配置ISE 2.1和AnyConnect 4.3状态USB检查

Contents

Introduction

本文描述如何配置思科身份服务引擎(ISE)提供全部存取给网络，只有当USB大容量存储器设备是断开的时。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 可适应的安全工具(ASA) CLI配置和安全套接字层SSL VPN配置基础知识
- 远程访问VPN配置基础知识在ASA的
- ISE和状态服务基础知识

Components Used

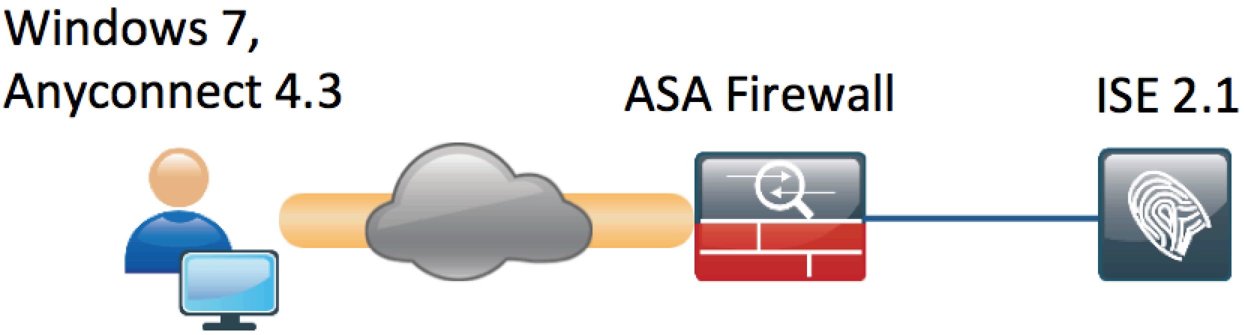
与AnyConnect安全移动性客户端4.3支持USB大容量存储器检查和修正一起的思科身份服务引擎(ISE)版本2.1。本文档中的信息基于以下软件版本：

- Cisco ASA软件版本9.2(4)及以后

- 与Cisco AnyConnect安全移动客户端版本4.3和以上的微软视窗版本7
- Cisco ISE，版本2.1及以后

Configure

Network Diagram



流下列：

- 用户没有被联络到VPN，接通专用的USB大容量存储器设备，并且内容为用户是可用的
- AnyConnect客户端起动的VPN会话通过ISE验证。终端的状态状况不知道，规则“Posture_Unknown”被击中结果，并且会话将重定向对ISE
- USB检查引入一个新的组登记AC ISE状态，他们不断地监控终端，只要在同一ISE被控制的网络依然是。可用唯一的逻辑修正的动作是阻拦他们的盘符确定的USB设备
- 在ASA的VPN会话是更新的，重定向ACL是被去除，并且全部存取授予

展示了VPN会话为例。状态功能为访问的其他类型也良好工作。

ASA

ASA为远程SSL VPN访问被配置使用ISE作为AAA服务器。需要配置与重定向ACL一起的Radius CoA ：

```
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
```

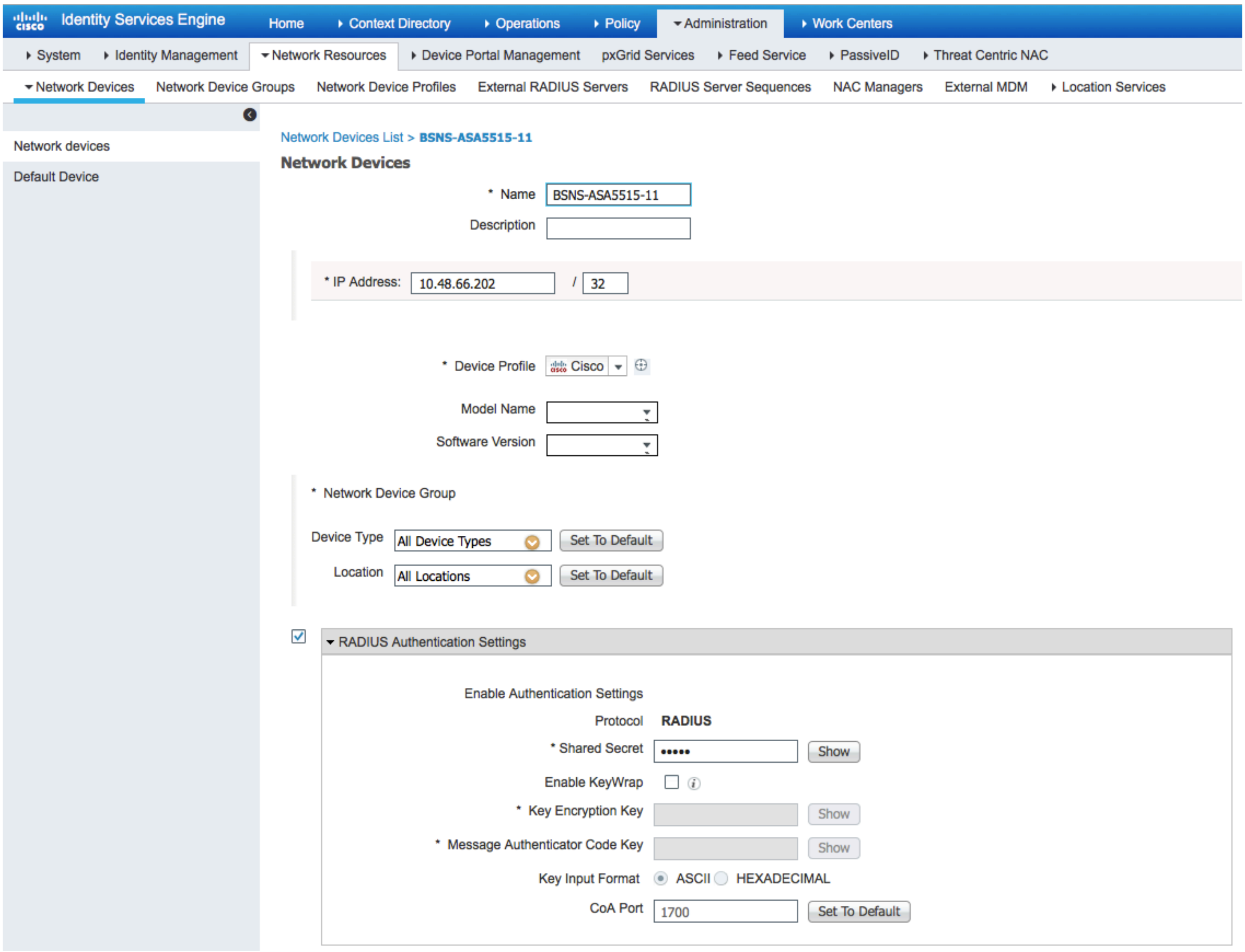
欲了解更详细的信息请参见：

与ISE版本1.3配置示例的AnyConnect 4.0集成

ISE

步骤1. Configure network设备

从**Administration >网络资源>网络Devices > Add** ASA。



Network Devices

* Name BSNS-ASA5515-11

Description

* IP Address: 10.48.66.202 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Device Type All Device Types

