

# Configurar a postura da versão 1.4 ISE com Microsoft WSUS

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Microsoft WSUS](#)

[ASA](#)

[ISE](#)

[Remediação da postura para WSUS](#)

[Exigência da postura para WSUS](#)

[Perfil de AnyConnect](#)

[Regras do abastecimento do cliente](#)

[Perfis da autorização](#)

[Regras da autorização](#)

[Verificar](#)

[PC com políticas actualizados GPO](#)

[Aprove uma atualização crítica no WSUS](#)

[Verifique o estado PC no WSUS](#)

[Sessão de VPN estabelecida](#)

[O módulo da postura recebe políticas do ISE e executa a remediação](#)

[Acesso de rede completo](#)

[Troubleshooting](#)

[Notas importantes](#)

[Detalhes da opção para a remediação WSUS](#)

[Serviço de Windows Update](#)

[Integração SCCM](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como configurar a funcionalidade da postura do Cisco Identity Services Engine (ISE) quando é integrado com os serviços da atualização do Microsoft Windows server (WSUS).

**Note:** Quando você alcança a rede, você está reorientado ao ISE para o abastecimento da versão 4.1 do Cliente de mobilidade Cisco AnyConnect Secure com um módulo da postura, que verifique o status de conformidade no WSUS e instale as atualizações necessárias para que a estação seja complacente. Uma vez que a estação é relatada como complacente, o ISE permite o acesso de rede completo.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Disposições, autenticação, e autorização de Cisco ISE
- O conhecimento básico sobre a maneira em que o ISE e Cisco AnyConnect posture o agente opera-se
- Configuração da ferramenta de segurança adaptável de Cisco (ASA)
- Conhecimento básico VPN e de 802.1x
- Configuração de Microsoft WSUS

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 7 de Microsoft Windows
- Versão 2012 de Microsoft Windows com versão 6.3 WSUS
- Versões ASA 9.3.1 de Cisco e mais atrasado
- Versões de software 1.3 de Cisco ISE e mais atrasado

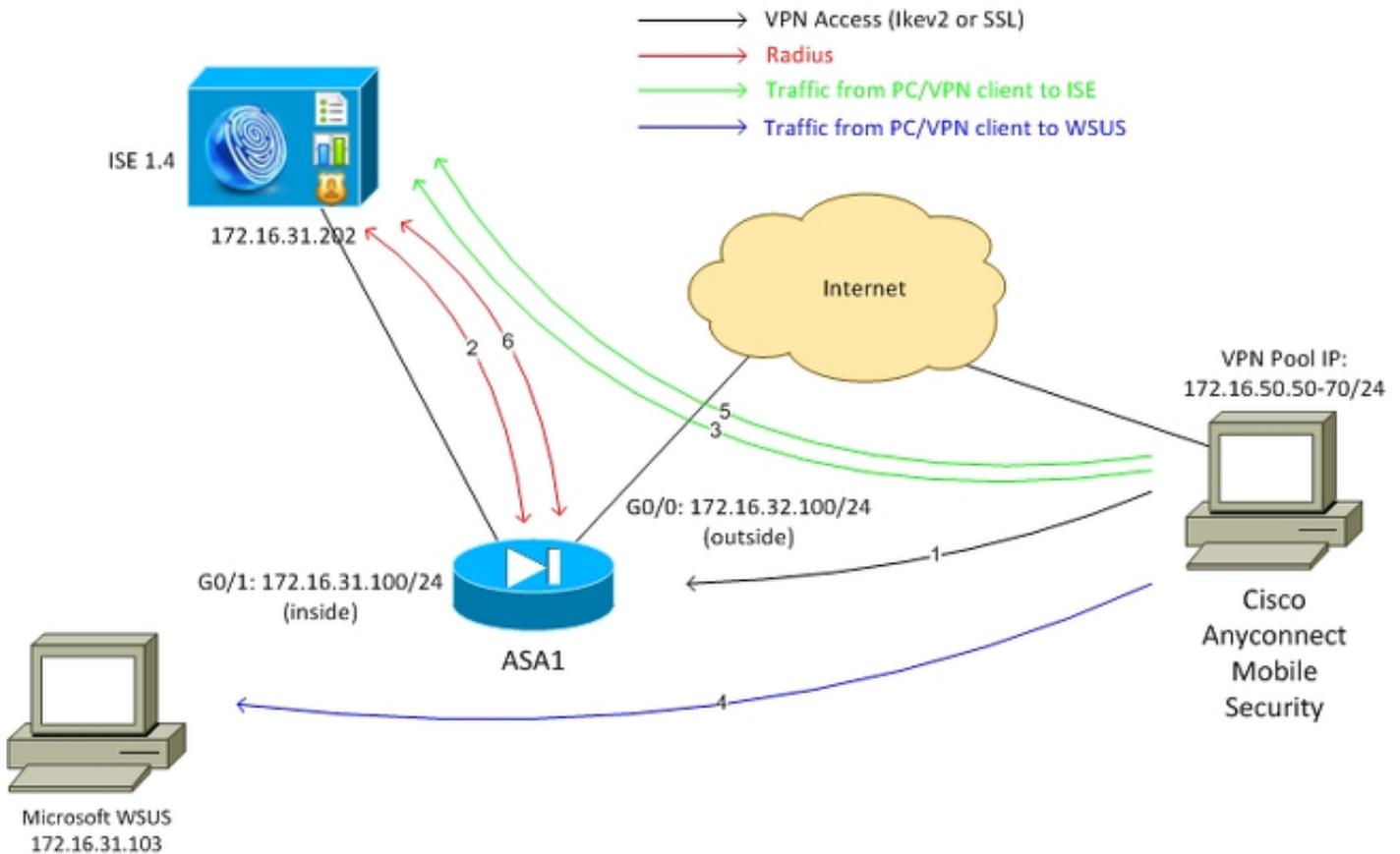
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar

Esta seção descreve como configurar o ISE e os elementos de rede relacionados.

