Configurar o 2.1 ISE e a verificação da postura USB de AnyConnect 4.3

Índice

Introdução

Este original descreve como configurar o Cisco Identity Services Engine (ISE) para fornecer o acesso direto à rede somente quando os dispositivos de memória de massa USB são desligados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração de CLI da ferramenta de segurança (ASA) e da configuração de VPN adaptáveis do Secure Socket Layer (SSL)
- Conhecimento básico da configuração do acesso remoto VPN no ASA
- Conhecimento básico do ISE e dos serviços da postura

Componentes Utilizados

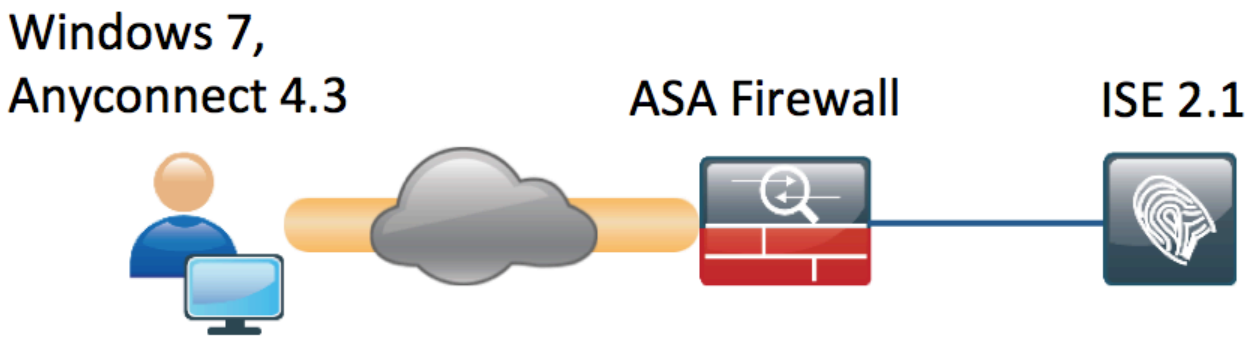
Versão 2.1 do Cisco Identity Services Engine (ISE) junto com a verificação e a remediação

seguras da memória de massa dos apoios USB do cliente 4.3 da mobilidade de AnyConnect. As informações neste documento são baseadas nestas versões de software:

- Versões de software de Cisco ASA 9.2(4) e mais atrasado
- Versão 7 de Microsoft Windows com versão 4.3 e mais recente do Cliente de mobilidade Cisco AnyConnect Secure
- Cisco ISE, 2.1 da liberação e mais tarde

Configurar

Diagrama de Rede



O fluxo é o seguinte:

- O usuário não é conectado ao VPN ainda, o dispositivo de memória de massa privado USB é obstruído dentro e satisfeito está disponível para o usuário
- A sessão de VPN iniciada pelo cliente de AnyConnect é autenticada através do ISE. O estado da postura do valor-limite não é sabido, a regra “Posture_Unknown” é batida e em consequência a sessão será reorientada ao ISE
- As verificações USB introduzem uma classe nova de verificam dentro a postura C.A. ISE, que monitorem continuamente o valor-limite enquanto permanece na mesma rede controlada ISE. A única ação lógica da remediação disponível é obstruir os dispositivos USB identificados por sua letra da unidade
- A sessão de VPN no ASA é atualizada, reorienta o ACL é removida e o acesso direto é concedido

A sessão de VPN foi apresentada apenas como um exemplo. A funcionalidade da postura está trabalhando muito bem igualmente para outros tipos do acesso.

ASA

O ASA é configurado para o acesso remoto SSL VPN usando o ISE como o servidor AAA. O CoA do raio junto com reorienta o ACL precisa de ser configurado:

```
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
```

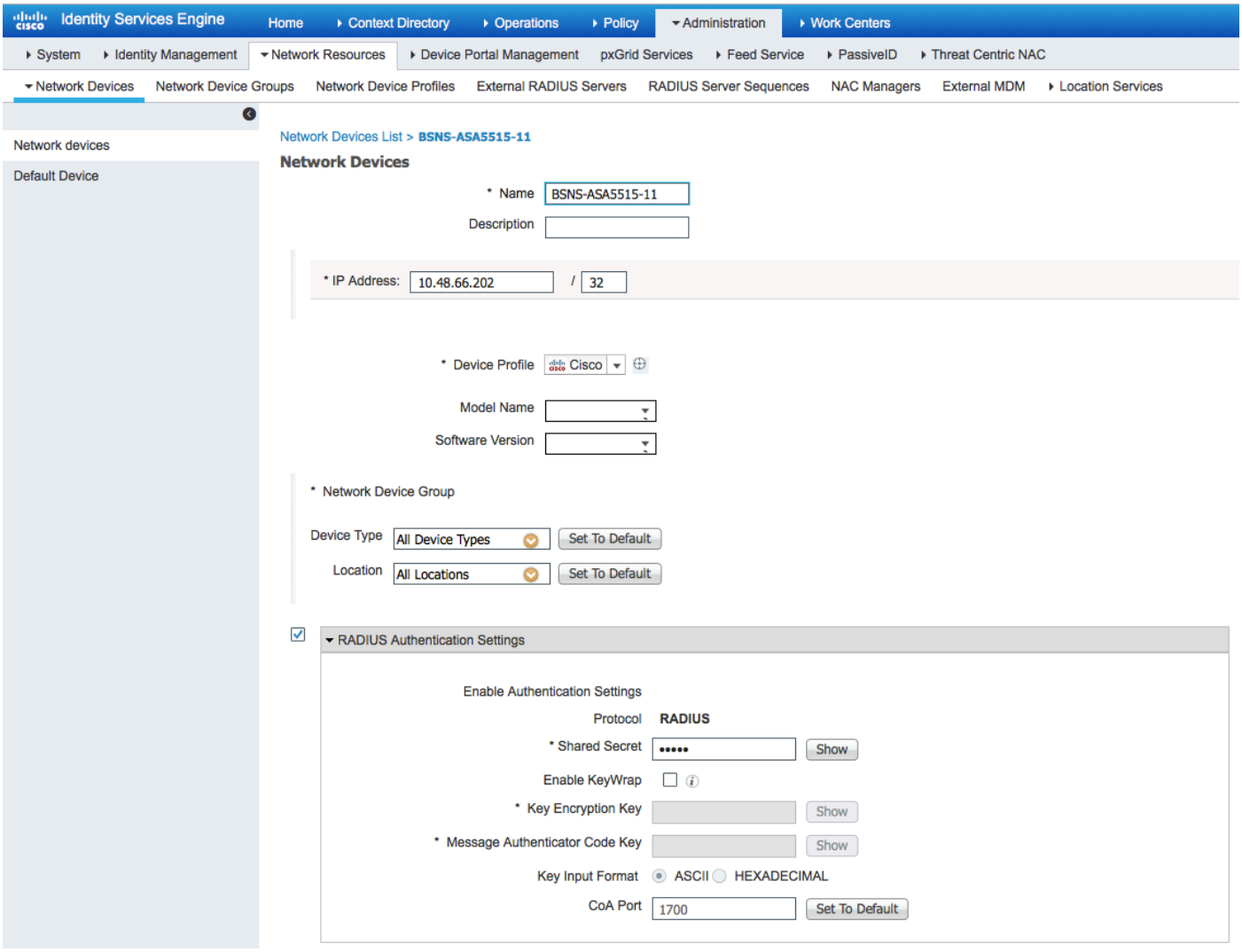
Satisfaça para mais detalhes referem:

Integração de AnyConnect 4.0 com exemplo de configuração da versão 1.3 ISE

ISE

Etapa 1. Configurar o dispositivo de rede

Do > Add ASA da **administração > dos recursos de rede > dos dispositivos de rede**.