Location All Locations

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol RADIUS

* Shared Secret •••••

Enable KeyWrap □

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

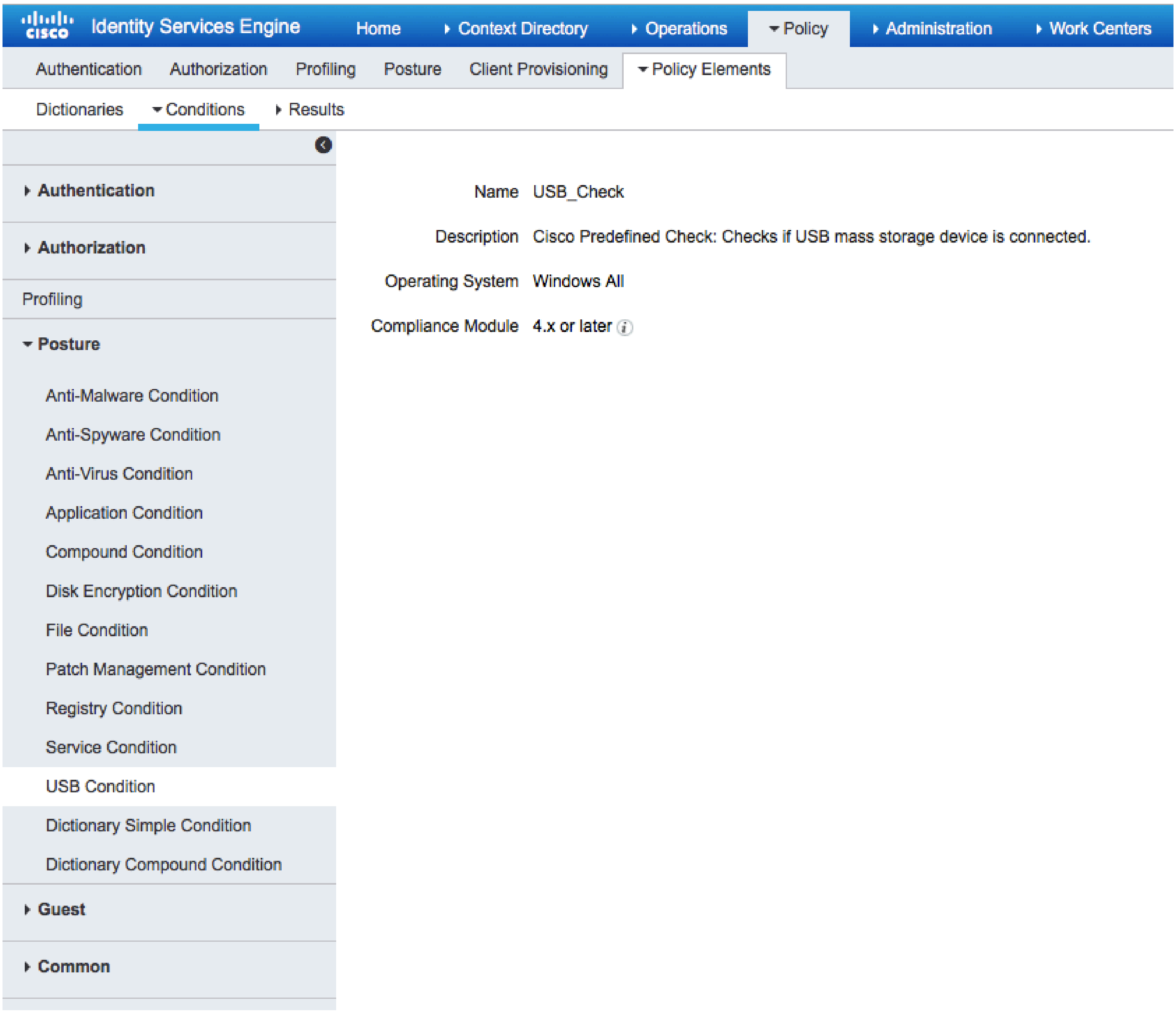
CoA Port 1700

步骤2.配置状态情况和策略

确定状态情况更新：**管理>System >设置>状态>更新**>**更新当前选项**。

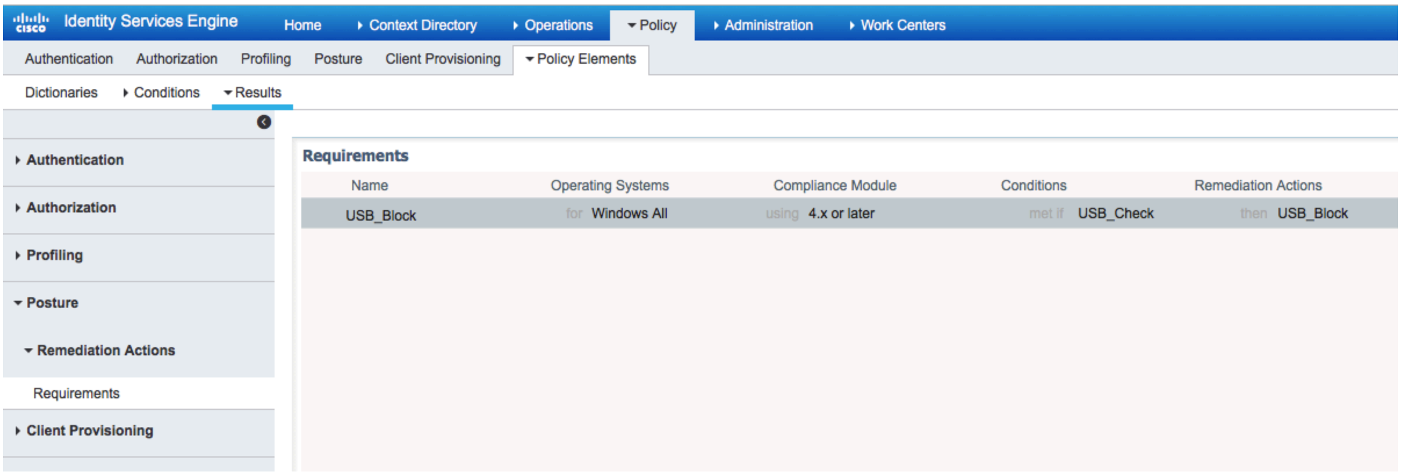
ISE 2.1附有一个预先配置的USB情况，检查USB大容量存储器设备是否被连接。

从**策略>Policy元素>调节>状态> USB情况**验证现有的情况：



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

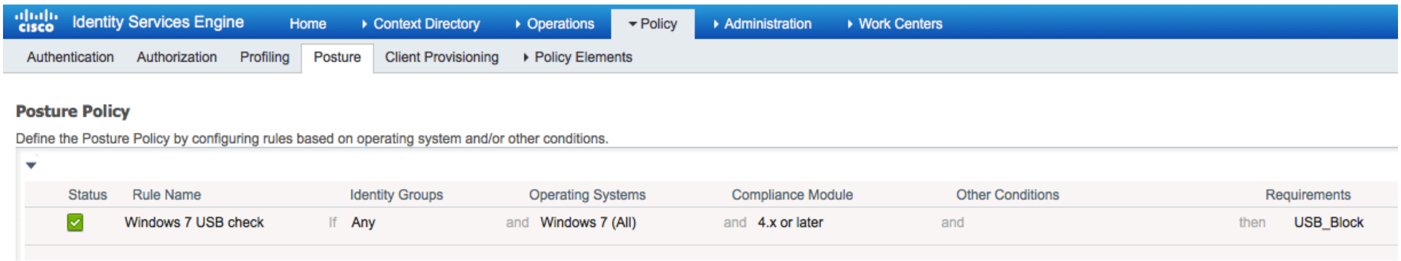
从**策略>Policy元素>发生>状态>需求**，验证使用该情况的预先配置的需求。