## Diagrama de Rede

Esta é a topologia que é usada para os exemplos durante todo este documento:



Está aqui o fluxo de tráfego, como ilustrado no diagrama da rede:

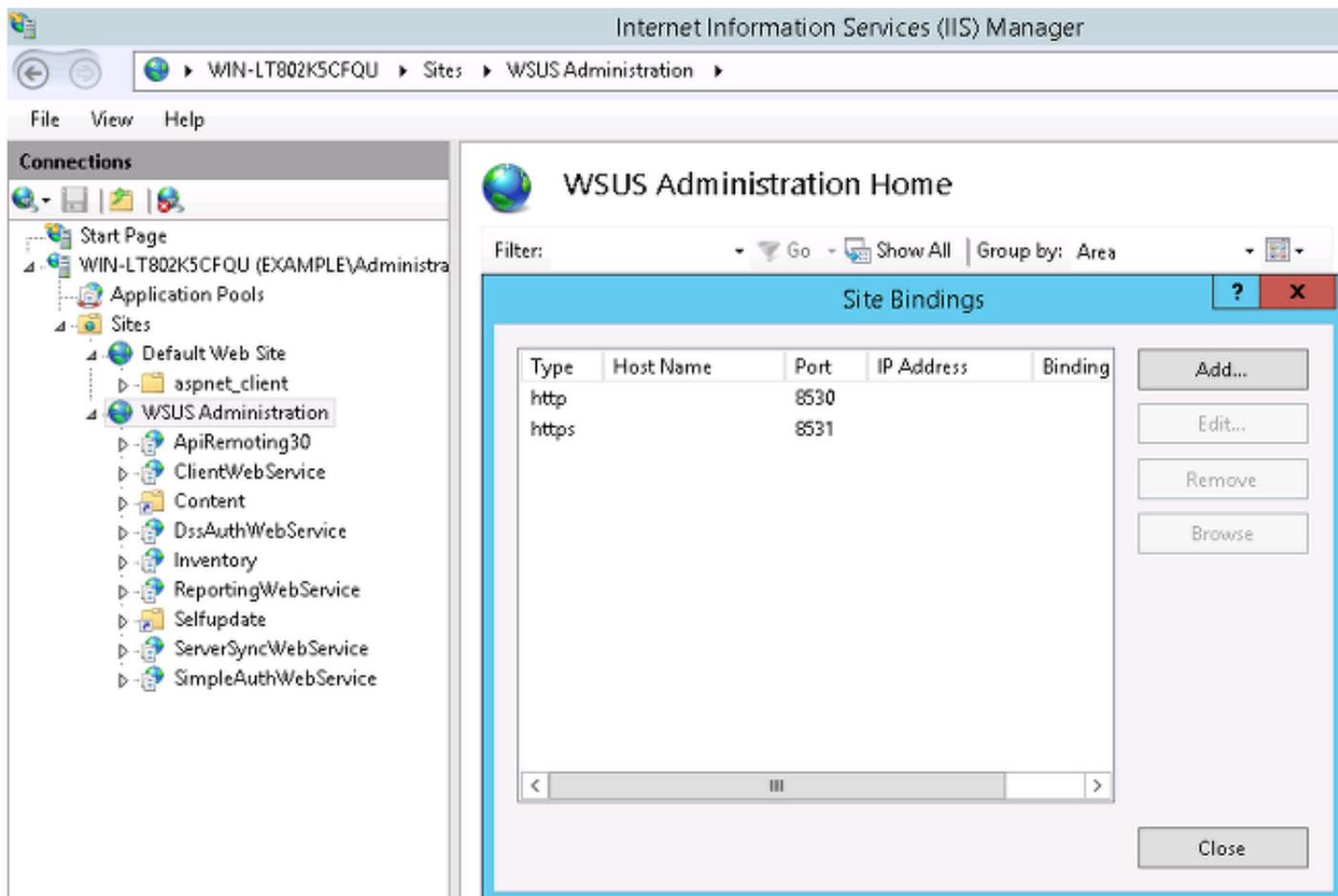
1. O usuário remoto conecta através de Cisco AnyConnect para o acesso VPN ao ASA. Este pode ser qualquer tipo de acesso unificado, tal como uma sessão prendida do desvio da autenticação 802.1x/MAC (MAB) que seja terminada no interruptor ou em uma sessão wireless que seja terminada no controlador do Wireless LAN (WLC).
2. Como parte do processo de autenticação, o ISE confirma que o estado da postura da estação final não é igual a complacente (regra da autorização de *ASA-VPN\_quarantine*) e que os atributos da reorientação estão retornados na mensagem da *aceitação de acesso do raio*. Em consequência, o ASA reorienta todo o tráfego de HTTP ao ISE.
3. O usuário abre um navegador da Web e incorpora todo o endereço. Após a reorientação ao ISE, o módulo da postura de Cisco AnyConnect 4 é instalado na estação. O módulo da postura transfere então as políticas do ISE (exigência para WSUS).
4. O módulo da postura procura por Microsoft WSUS, e executa a remediação.
5. Após a remediação bem sucedida, o módulo da postura envia um relatório ao ISE.
6. O ISE emite uma mudança do raio da autorização (CoA) que fornece o acesso de rede completo a um usuário complacente VPN (regra da autorização de *ASA-VPN\_compliant*).

**Note:** Para que a remediação trabalhe (a capacidade para instalar atualizações de Microsoft Windows em um PC), o usuário deve ter direitos administrativos locais.

## Microsoft WSUS

**Note:** Uma configuração detalhada do WSUS é fora do âmbito deste documento. Para detalhes, refira os [serviços da atualização de Windows Server da distribuição em sua documentação Microsoft da organização](#).

O serviço WSUS é distribuído através da porta TCP padrão 8530. É importante recordar que para a remediação, outras portas estão usadas igualmente. Eis porque é seguro adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT de WSUS ao Access Control List da reorientação (ACL) no ASA (descrito mais tarde neste documento).