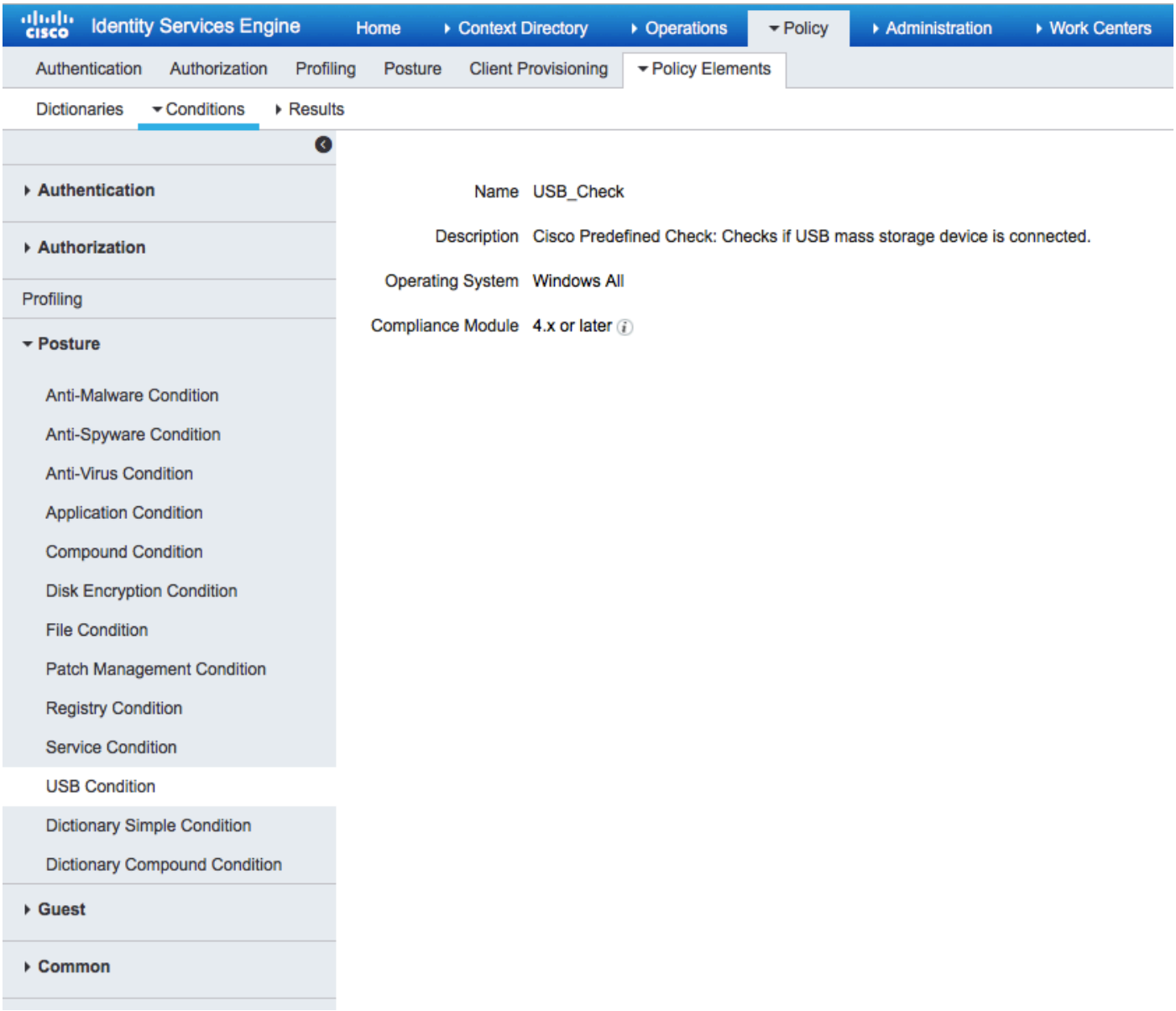


Etapa 2. Configurar condições e políticas da postura

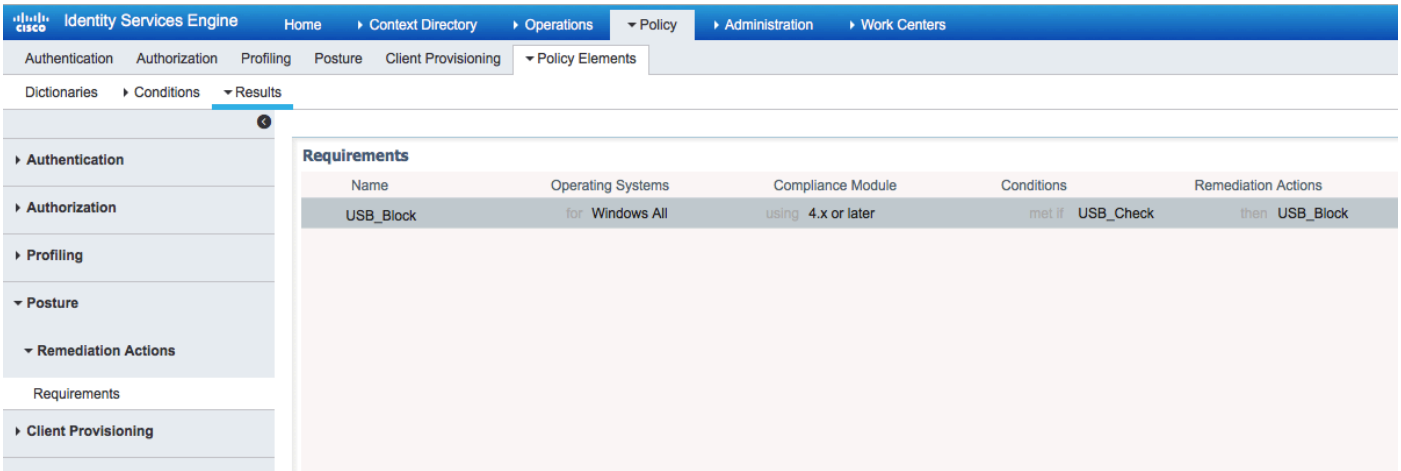
Certifique-se que condições da postura está atualizada: **A administração > o sistema > os ajustes > a postura > atualizam > opção da atualização agora**.

O 2.1 ISE vem com uma condição preconfigured USB, que verifique se um dispositivo de memória de massa USB é conectado.

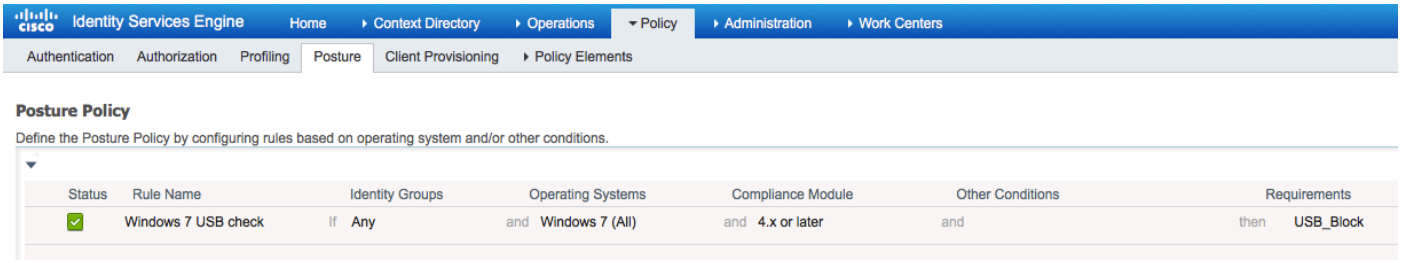
Da política > dos elementos da política > condiciona > postura > condição USB verificam condição existente:



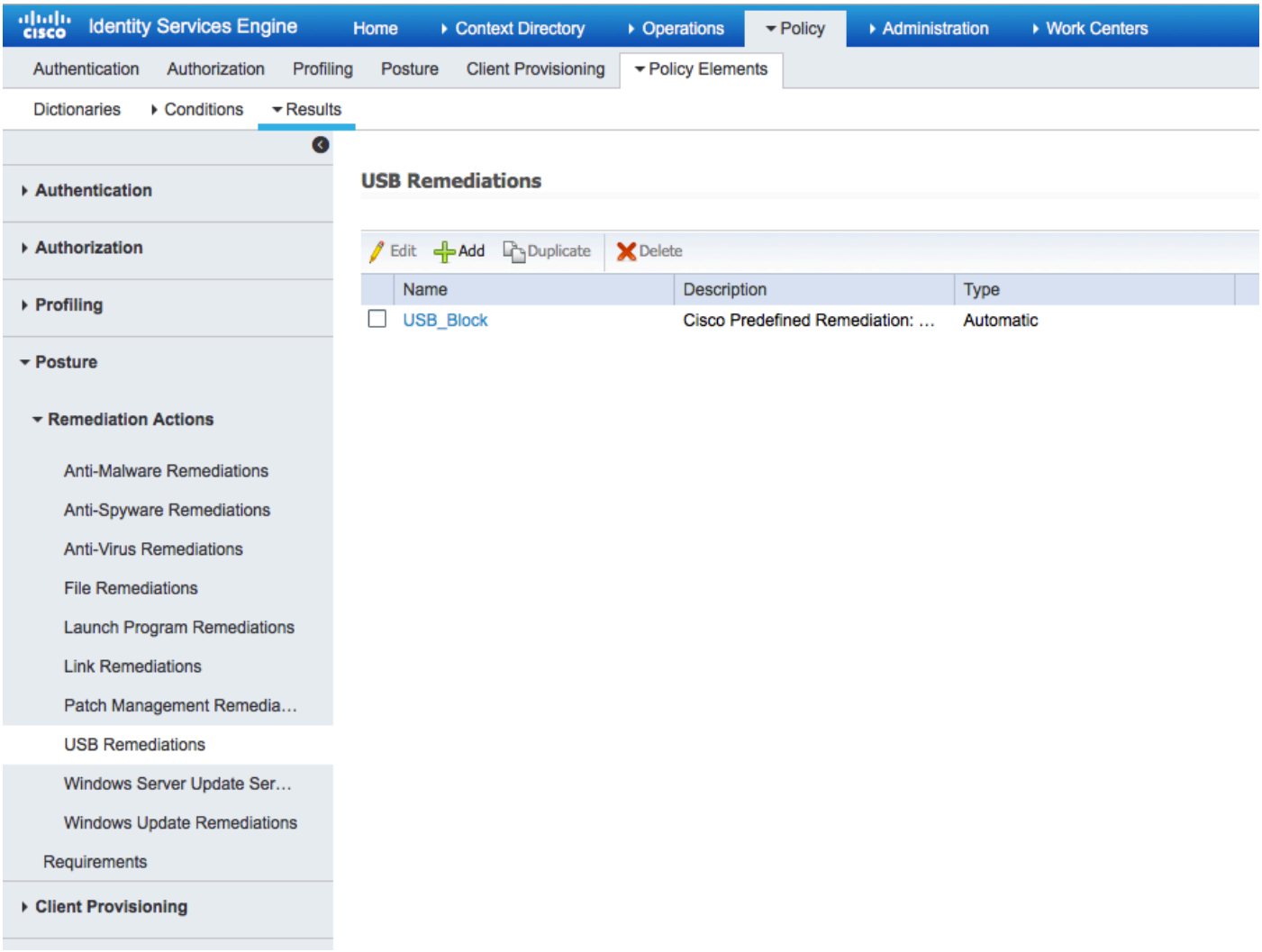
Da política > dos elementos da política > resultam > a postura > as exigências, verificam a exigência preconfigured que usa essa circunstância.



Da política > da postura, adicionar uma condição para que todo o Windows use essa exigência:

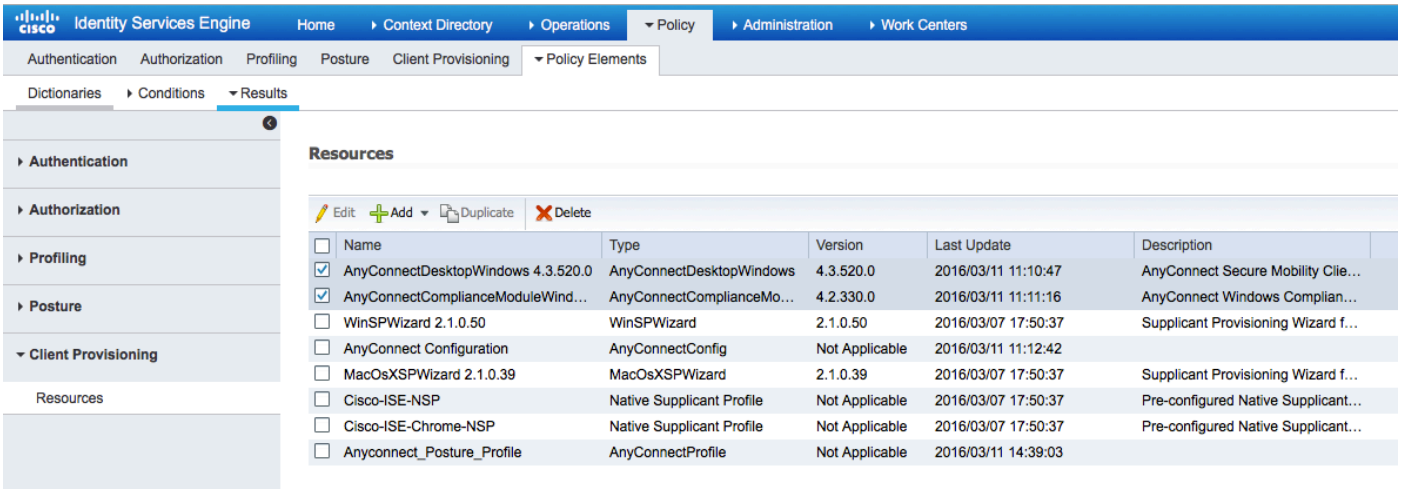


Da política > dos elementos da política > resultam > as ações da postura > da remediação > as remediações USB verificam a ação preconfigured da remediação para obstruir dispositivos de armazenamento USB:



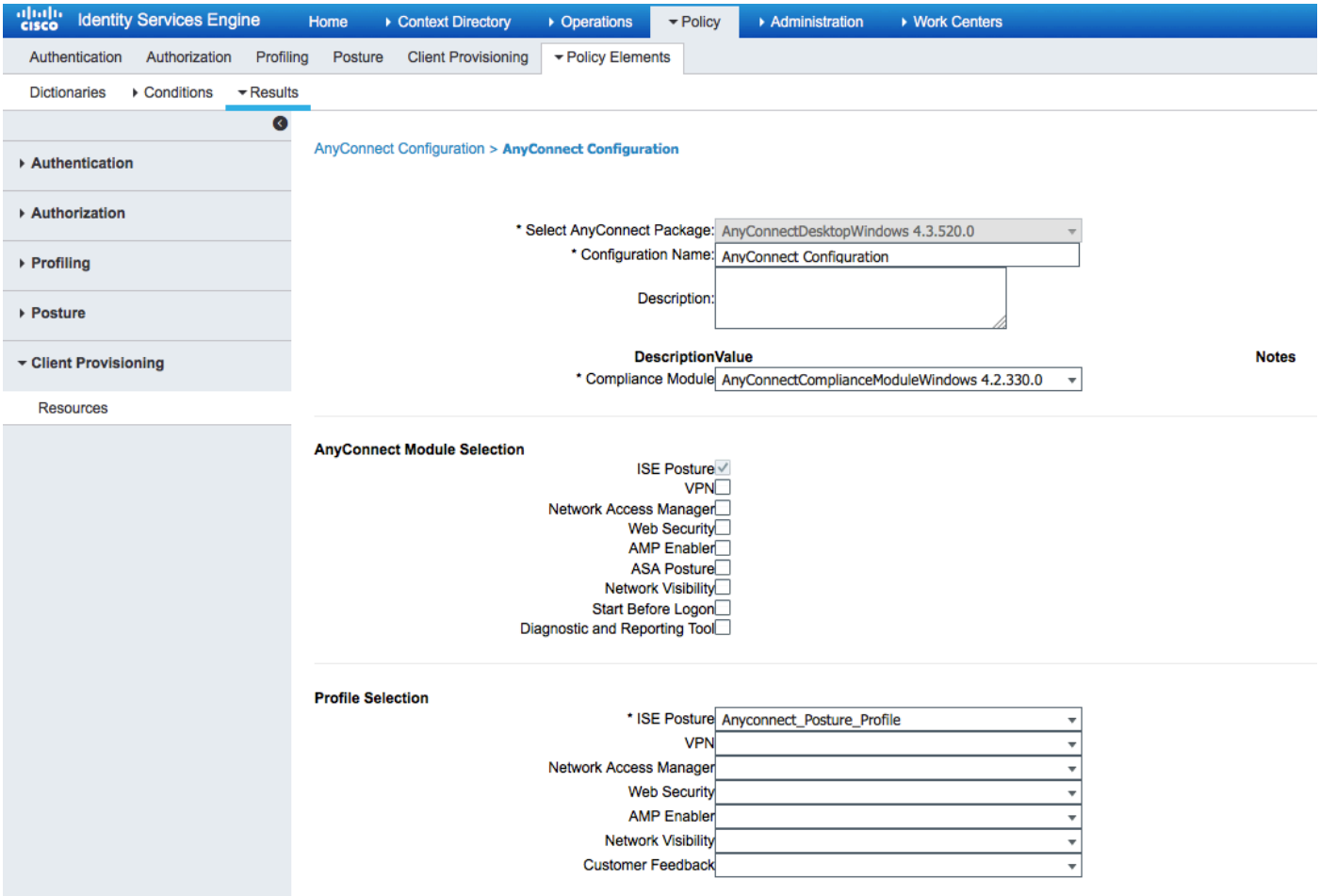
Etapa 3. Configurar recursos e política do abastecimento do cliente