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

从**策略>状态**，请添加所有Windows的一个条件能使用该需求：

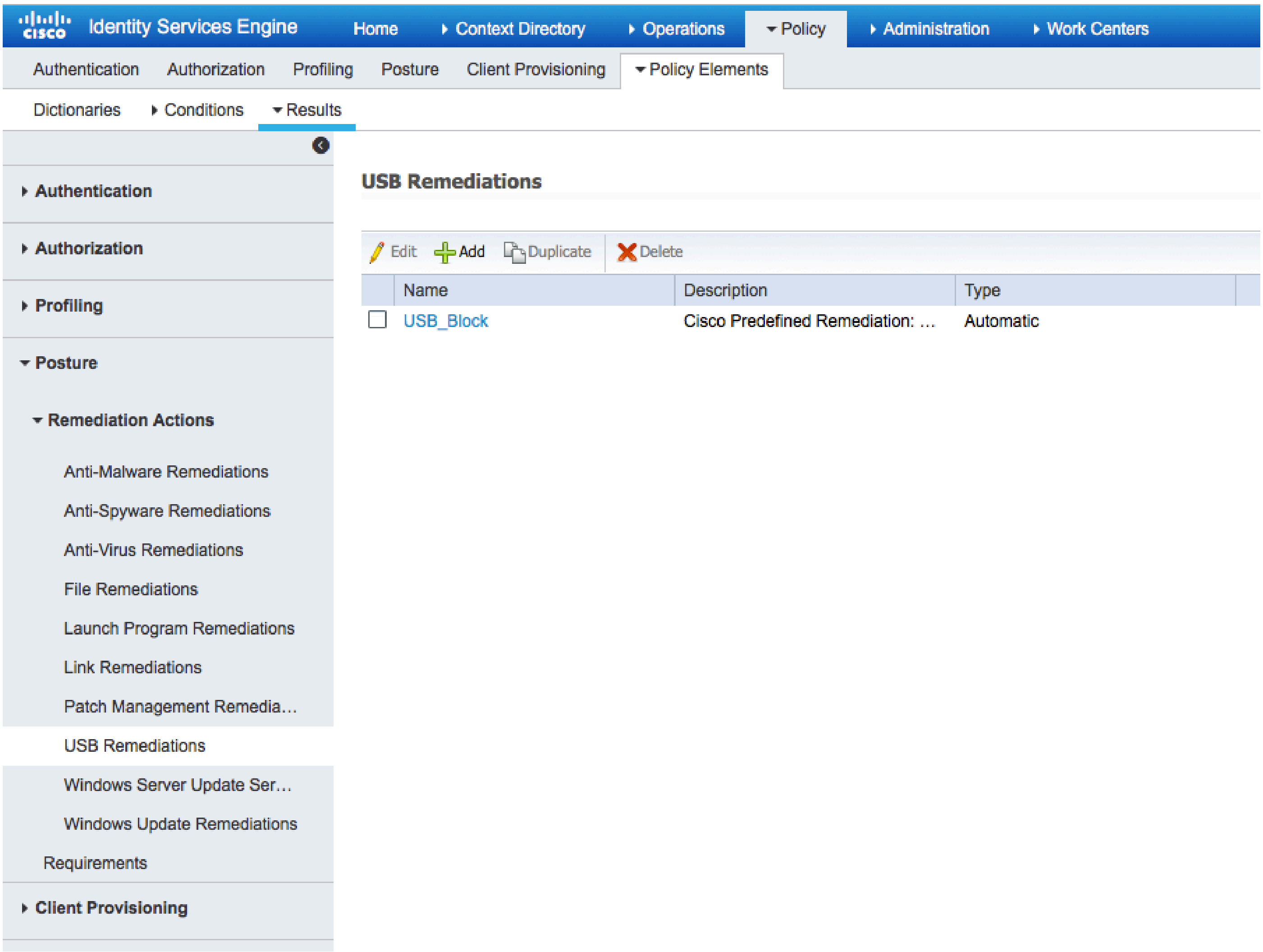


Posture Policy

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

从**策略>Policy元素>发生>状态>修正动作> USB补救**验证预先配置的修正动作阻拦USB存储设备：

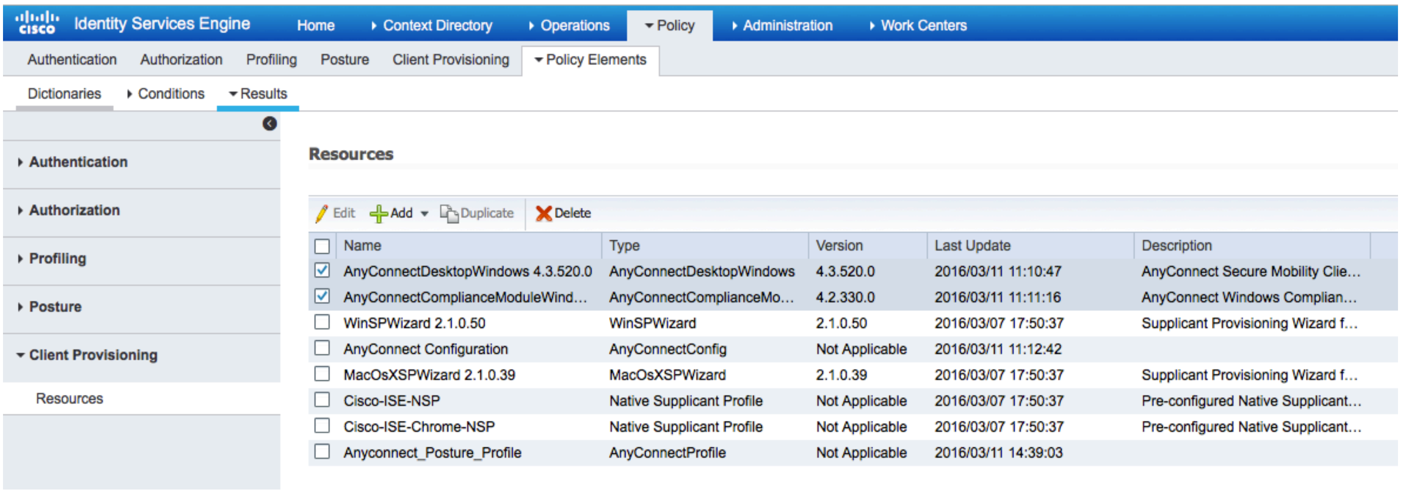


USB Remediations

	Name	Description	Type
□	USB_Block	Cisco Predefined Remediation: …	Automatic

步骤3.配置客户端设置资源和策略

从**策略>Policy元素>客户端设置>资源**从Cisco.com请下载标准模块并且手工加载AnyConnect 4.3程序包：

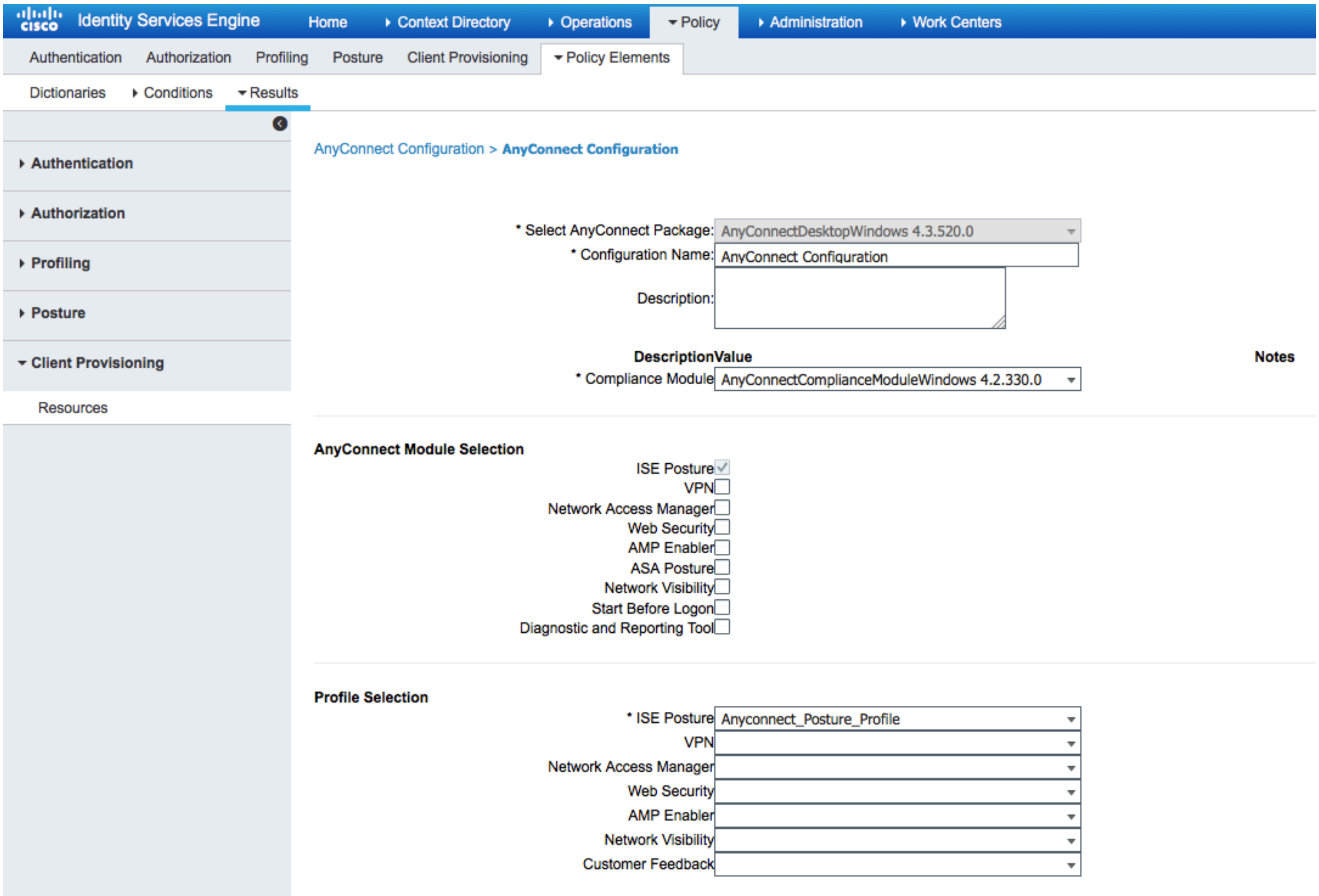


Resources

□	Name	Type	Version	Last Update	Description
☑	AnyConnectDesktopWindows 4.3.520.0	AnyConnectDesktopWindows	4.3.520.0	2016/03/11 11:10:47	AnyConnect Secure Mobility Clie...
☑	AnyConnectComplianceModuleWind...	AnyConnectComplianceMo...	4.2.330.0	2016/03/11 11:11:16	AnyConnect Windows Complian...
□	WinSPWizard 2.1.0.50	WinSPWizard	2.1.0.50	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
□	AnyConnect Configuration	AnyConnectConfig	Not Applicable	2016/03/11 11:12:42	
□	MacOsXSPWizard 2.1.0.39	MacOsXSPWizard	2.1.0.39	2016/03/07 17:50:37	Supplicant Provisioning Wizard f...
□	Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
□	Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/03/07 17:50:37	Pre-configured Native Supplicant...