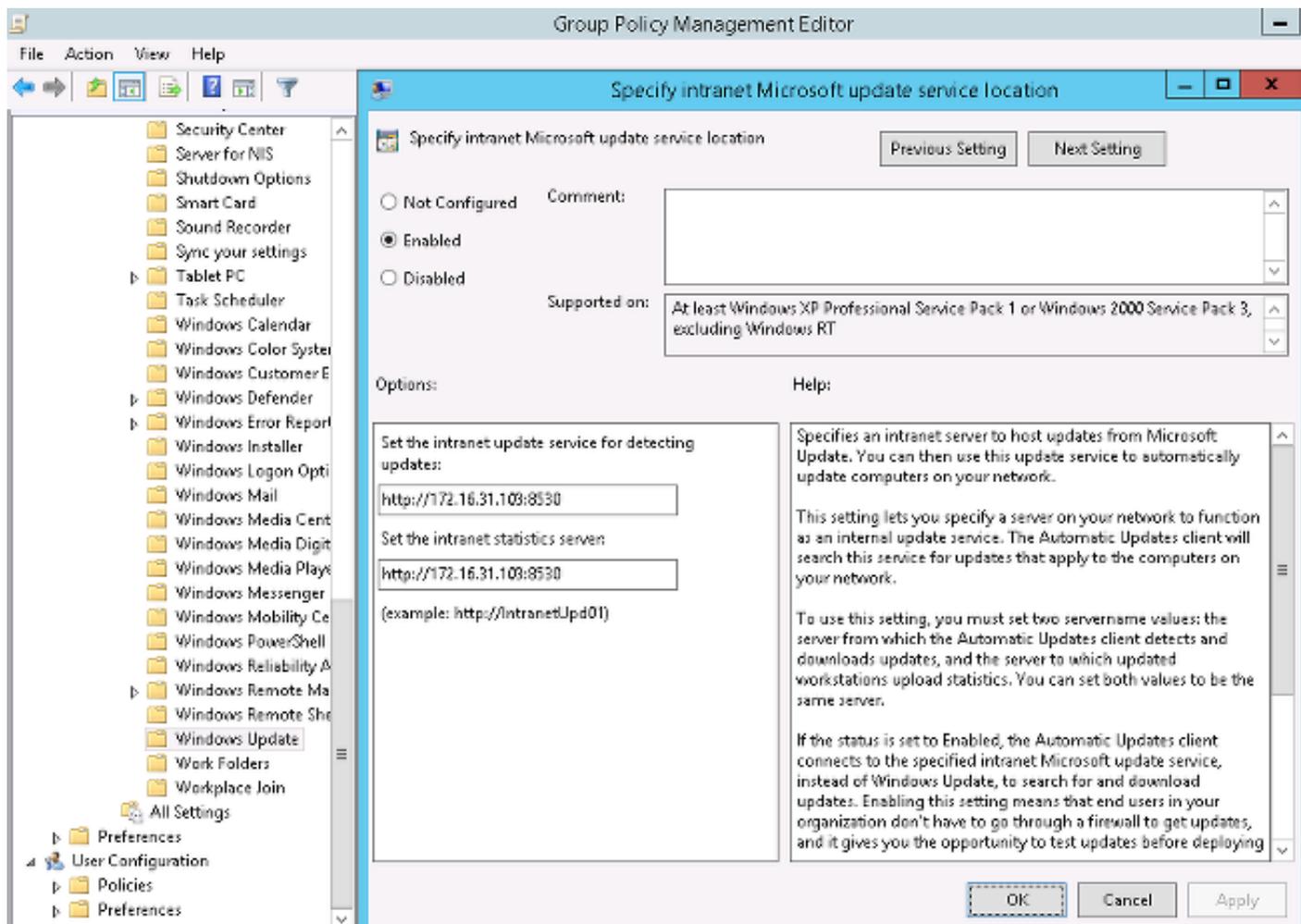


The screenshot shows the Internet Information Services (IIS) Manager interface. The left pane displays the 'Connections' tree with 'WSUS Administration' selected. The right pane shows the 'WSUS Administration Home' page with the 'Site Bindings' dialog box open. The dialog box contains a table with the following data:

Type	Host Name	Port	IP Address	Binding
http		8530		
https		8531		

Buttons for 'Add...', 'Edit...', 'Remove', 'Browse', and 'Close' are visible on the right side of the dialog box.

A política do grupo para o domínio é configurada para atualizações e pontos de Microsoft Windows ao server local WSUS:



Estas são as atualizações recomendadas que são permitidas para as políticas granuladas que são baseadas em níveis diferentes da severidade:

📁 **Windows Update**

**Turn on recommended updates via Automatic Updates**

Edit [policy setting](#).

Requirements:  
At least Windows Vista

Description:  
Specifies whether Automatic Updates will deliver both important as well as recommended updates from the Windows Update update service.

When this policy is enabled, Automatic Updates will install recommended updates as well as important updates from Windows Update update service.

When disabled or not configured Automatic Updates will continue to deliver important updates if it is already configured to do so.

Setting	State
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured
Do not adjust default option to 'Install Updates and Shut Do...	Not configured
Enabling Windows Update Power Management to automati...	Not configured
Always automatically restart at the scheduled time	Not configured
Configure Automatic Updates	Enabled
Specify intranet Microsoft update service location	Enabled
Automatic Updates detection frequency	Enabled
Do not connect to any Windows Update Internet locations	Not configured
Allow non-administrators to receive update notifications	Not configured
Turn on Software Notifications	Not configured
Allow Automatic Updates immediate installation	Not configured
<b>Turn on recommended updates via Automatic Updates</b>	<b>Enabled</b>
No auto-restart with logged on users for scheduled automat...	Not configured
Re-prompt for restart with scheduled installations	Not configured
Delay Restart for scheduled installations	Not configured
Reschedule Automatic Updates scheduled installations	Not configured
Enable client-side targeting	Enabled
Allow signed updates from an intranet Microsoft update ser...	Not configured

A escolha de objetivos do lado do cliente permite a flexibilidade distante maior. O ISE pode usar as políticas da postura que são baseadas nos recipientes diferentes do computador do microsoft active directory (AD). O WSUS pode aprovar as atualizações que são baseadas nesta sociedade.

## ASA

O acesso simples do secure sockets layer (SSL) VPN para o usuário remoto é empregado (os detalhes de que seja fora do âmbito deste documento).

Está aqui um exemplo de configuração:

```
interface GigabitEthernet0/0
  nameif outside
  security-level 10
  ip address 172.16.32.100 255.255.255.0

interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.31.100 255.255.255.0

aaa-server ISE protocol radius
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
  key cisco

webvpn
  enable outside
  anyconnect-essentials
  anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable

group-policy POLICY internal
group-policy POLICY attributes
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group SSLVPN type remote-access
tunnel-group SSLVPN general-attributes
  address-pool POOL-VPN
  authentication-server-group ISE
  accounting-server-group ISE
  default-group-policy POLICY

ip local pool POOL-VPN 172.16.50.50-172.16.50.60 mask 255.255.255.0
```

É importante configurar uma lista de acesso no ASA, que é usado a fim determinar o tráfego que deve ser reorientado ao ISE (para os usuários que não são ainda complacentes):

```
access-list Posture-redirect extended deny udp any any eq domain
access-list Posture-redirect extended deny ip any host 172.16.31.103
access-list Posture-redirect extended deny ip any host 172.16.31.202
access-list Posture-redirect extended deny icmp any any
access-list Posture-redirect extended permit tcp any any eq www
```

Somente o Domain Name System (DNS), o ISE, WSUS, e o tráfego do Internet Control Message

Protocol (ICMP) são permitidos usuários NON-complacentes. Todo o outro tráfego (HTTP) é reorientado ao ISE para o abastecimento de AnyConnect 4, que é responsável para a postura e a remediação.