Da política > dos elementos da política > do abastecimento > dos recursos do cliente transfira o módulo da conformidade de Cisco.com e transfira arquivos pela rede manualmente o pacote de AnyConnect 4.3:

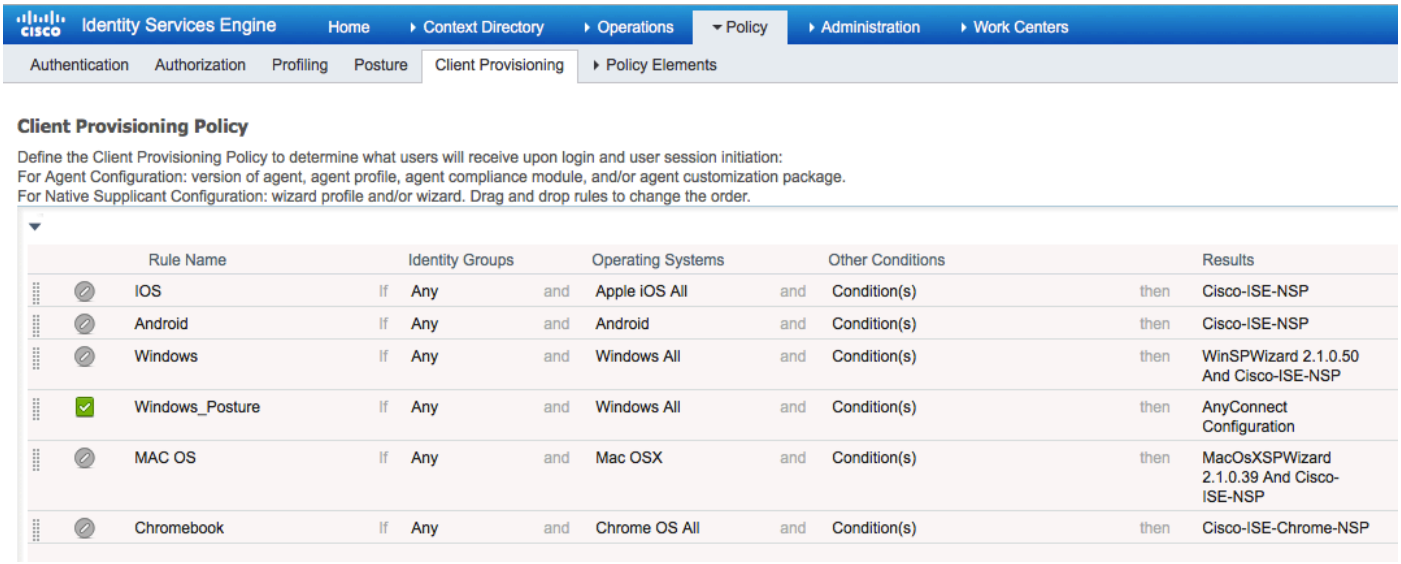


Usar-se **adiciona > agente NAC ou o perfil da postura de AnyConnect** cria um perfil da postura de AnyConnect (nome: *Anyconnect_Posture_Profile*) com configurações padrão.

Usar-se **adiciona > configuração de AnyConnect** adiciona uma configuração de AnyConnect (nome: Configuração de AnyConnect):

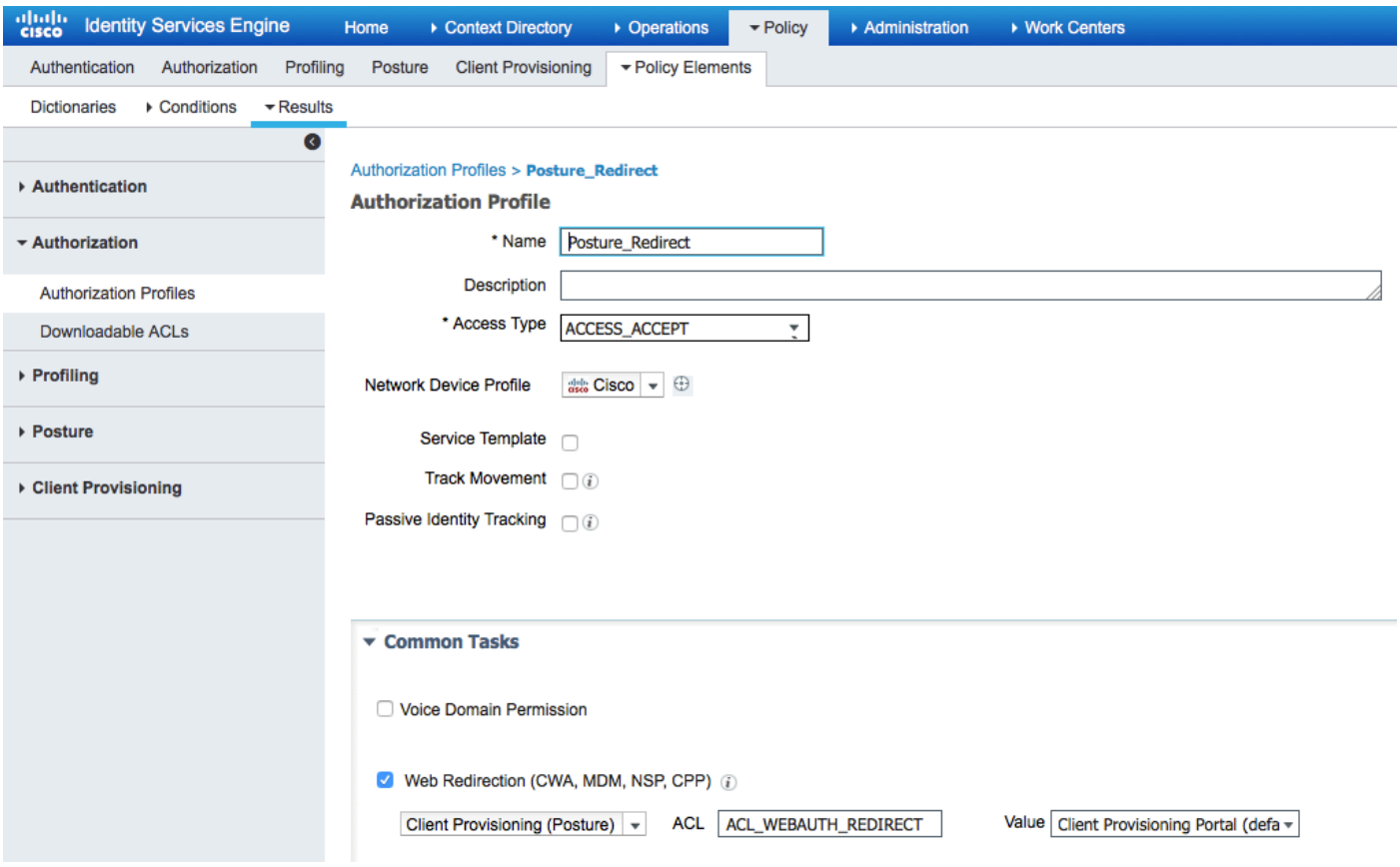


Da política > do abastecimento do cliente crie uma política nova (Windows_Posture) para que Windows use a configuração de AnyConnect:



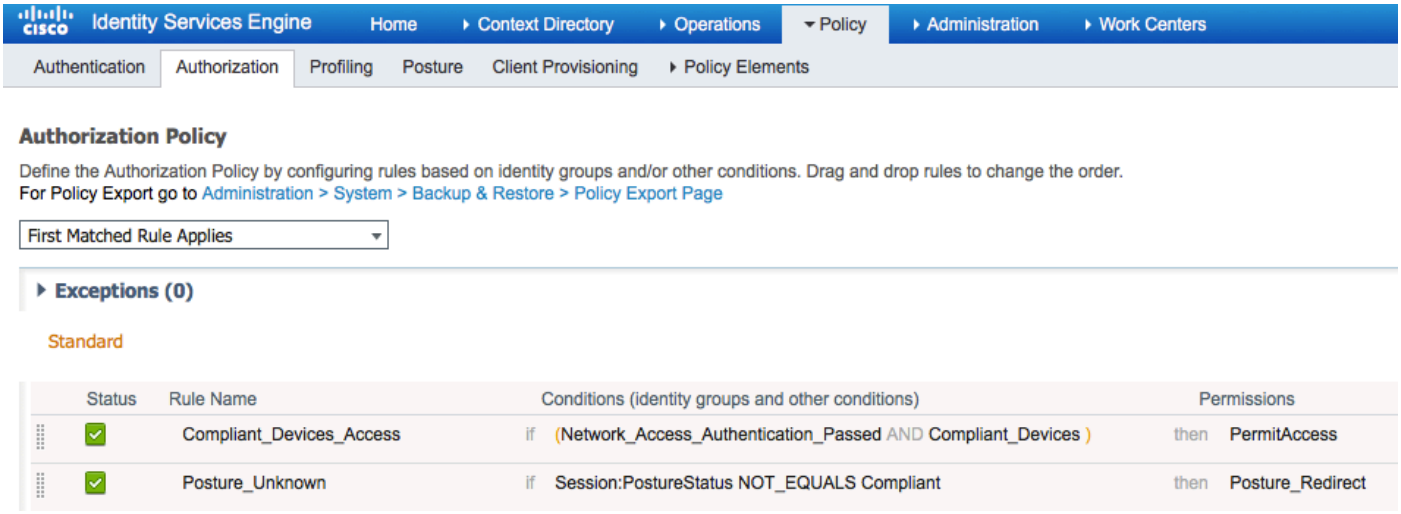
Etapa 4. Configurar regras da autorização

Da política > dos elementos da política > resulta > a autorização adiciona um perfil da autorização (nome: Posture_Redirect) que reorienta a um portal do abastecimento do cliente do padrão:



Nota: ACL_WEBAUTH_REDIRECT ACL é definido no ASA.

Da política > da autorização crie uma regra da autorização para a reorientação. Uma regra da autorização para dispositivos complacentes preconfigured no ISE:

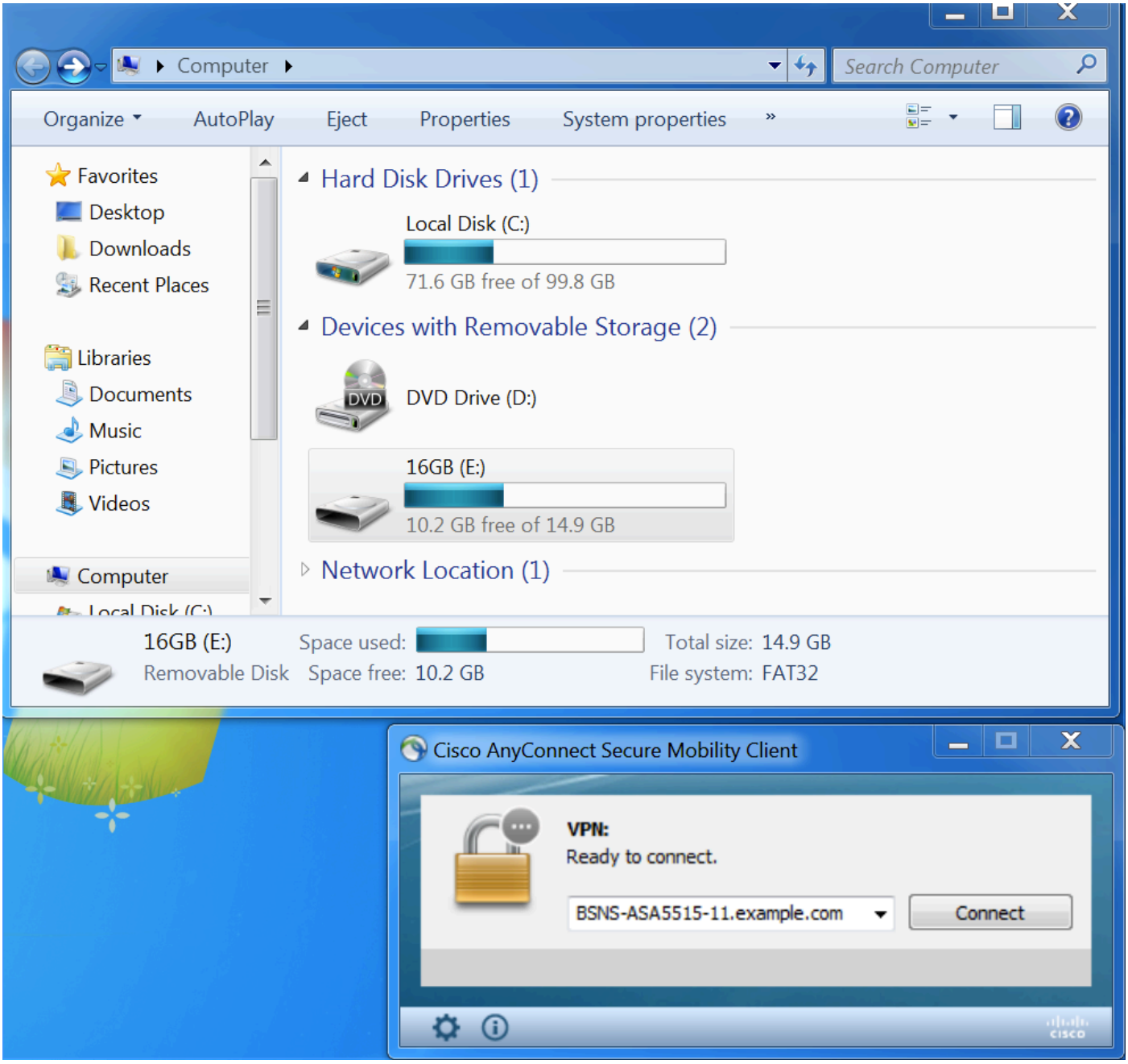


Se o valor-limite é complacente, o acesso direto está fornecido. Se o estado é desconhecido ou noncompliant, a reorientação para o abastecimento do cliente está retornada.