□	Anyconnect_Posture_Profile	AnyConnectProfile	Not Applicable	2016/03/11 14:39:03	

使用**Add> NAC代理程序或AnyConnect状态配置文件请**创建一个AnyConnect状态配置文件(名字：*Anyconnect_Posture_Profile*)与默认设置。

使用**Add> AnyConnect配置请**添加一种AnyConnect配置(名字：AnyConnect配置) ：



AnyConnect Configuration > **AnyConnect Configuration**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.3.520.0
* Configuration Name: AnyConnect Configuration
Description:

Description	Value	Notes
* Compliance Module	AnyConnectComplianceModuleWindows 4.2.330.0	

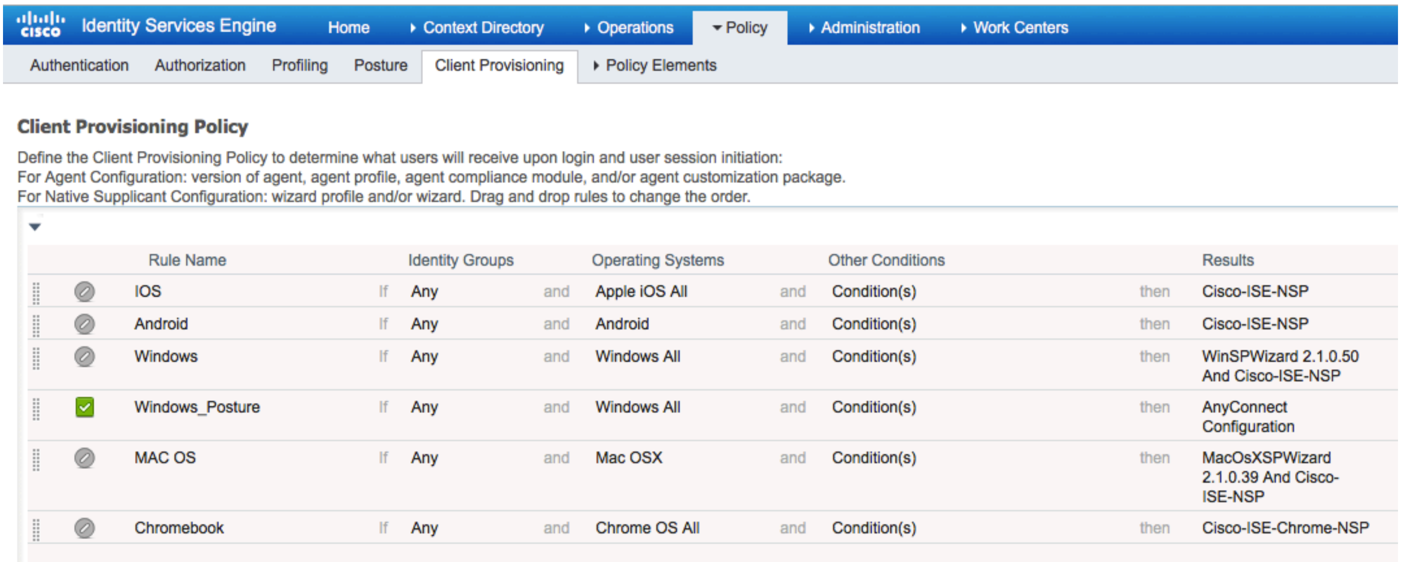
AnyConnect Module Selection

ISE Posture ☑
VPN □
Network Access Manager □
Web Security □
AMP Enabler □
ASA Posture □
Network Visibility □
Start Before Logon □
Diagnostic and Reporting Tool □

Profile Selection

* ISE Posture: Anyconnect_Posture_Profile
VPN:
Network Access Manager:
Web Security:
AMP Enabler:
Network Visibility:
Customer Feedback:

从**策略>客户端设置置请**创建一个新的策略(Windows_Posture) Windows的能使用AnyConnect配置：



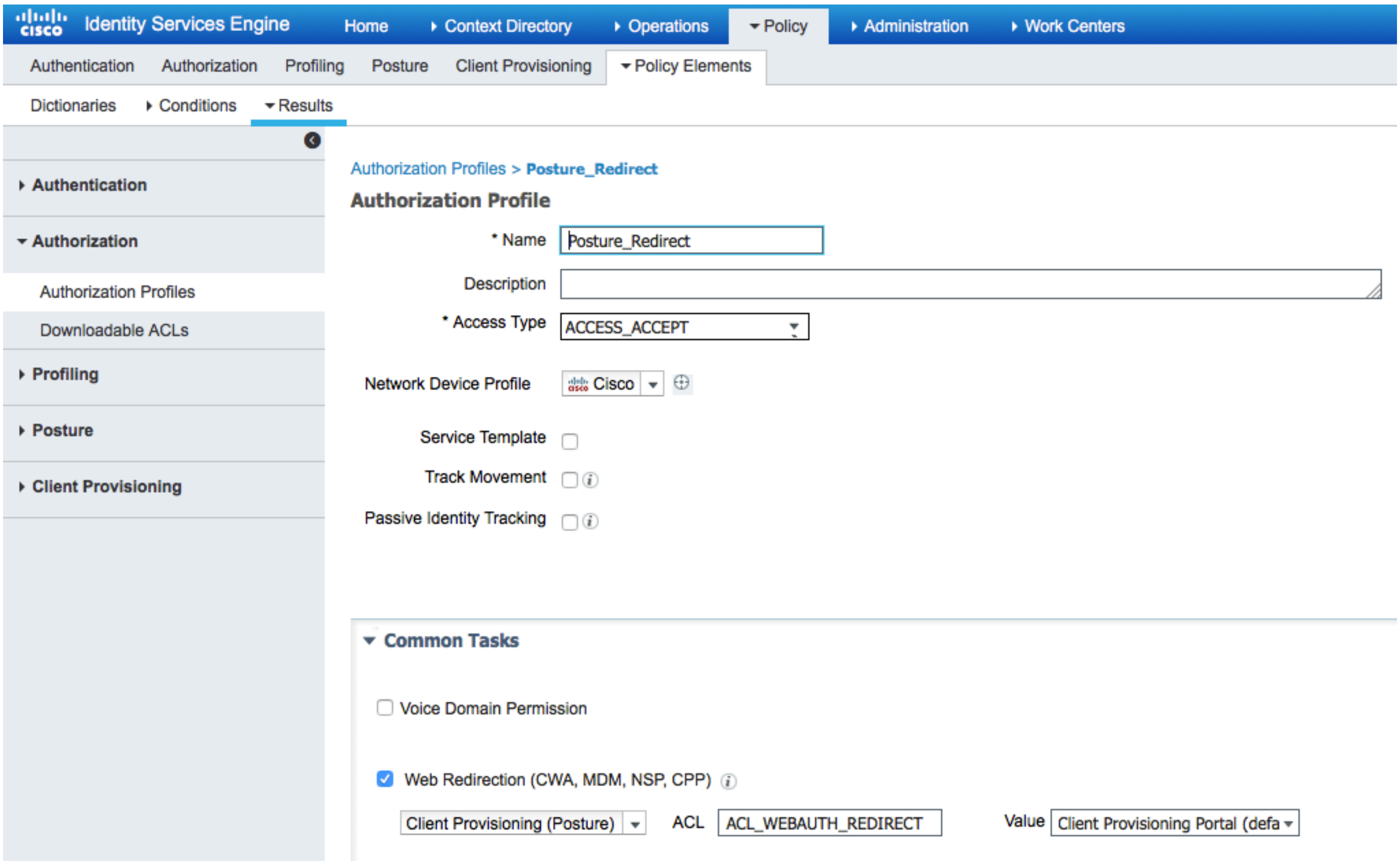
Client Provisioning Policy

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

步骤4.配置授权规则

从**策略>Policy元素>发生>授权**添加授权配置文件(名字：Posture_Redirect)该重定向对默认客户端设置的门户：



Authorization Profile

* Name: Posture_Redirect
Description:
* Access Type: ACCESS_ACCEPT
Network Device Profile: Cisco
Service Template □
Track Movement □
Passive Identity Tracking □