## ISE

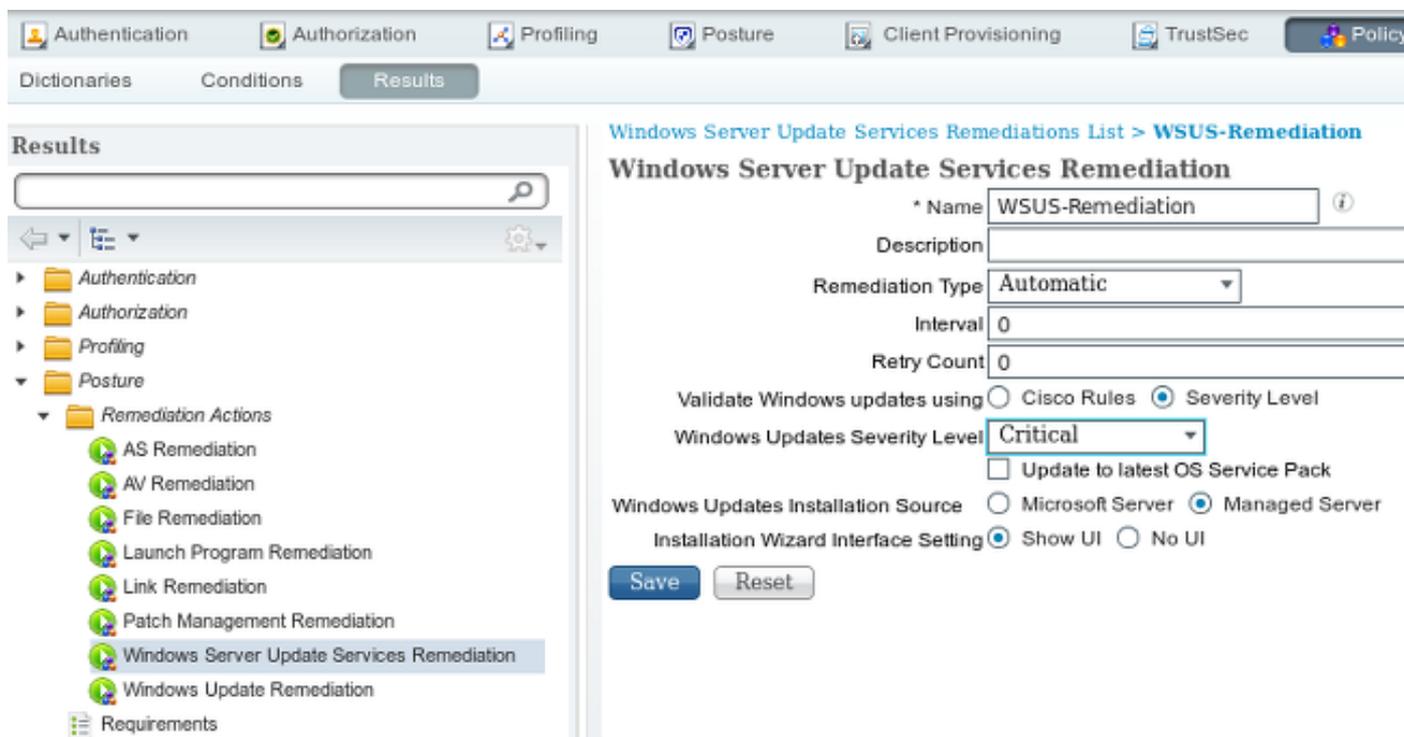
**Note:** O abastecimento e a postura de AnyConnect 4 são fora do âmbito deste documento. Refira a [integração de AnyConnect 4.0 com exemplo de configuração da versão 1.3 ISE](#) para mais detalhes, como como configurar o ASA como um dispositivo de rede e instalar o aplicativo de Cisco AnyConnect 7.

### Posture a remediação para WSUS

Termine estas etapas a fim configurar a remediação da postura para WSUS:

1. Navegue à **política > às circunstâncias > à remediação das ações da postura > da remediação > dos serviços da atualização de Windows Server** a fim criar uma regra nova.
2. Verifique que o ajuste das *atualizações de Microsoft Windows* está ajustado ao **nível de seriedade**. Esta parte é responsável para a detecção se o processo da remediação é iniciado.

O agente da atualização de Microsoft Windows então conecta ao WSUS e verifica se haja alguma atualização *crítica* para esse PC que esperar a instalação:



The screenshot displays the Cisco ISE Policy Editor interface. The top navigation bar includes tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy. The 'Results' tab is active. On the left, a tree view shows the configuration hierarchy: Authentication, Authorization, Profiling, Posture, Remediation Actions, AS Remediation, AV Remediation, File Remediation, Launch Program Remediation, Link Remediation, Patch Management Remediation, Windows Server Update Services Remediation (highlighted), Windows Update Remediation, and Requirements. The main area shows the configuration for 'Windows Server Update Services Remediation'. The configuration includes: Name: WSUS-Remediation; Description: (empty); Remediation Type: Automatic; Interval: 0; Retry Count: 0; Validate Windows updates using: Severity Level (selected); Windows Updates Severity Level: Critical; Update to latest OS Service Pack: (unchecked); Windows Updates Installation Source: Managed Server (selected); Installation Wizard Interface Setting: Show UI (selected). 'Save' and 'Reset' buttons are visible at the bottom.

### Exigência da postura para WSUS

Navegue à **política > às circunstâncias > à postura > às exigências** a fim criar uma regra nova. A

regra usa uma condição do manequim chamada *pr\_WSUSRule*, assim que significa que o WSUS está contactado a fim verificar para ver se há a condição quando a remediação é necessária (atualizações *críticas*).

Uma vez que esta circunstância é estada conforme, o WSUS instala as atualizações que foram configuradas para esse PC. Estes podem incluir qualquer tipo de atualizações, e igualmente aqueles com severidade mais baixa nivelam:

Requirements			
Name	Operating Systems	Conditions	Remediation Actions
Any_AS_Definition_Mac	for Mac OSX	met if ANY_as_mac_def	else AnyASDefRemediationMac
Any_AV_Installation_Win	for Windows All	met if ANY_av_win_inst	else Message Text Only
Any_AV_Definition_Win	for Windows All	met if ANY_av_win_def	else AnyAVDefRemediationWin
Any_AS_Installation_Win	for Windows All	met if ANY_as_win_inst	else Message Text Only
Any_AS_Definition_Win	for Windows All	met if ANY_as_win_def	else AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	met if ANY_av_mac_inst	else Message Text Only
Any_AV_Definition_Mac	for Mac OSX	met if ANY_av_mac_def	else AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	met if ANY_as_mac_inst	else Message Text Only
WSUS	for Windows All	met if pr_WSUSRule	else WSUS-Remediation

## Perfil de AnyConnect

Configurar o perfil do módulo da postura, junto com o perfil de AnyConnect 4 (como descrito na [integração de AnyConnect 4.0 com exemplo de configuração da versão 1.3 ISE](#)):

The screenshot shows the Cisco ISE Policy Elements configuration interface. The top navigation bar includes Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The left sidebar shows a tree view with folders for Authentication, Authorization, Profiling, Posture, Client Provisioning, Resources, and TrustSec. The main content area is titled "AnyConnect Configuration > AnyConnect Configuration".

Configuration details include:

- \* Select AnyConnect Package: AnyConnectDesktopWindows 4.1.2011.0
- \* Configuration Name: AnyConnect Configuration
- Description: (Empty text box)
- \* Compliance Module: AnyConnectComplianceModuleWindows 3.6.9

**AnyConnect Module Selection**

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

**Profile Selection**

- \* ISE Posture: AC4 profile
- VPN: (Empty dropdown)

## Regras do abastecimento do cliente

Uma vez que o perfil de AnyConnect está pronto, pode ser provido da política de *abastecimento do cliente*:

The screenshot shows the Cisco ISE Client Provisioning Policy configuration page. The top navigation bar includes Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The left sidebar shows a tree view with folders for Authentication, Authorization, Profiling, Posture, Client Provisioning, Resources, and TrustSec. The main content area is titled "Client Provisioning Policy".

