端報告的詳細資訊：



疑難排解

ISE能夠提供故障條件的詳細資訊，應相應地採取行動。

參考資料

- [配置外部伺服器以進行安全裝置使用者授權]
- [Cisco ASA系列VPN CLI配置指南9.1]
- [思科身份服務引擎管理員指南2.0版]
- [技術支援與文件 - Cisco Systems]