Common Tasks

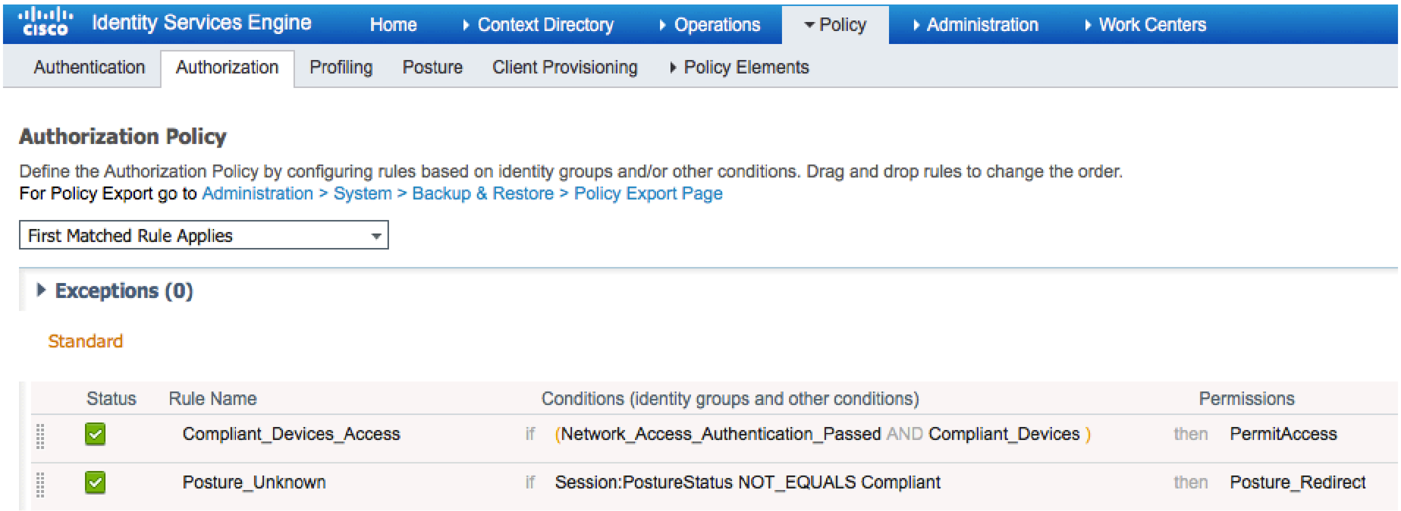
□ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL ACL_WEBAUTH_REDIRECT Value Client Provisioning Portal (defa

注意：ACL_WEBAUTH_REDIRECT ACL在ASA被定义。

从**策略>授权请**创建重定向的一个授权规则。兼容设备的一个授权规则在ISE预先配置：



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

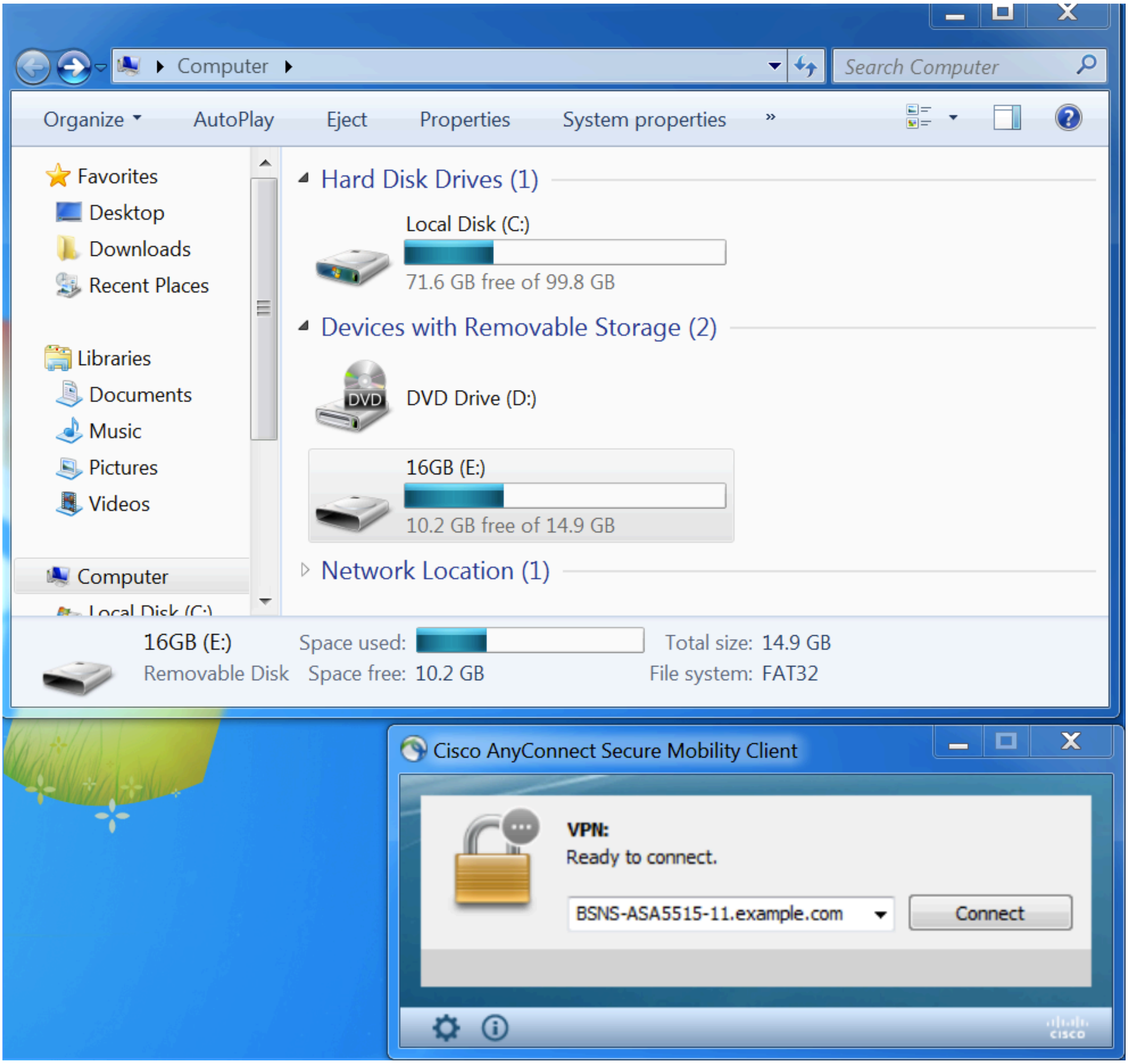
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess
☑	Posture_Unknown	if	Session:PostureStatus NOT_EQUALS Compliant	then	Posture_Redirect