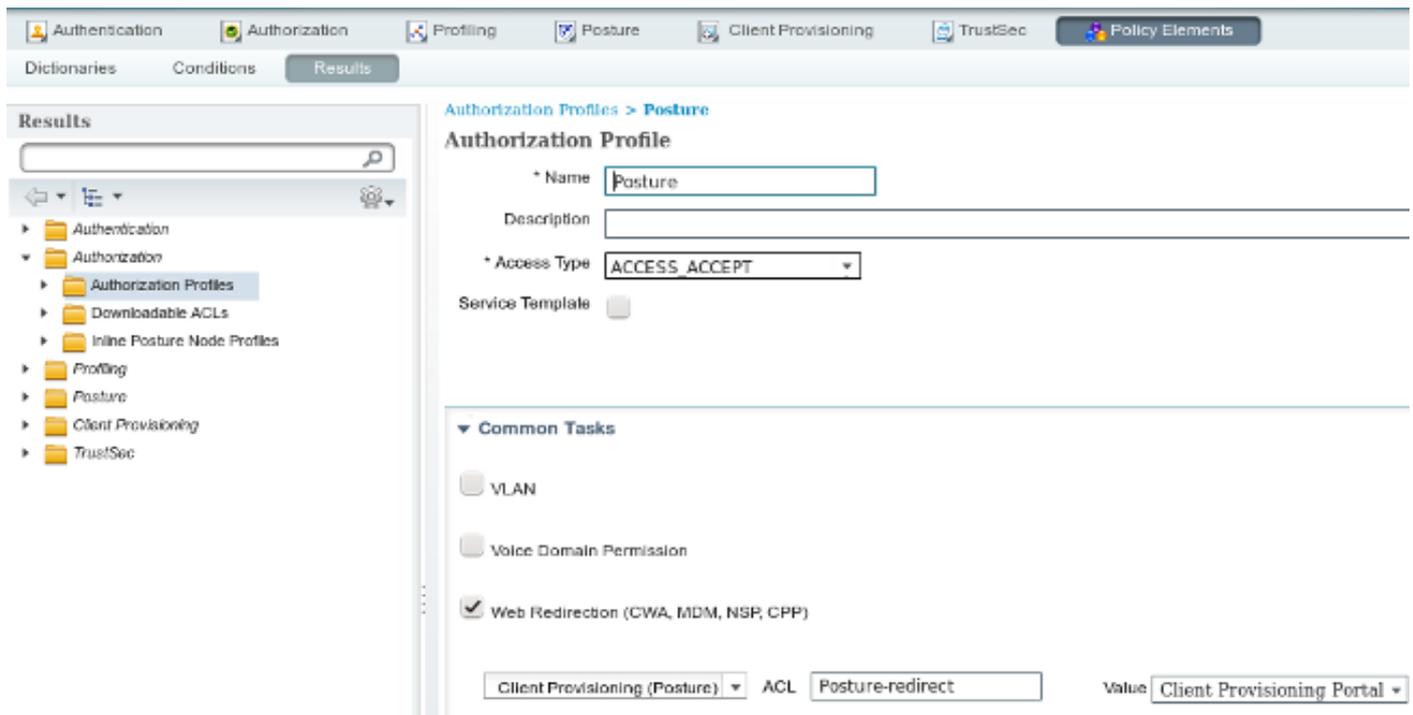
Define the Client Provisioning Policy to determine what users will receive upon login and user session initialization:  
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AC4	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration

O aplicativo inteiro, junto com a configuração, é instalado no valor-limite, que é reorientado à página do portal do abastecimento do cliente. AnyConnect 4 pôde ser promovido e um módulo adicional (postura) ser instalado.

## Perfis da autorização

Crie um perfil da autorização para a reorientação ao perfil do abastecimento do cliente:



## Regras da autorização

Esta imagem mostra as regras da autorização:

### 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
✓	ASA-VPN_quarantine	if (Session.PostureStatus EQUALS Unknown OR Session.PostureStatus EQUALS NonCompliant)	then Posture
✓	ASA-VPN_compliant	if Session.PostureStatus EQUALS Compliant	then PermitAccess

Pela primeira vez, a regra de *ASA-VPN\_quarantine* é usada. Em consequência, o perfil da autorização da *postura* é retornado, e o valor-limite é reorientado ao portal do abastecimento do cliente para o abastecimento de AnyConnect 4 (com módulo da postura).

Uma vez que complacente, a regra de *ASA-VPN\_compliant* é usada e o acesso de rede completo é permitido.