Verificar

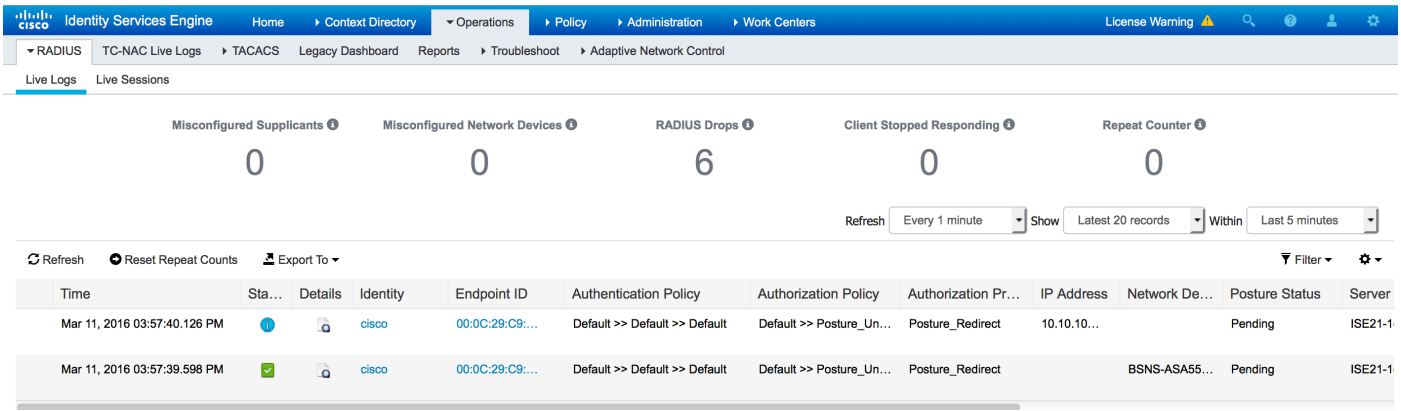
Antes do estabelecimento da sessão de VPN

O dispositivo USB obstruído dentro, e seu índice estão disponíveis para o usuário.



Estabelecimento da sessão de VPN

Durante a autenticação, o ISE retornará reorienta a lista de acesso e reorienta a URL como parte do perfil da autorização de Posture_Redirect



Uma vez que a sessão de VPN é estabelecida, o tráfego ASA do cliente obterá reorientado de

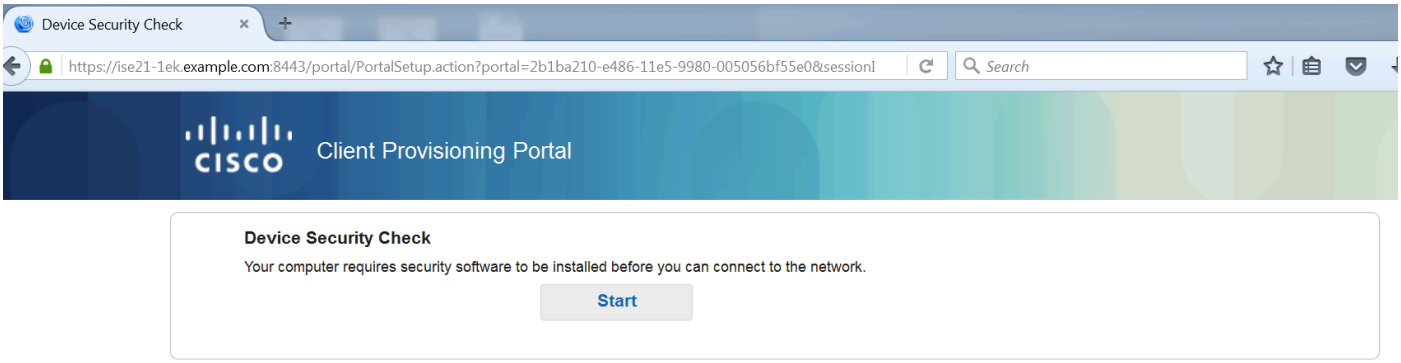
acordo com reorienta a lista de acesso:

```
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
```

Abastecimento do cliente

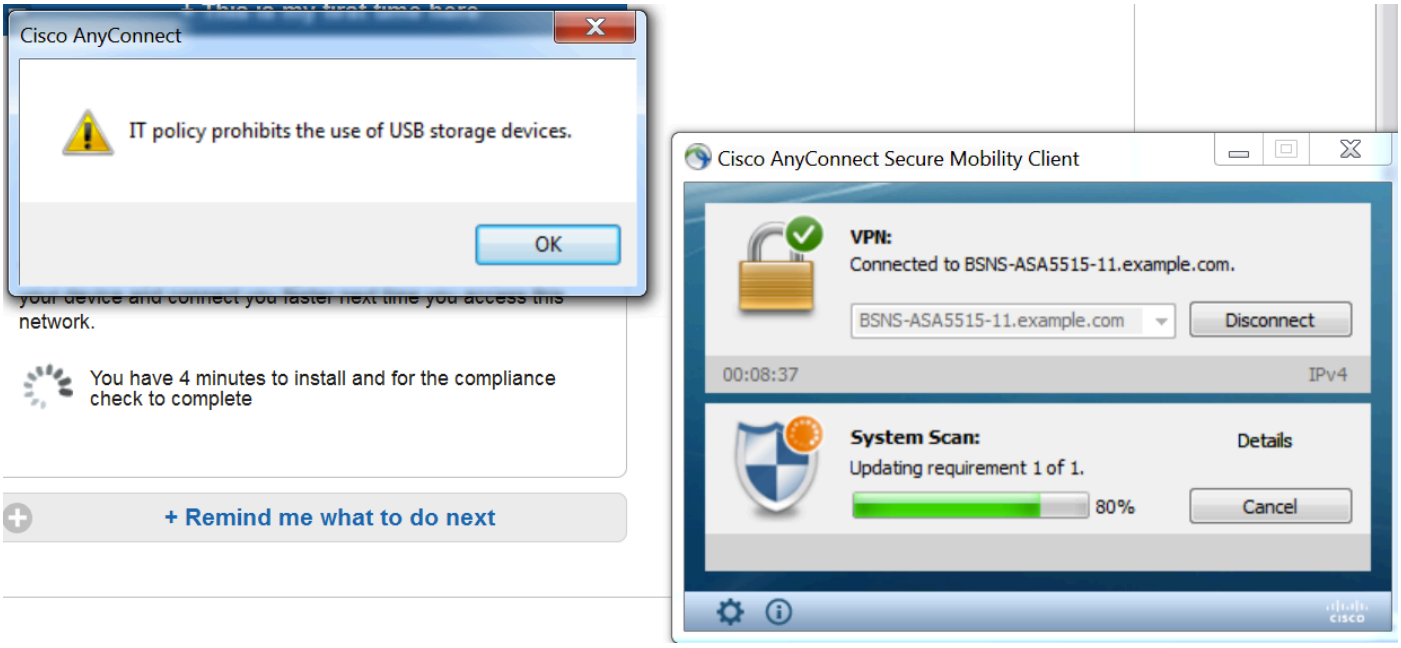
Nessa fase, o tráfego do web browser do valor-limite é reorientado ao ISE para o abastecimento do cliente:



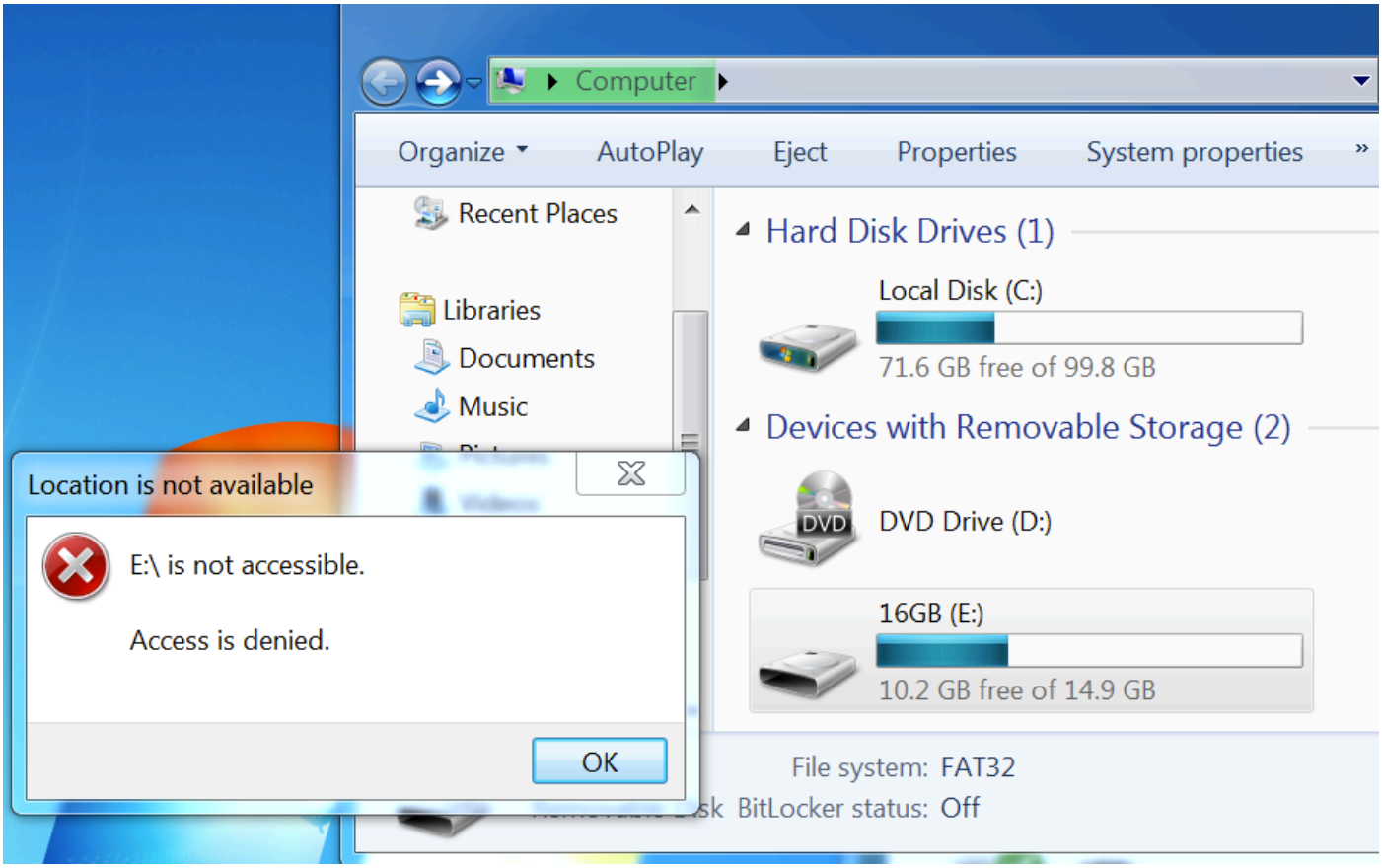
Se necessário, AnyConnect junto com o módulo da postura e da conformidade é atualizado.

Verificação da postura e CoA

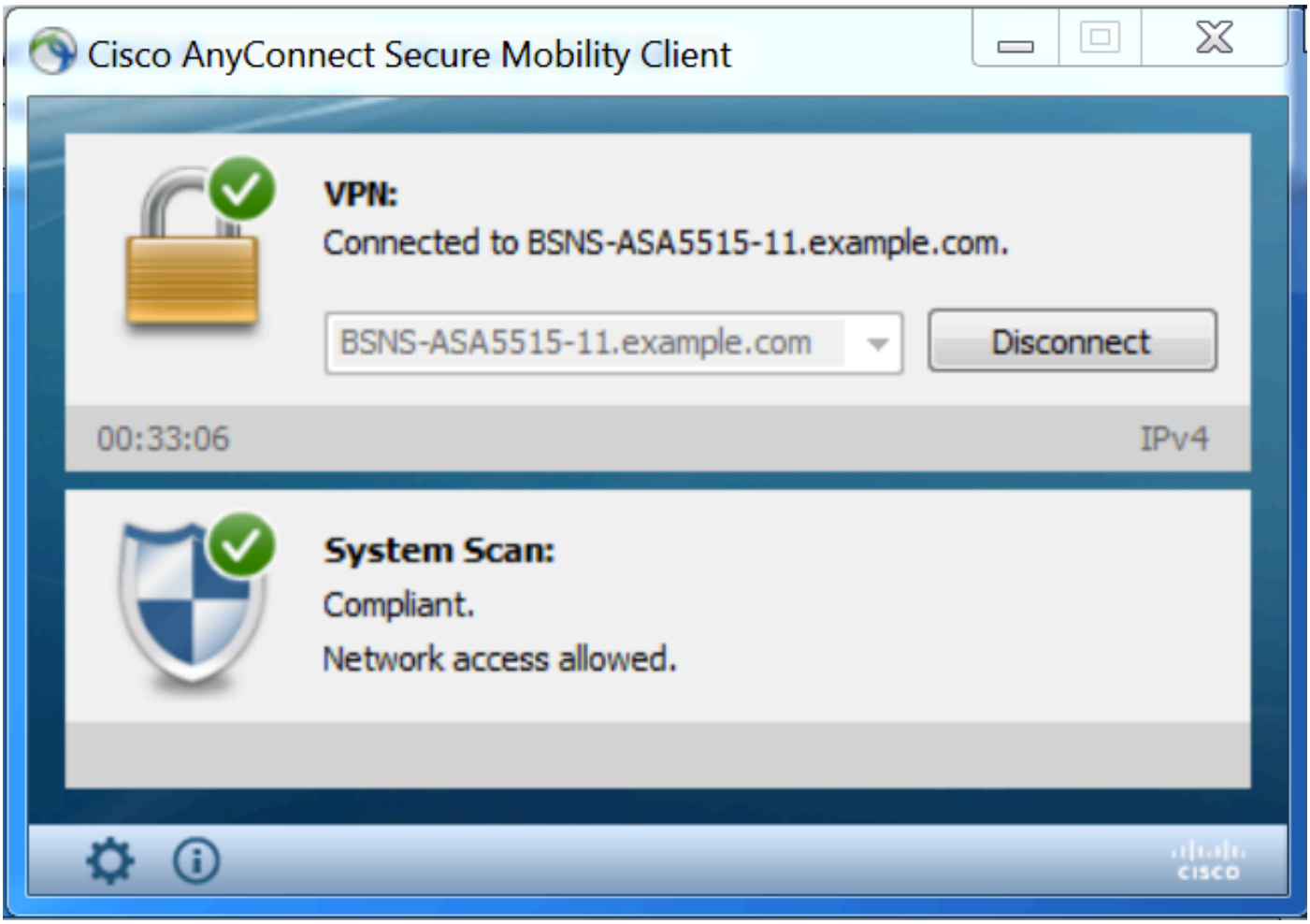
O módulo da postura é executado, descobre ISE (se pôde exigir para ter o registro DNS A para que enroll.cisco.com suceda), transfere e verifica condições da postura, ação nova do dispositivo do bloco USB OPSWAT v4. A mensagem configurada será indicada para o usuário:



Uma vez que a mensagem é confirmada, o dispositivo USB está já não disponível para o usuário:

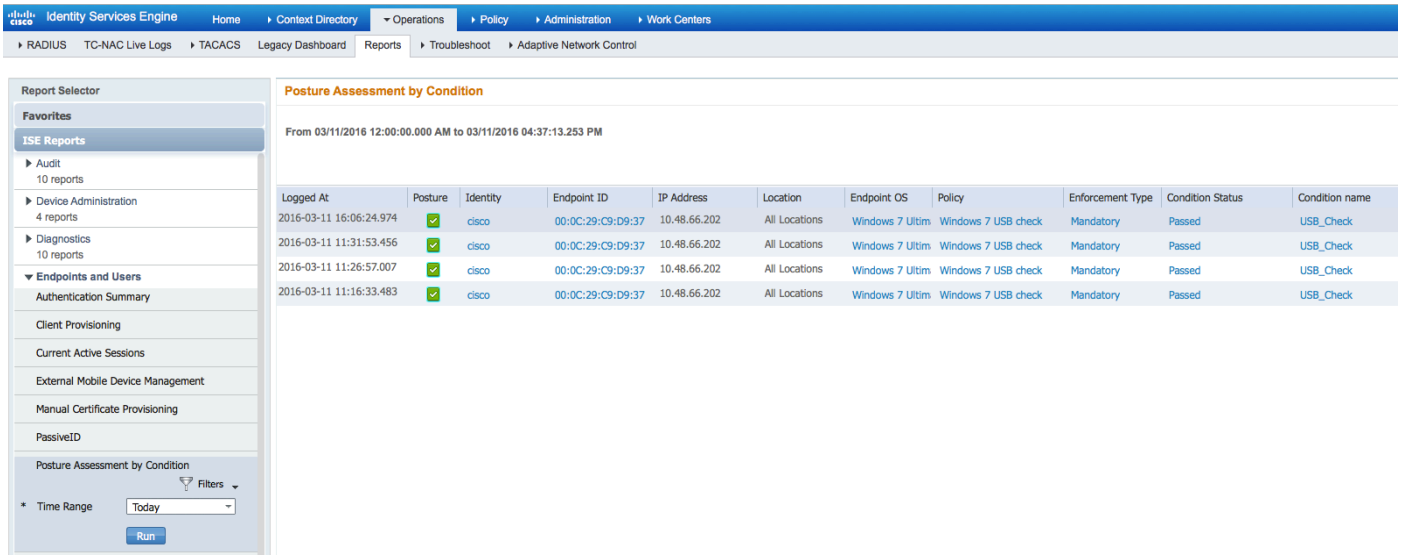


O ASA remove a reorientação ACL que fornece o acesso direto. AnyConnect relata a conformidade:

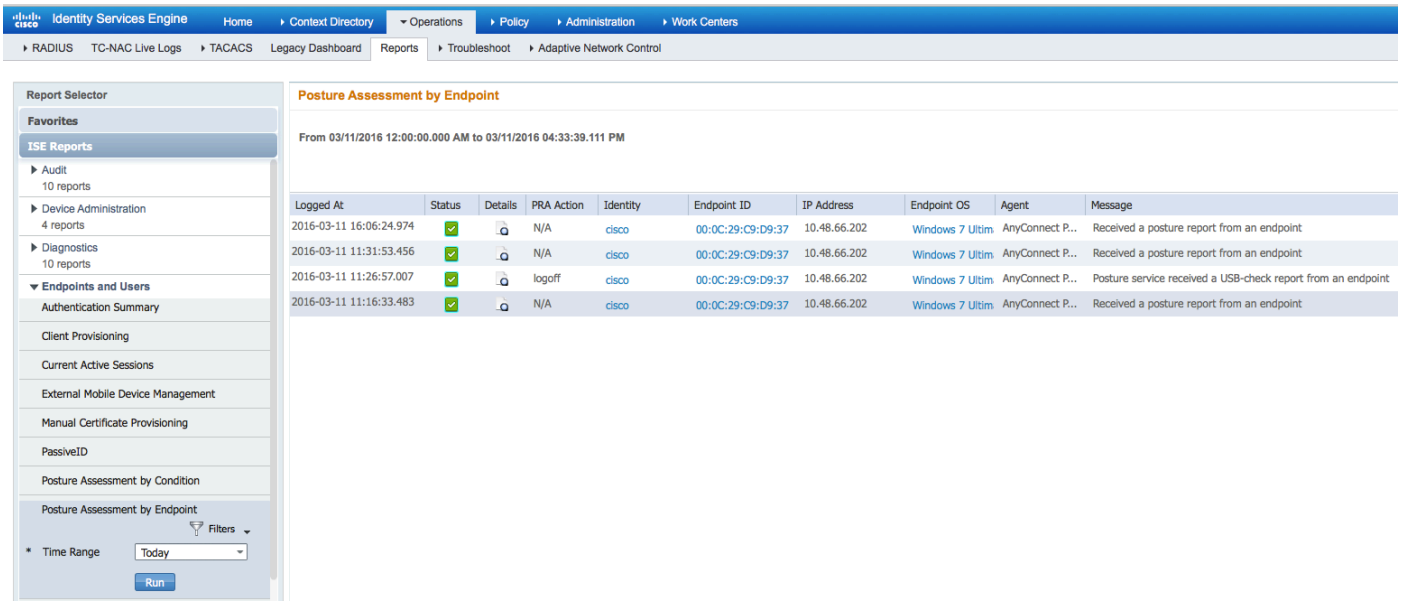


Igualmente os relatórios detalhados no ISE podem confirmar que as circunstâncias exigidas estão passadas.

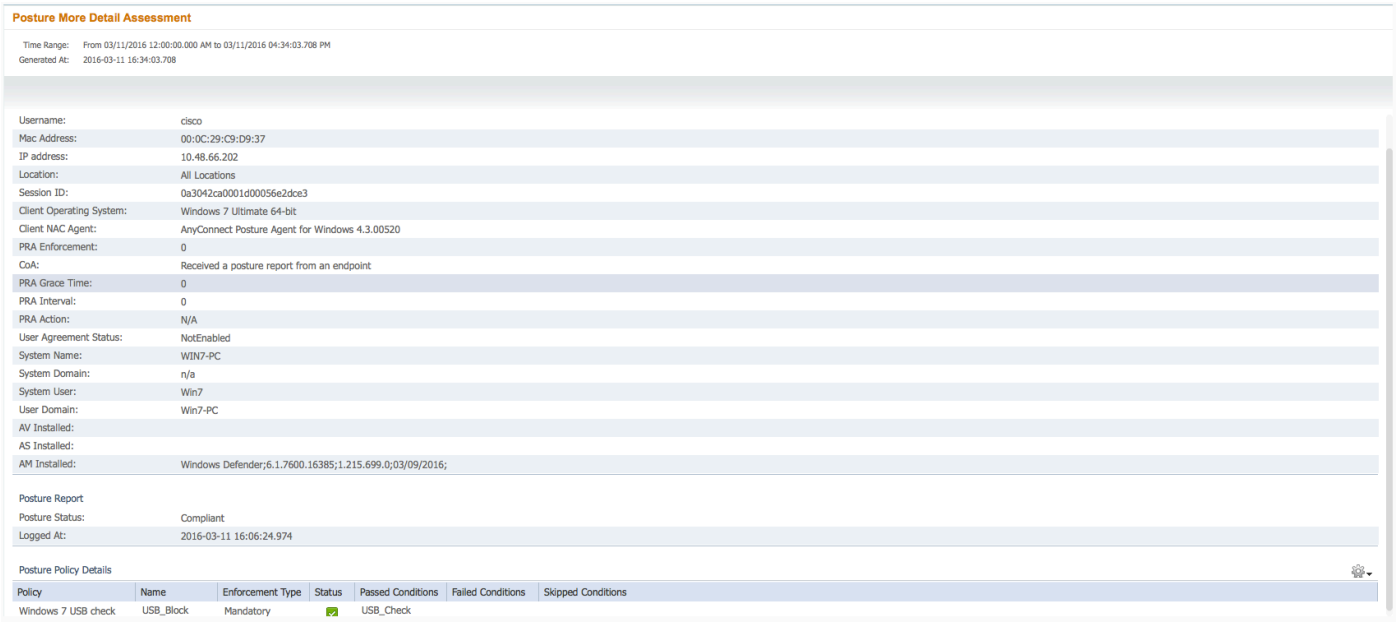
Avaliação da postura pela circunstância:



Avaliação da postura pelo valor-limite:



Detalhes de relatório do valor-limite:



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		

Troubleshooting

O ISE pode fornecer os detalhes nas circunstâncias de falha, ações deve ser tomado em conformidade.

Referências

- Como configurar um servidor externo para autorização de usuário de dispositivo de segurança
- Guia de configuração de CLI para VPN da Cisco ASA Series, 9.1
- Guia do administrador do Cisco Identity Services Engine, liberação 2.0
- Suporte Técnico e Documentação - Cisco Systems