如果终端是兼容的，全部存取提供。如果状态是未知或固执的，客户端设置的重定向返回。

Verify

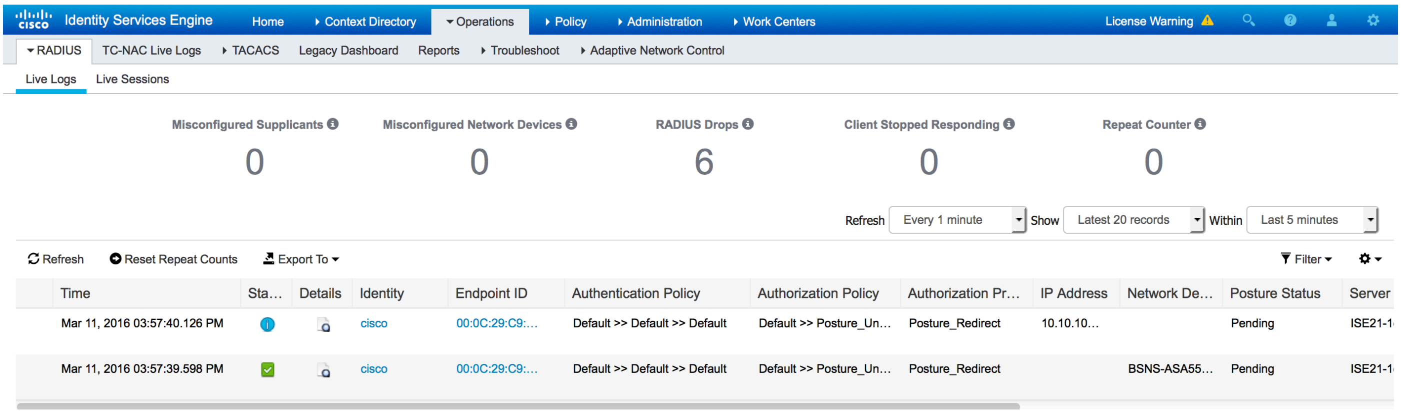
在VPN会话建立前

USB设备接通的和其内容为用户是可用的。



VPN会话建立

作为Posture_Redirect授权配置文件一部分，在认证时， ISE将返回重定向访问列表和重定向URL



Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 6 | Client Stopped Responding 0 | Repeat Counter 0

Refresh Every 1 minute Show Latest 20 records Within Last 5 minutes

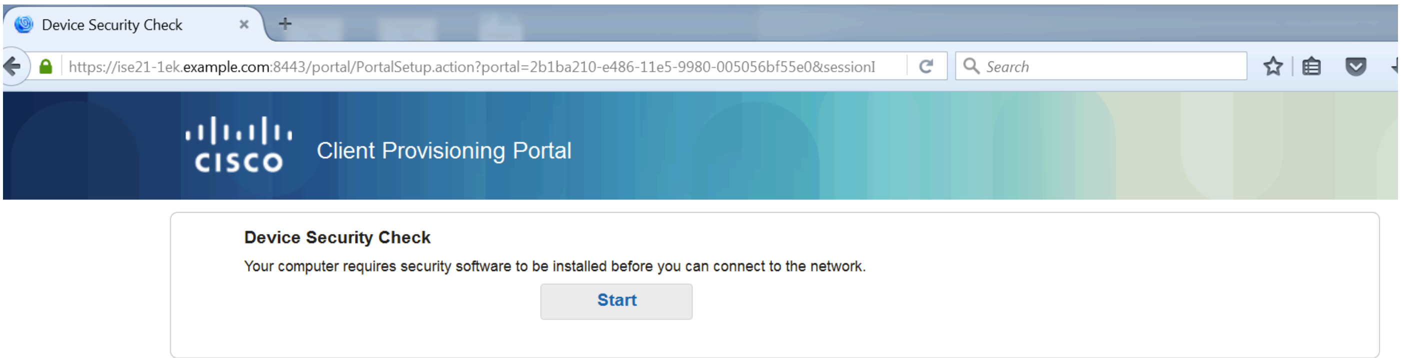
Time	Sta...	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Pr...	IP Address	Network De...	Posture Status	Server
Mar 11, 2016 03:57:40.126 PM	●		cisco	00:0C:29:C9:...	Default >> Default >> Default	Default >> Posture_Un...	Posture_Redirect	10.10.10...		Pending	ISE21-1
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

一旦VPN会话建立，从客户端的ASA数据流根据重定向访问列表将重新定向：

```
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
```

客户端设置

在该阶段，终端Web浏览器数据流重定向对客户端设置的ISE ：



Device Security Check
https://ise21-1ek.example.com:8443/portal/PortalSetup.action?portal=2b1ba210-e486-11e5-9980-005056bf55e0&sessionI
Search
Client Provisioning Portal

Device Security Check

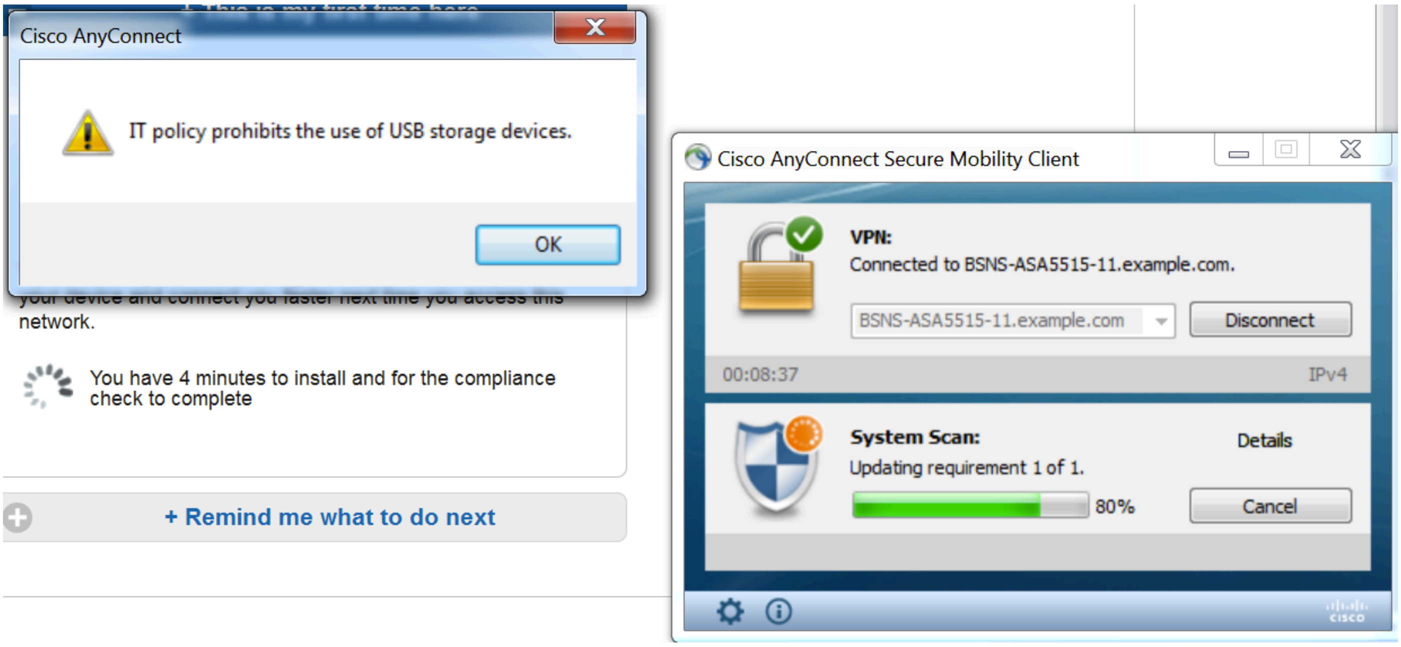
Your computer requires security software to be installed before you can connect to the network.

Start

若需要，与状态和标准模块一起的AnyConnect是更新的。

状态检查和CoA

状态模块被执行，发现ISE (也许要求有enroll.cisco.com的DNS A记录能成功)，下载并且检查状态情况，新的OPSWAT v4块USB设备动作。被配置的消息为用户将显示：



Cisco AnyConnect

IT policy prohibits the use of USB storage devices.

OK

your device and connect you faster next time you access this network.

You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

Cisco AnyConnect Secure Mobility Client

VPN:
Connected to BSNS-ASA5515-11.example.com.