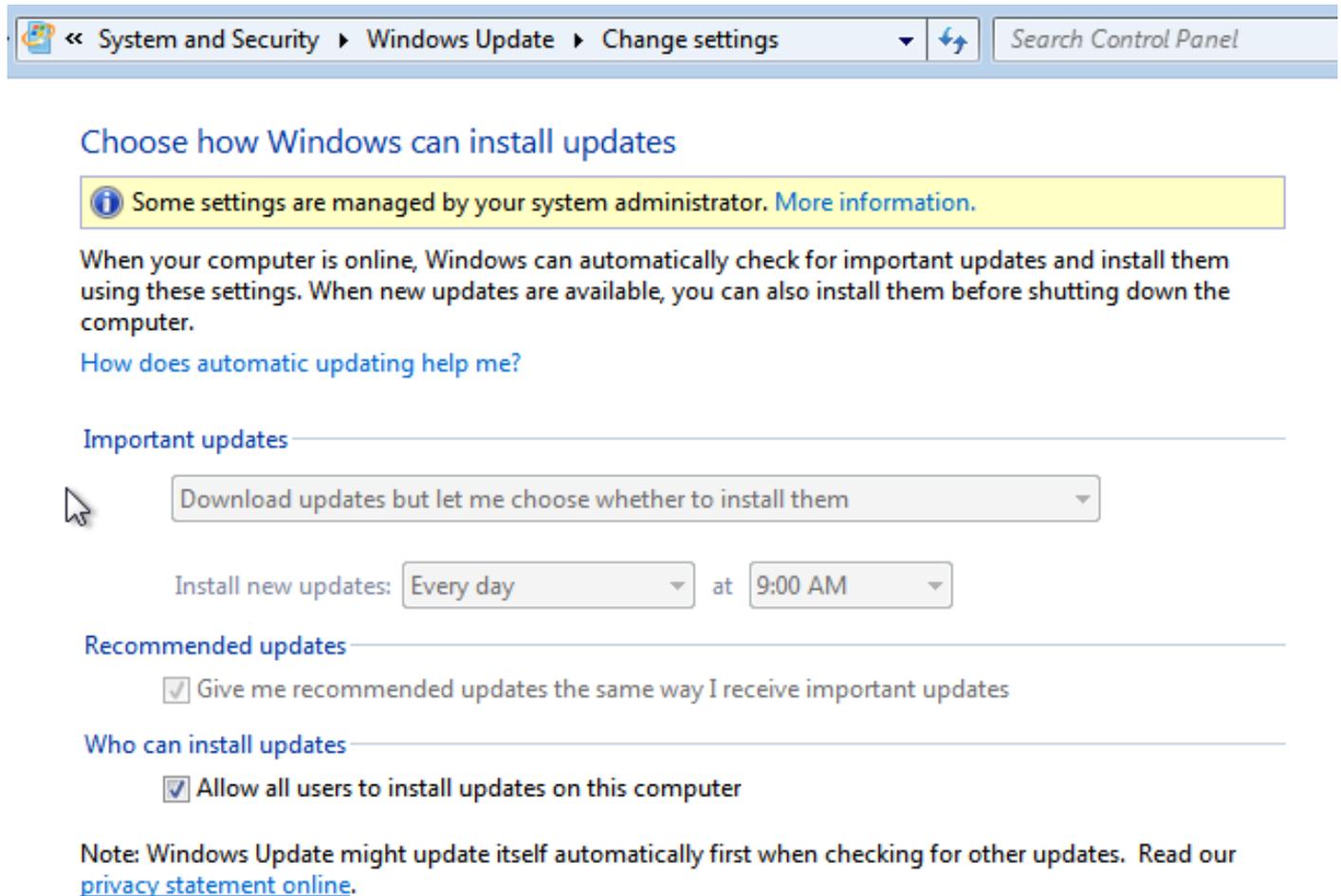
## Verificar

Esta seção fornece a informação que você pode usar a fim verificar que você configuração trabalha corretamente.

## PC com políticas actualizados GPO

As políticas de domínio com a configuração WSUS devem ser introduzidas após os logs PC no domínio. Isto pode ocorrer antes que a sessão de VPN esteja estabelecida (fora da faixa) ou em seguida se o *começo antes que a funcionalidade do fazer logon* esteja usada (ele pode igualmente ser usado para o 802.1x prendido/acesso Wireless).

Uma vez que o cliente de Microsoft Windows tem a configuração correta, este pode ser refletido dos ajustes de Windows Update:



The screenshot shows the Windows Update settings page in the Control Panel. The breadcrumb navigation at the top reads: < System and Security > Windows Update > Change settings. A search bar on the right says 'Search Control Panel'. The main heading is 'Choose how Windows can install updates'. A yellow warning box states: 'Some settings are managed by your system administrator. More information.' Below this, a text block explains that Windows can automatically check for updates. A link asks 'How does automatic updating help me?'. The 'Important updates' section has a dropdown menu set to 'Download updates but let me choose whether to install them'. Below that, 'Install new updates' is set to 'Every day' at '9:00 AM'. The 'Recommended updates' section has a checked checkbox for 'Give me recommended updates the same way I receive important updates'. The 'Who can install updates' section has a checked checkbox for 'Allow all users to install updates on this computer'. A note at the bottom states: 'Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.'

Se necessário, um grupo o objeto da política que (GPO) refresca e descoberta do servidor IP Phone Agent da atualização de Microsoft Windows pode ser usado:

```
C:\Users\Administrator>gpupdate /force
Updating Policy...
```

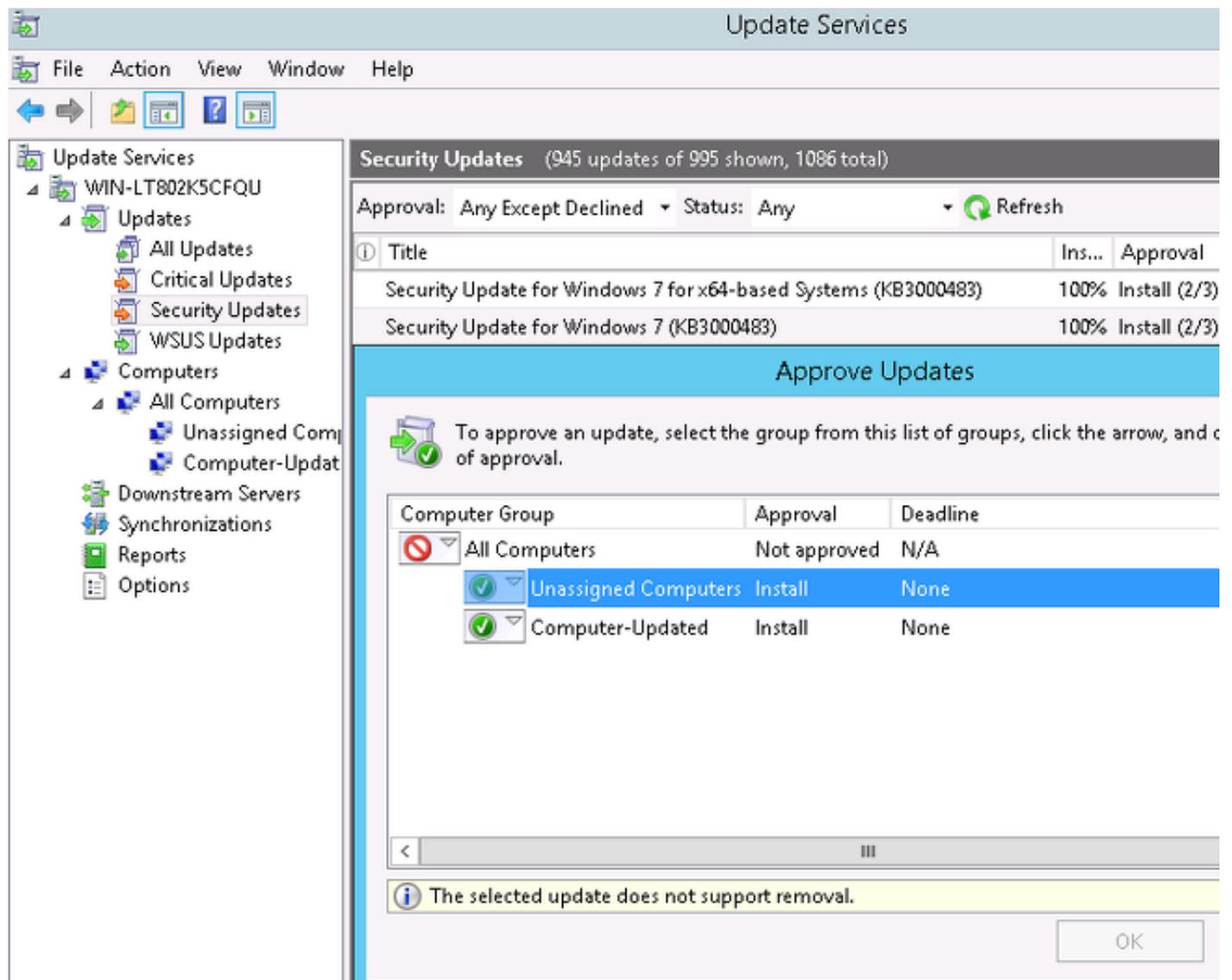
```
User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