BSNS-ASA5515-11.example.com

Disconnect

00:08:37 IPv4

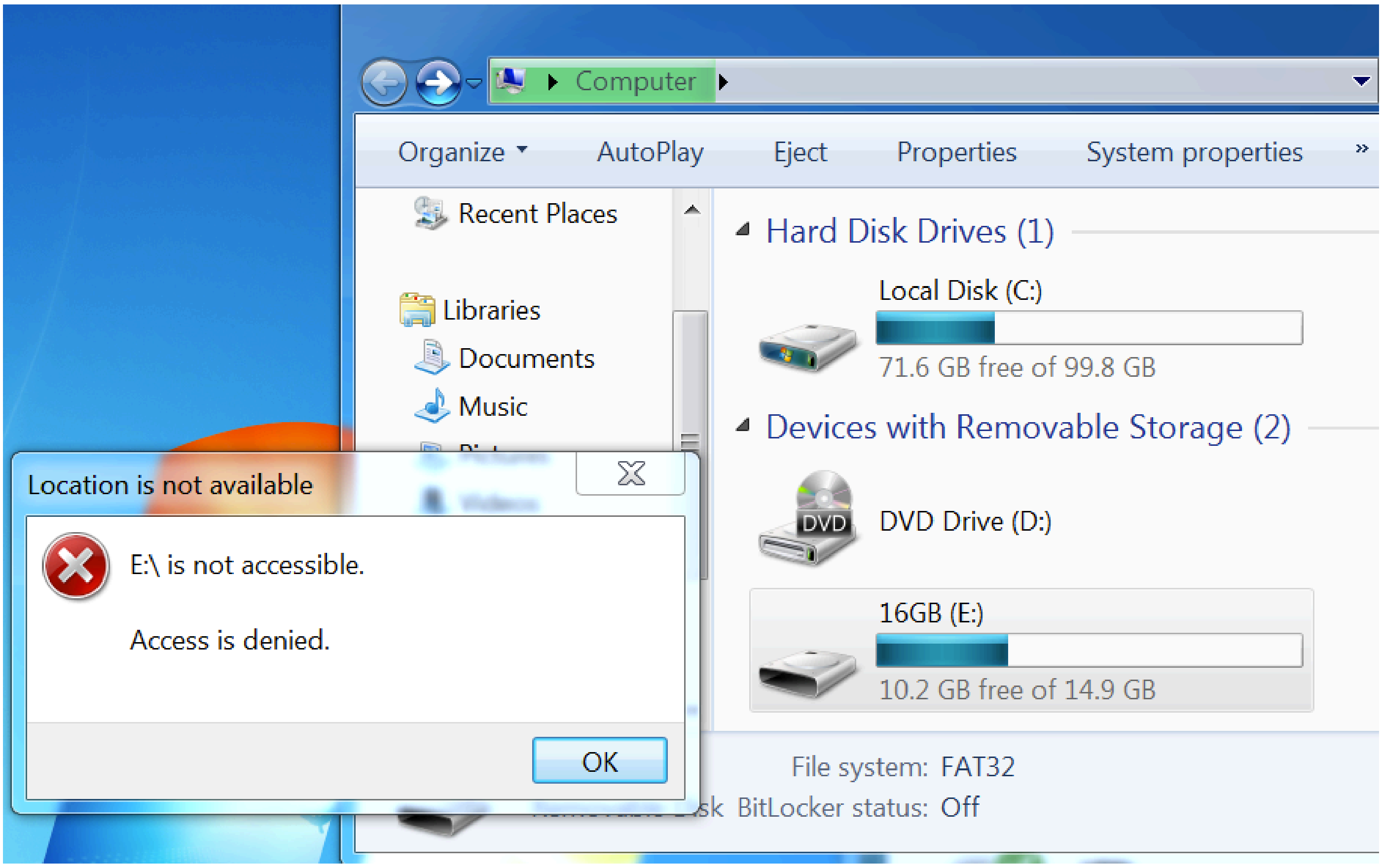
System Scan:
Updating requirement 1 of 1.

Details

80%

Cancel

一旦消息被确认， USB设备为用户不再是可用的：



Location is not available

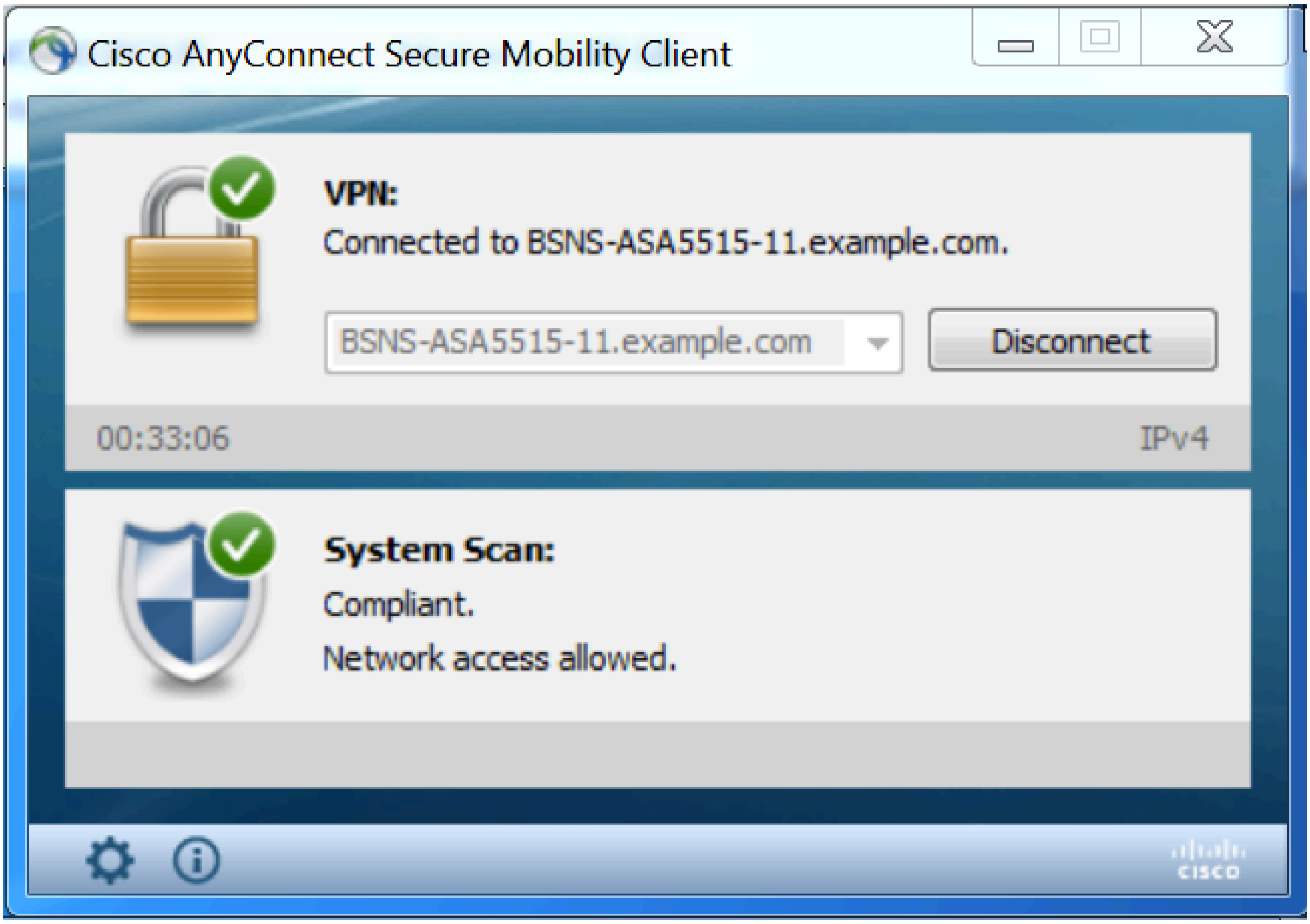
E:\ is not accessible.

Access is denied.

File system: FAT32

BitLocker status: Off

ASA取消重定向ACL提供全部存取。AnyConnect报告标准：



Cisco AnyConnect Secure Mobility Client

VPN:

Connected to BSNS-ASA5515-11.example.com.

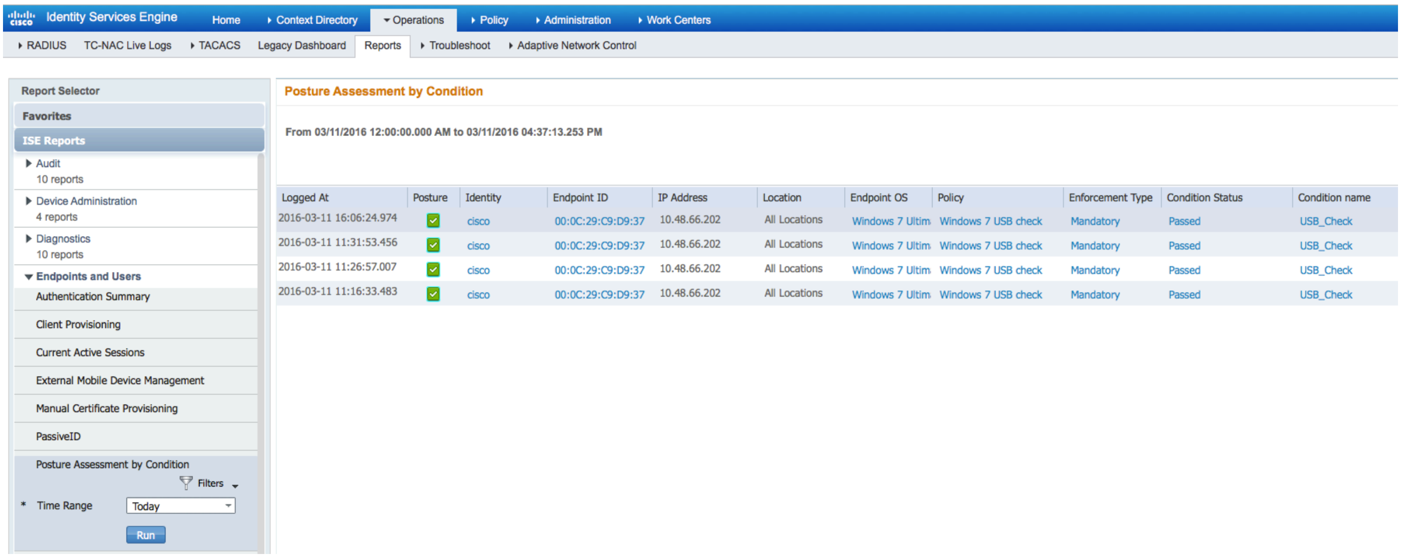
System Scan:

Compliant.

Network access allowed.

并且关于ISE的详细资料报表能确认必需的情况通过。

由情况的状态评估：

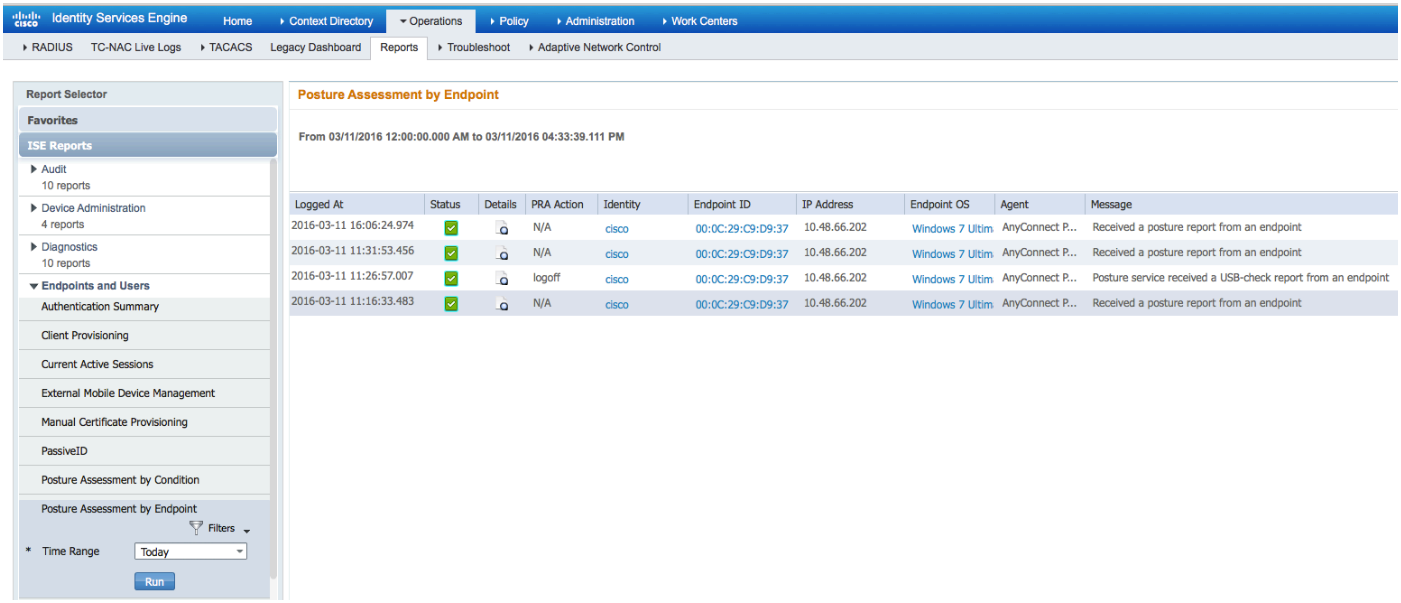


Posture Assessment by Condition

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

由终端的状态评估：

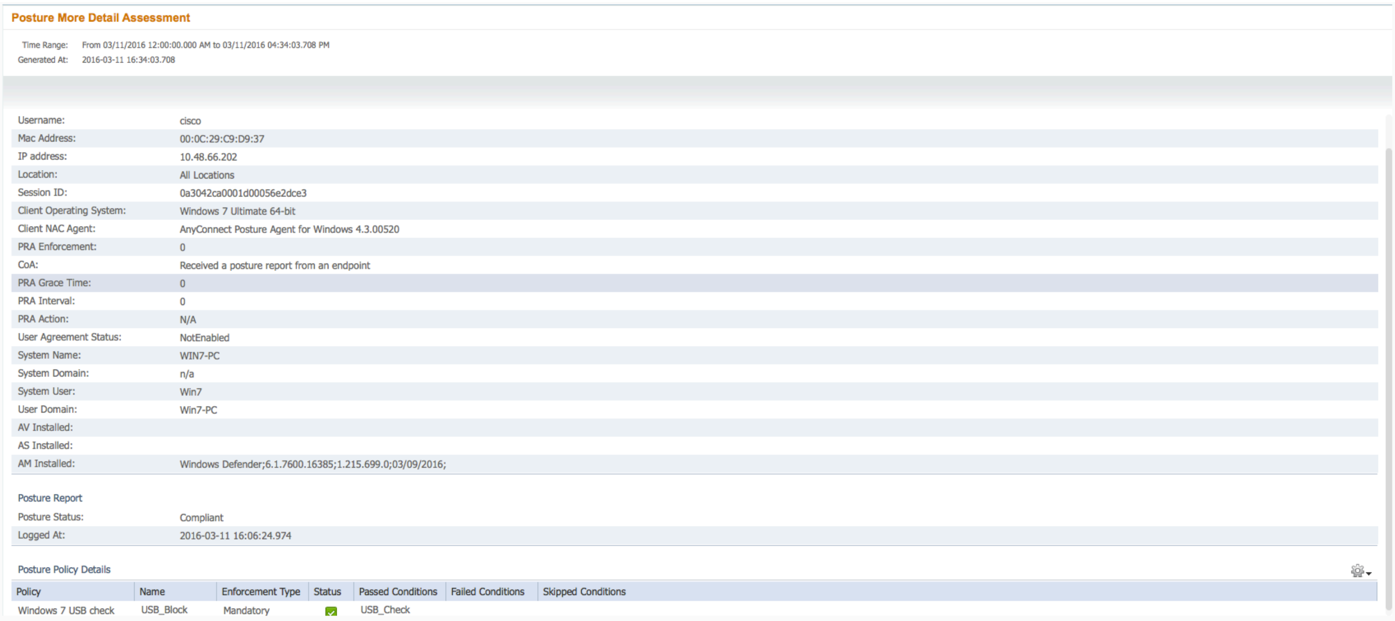


Posture Assessment by Endpoint

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

终端报告详细资料：



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 NAC 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		

Troubleshoot

ISE能提供细节在失败条件，动作应该相应地采取。

参考

- 为安全设备用户授权配置外部服务器
- 思科 ASA 系列 VPN CLI 配置指南，版本 9.1
- 思科身份服务引擎管理员指南，版本2.0
- Technical Support & Documentation - Cisco Systems