```
C:\Users\Administrator>wuauclt.exe /detectnow
```

```
C:\Users\Administrator>
```

## Aprove uma atualização crítica no WSUS

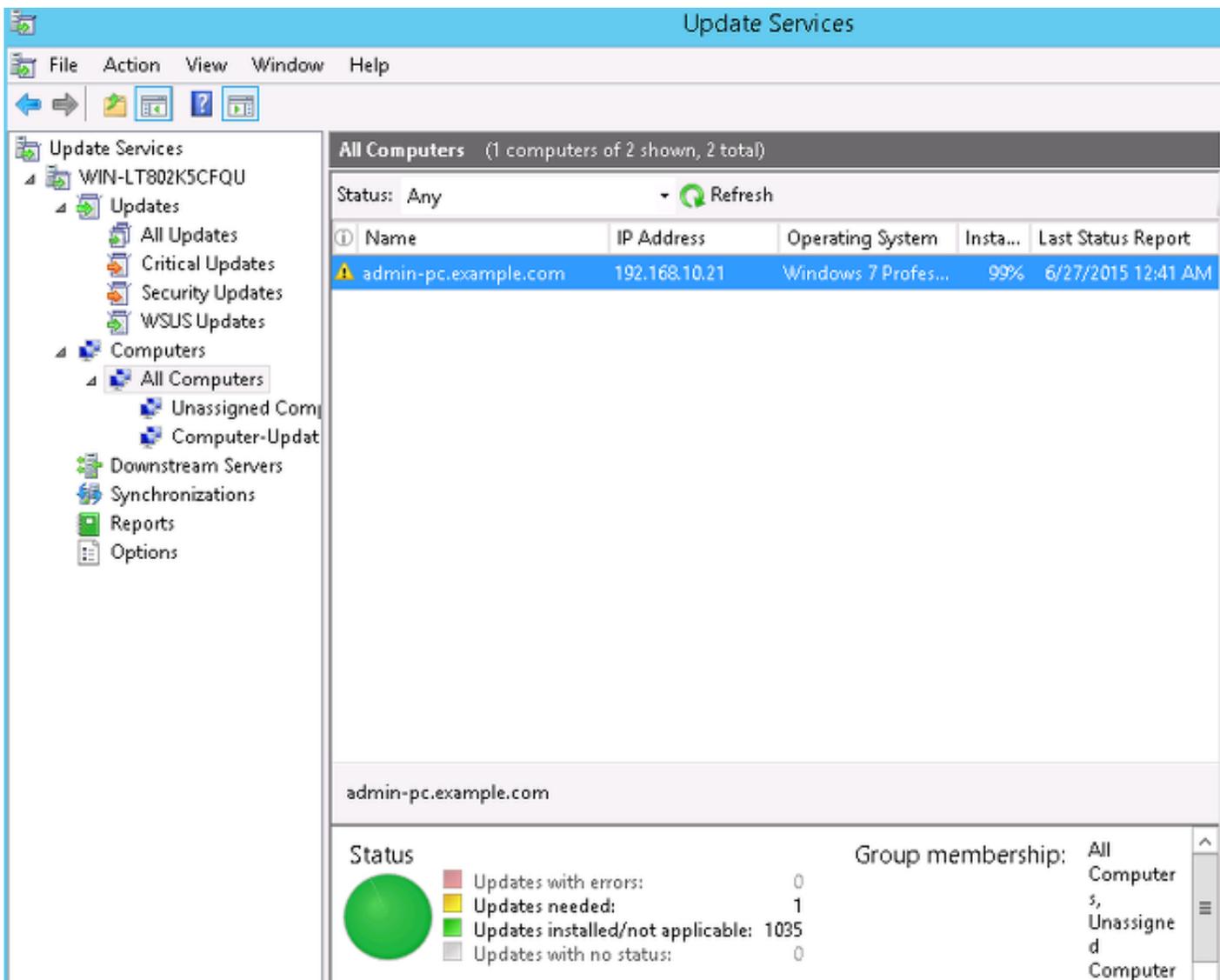
O processo de aprovação pode tirar proveito da escolha de objetivos da site de cliente:



Envie novamente o relatório com *wuauctl* se necessário.

## Verifique o estado PC no WSUS

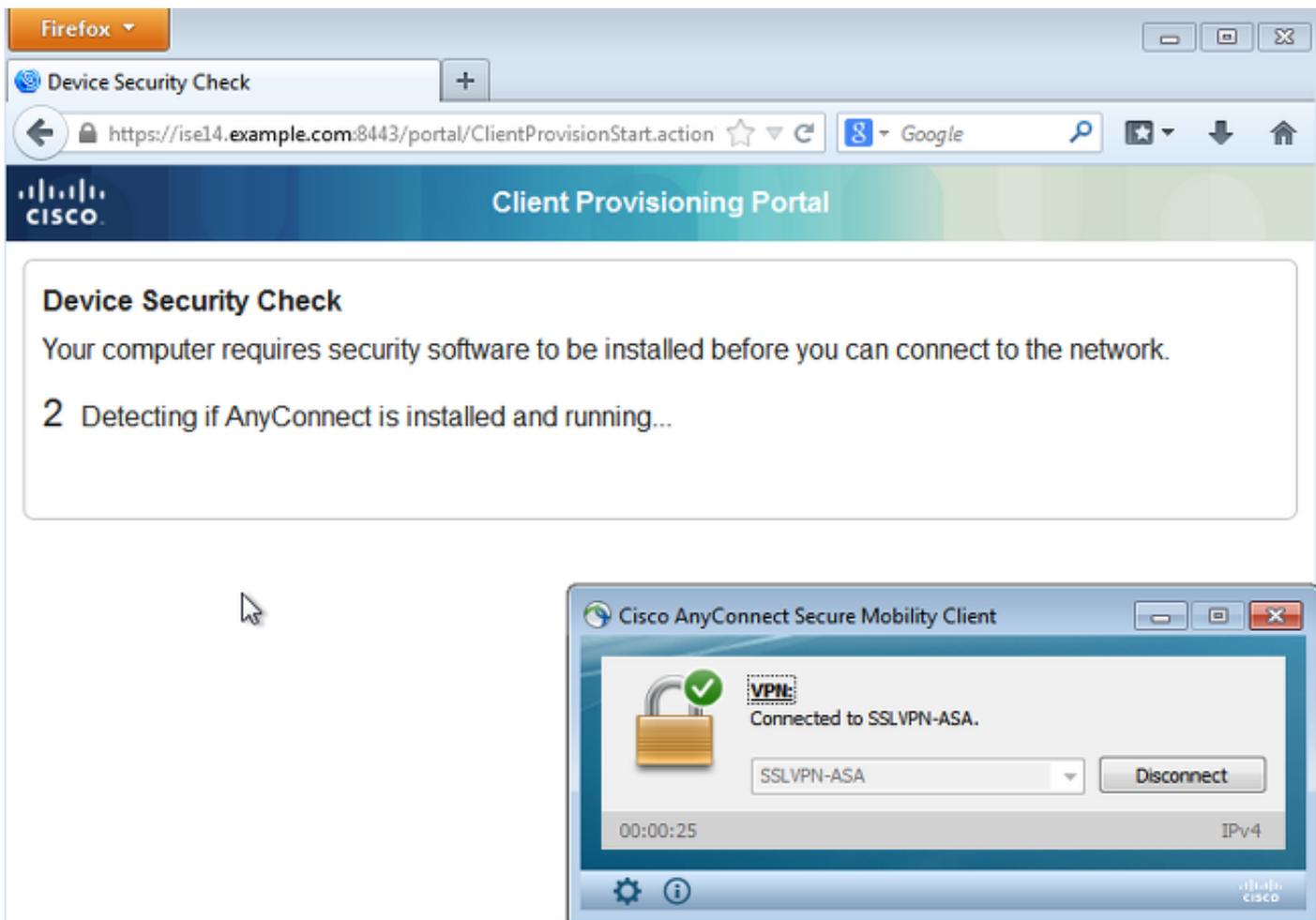
Esta imagem mostra como verificar o estado PC no WSUS:



Uma atualização deve ser instalada para o seguinte refresca com o WSUS.

## Sessão de VPN estabelecida

Depois que a sessão de VPN é estabelecida, a regra da autorização de *ASA-VPN\_quarantine* ISE está usada, que retorna o perfil da autorização da *postura*. Em consequência, o tráfego de HTTP do valor-limite é reorientado para abastecimentos do módulo da atualização e da postura de AnyConnect os 4:



Neste momento, o estado da sessão no ASA indica acesso limitado com a reorientação do tráfego de HTTP ao ISE:

```
asav# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : cisco                      Index       : 69
Assigned IP   : 172.16.50.50                Public IP   : 192.168.10.21
```

```
<...some output omitted for clarity...>
```

```
ISE Posture:
```

```
Redirect URL : https://ise14.example.com:8443/portal/gateway?sessionId=ac101f64000
45000556b6a3b&portal=283258a0-e96e-...
Redirect ACL : Posture-redirect
```

## O módulo da postura recebe políticas do ISE e executa a remediação

O módulo da postura recebe as políticas do ISE. `ise-psc.log` debuga e mostra a exigência que é enviada ao módulo da postura:

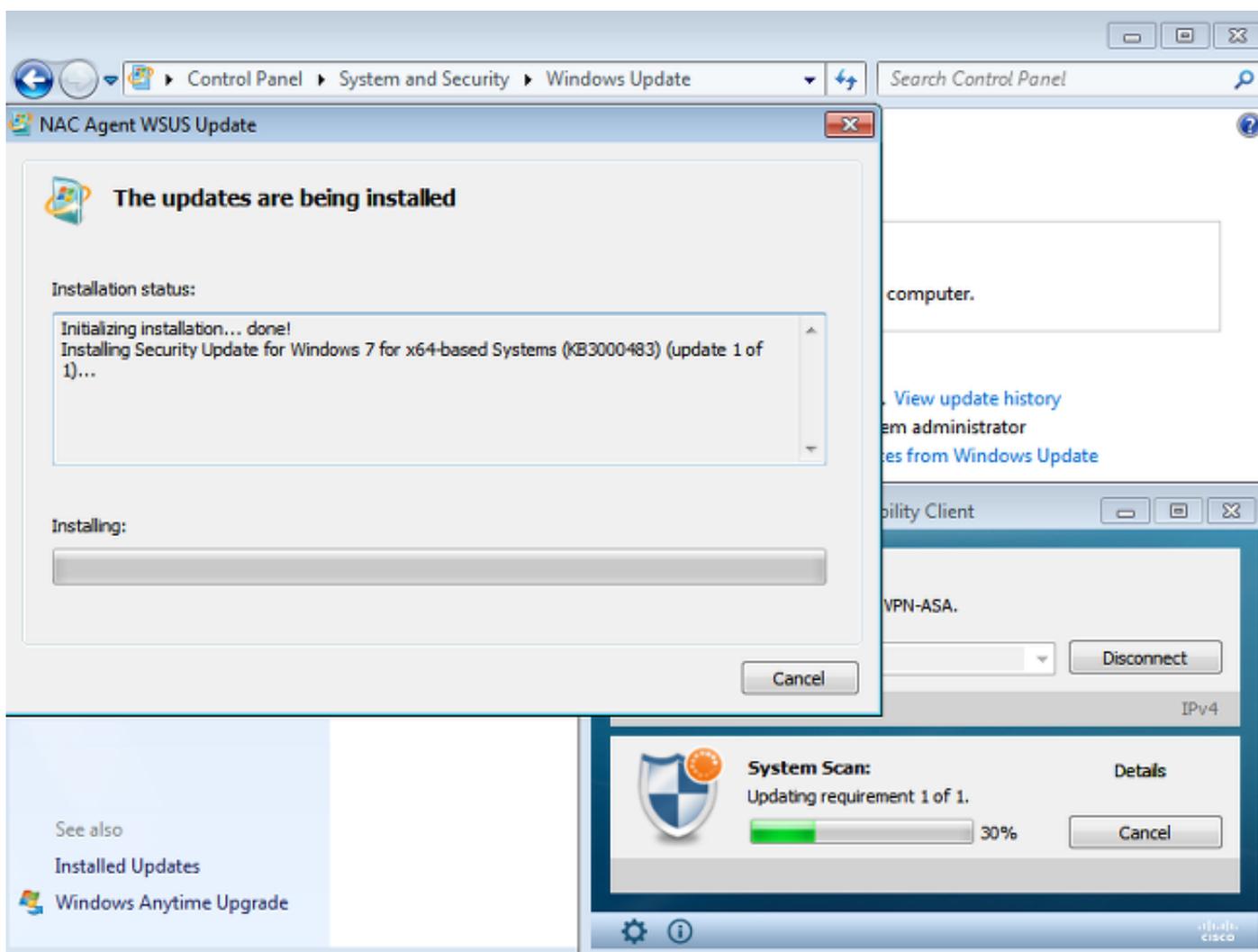
```
2015-06-05 07:33:40,493 DEBUG [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
<version>2</version>
<encryption>0</encryption>
```

```

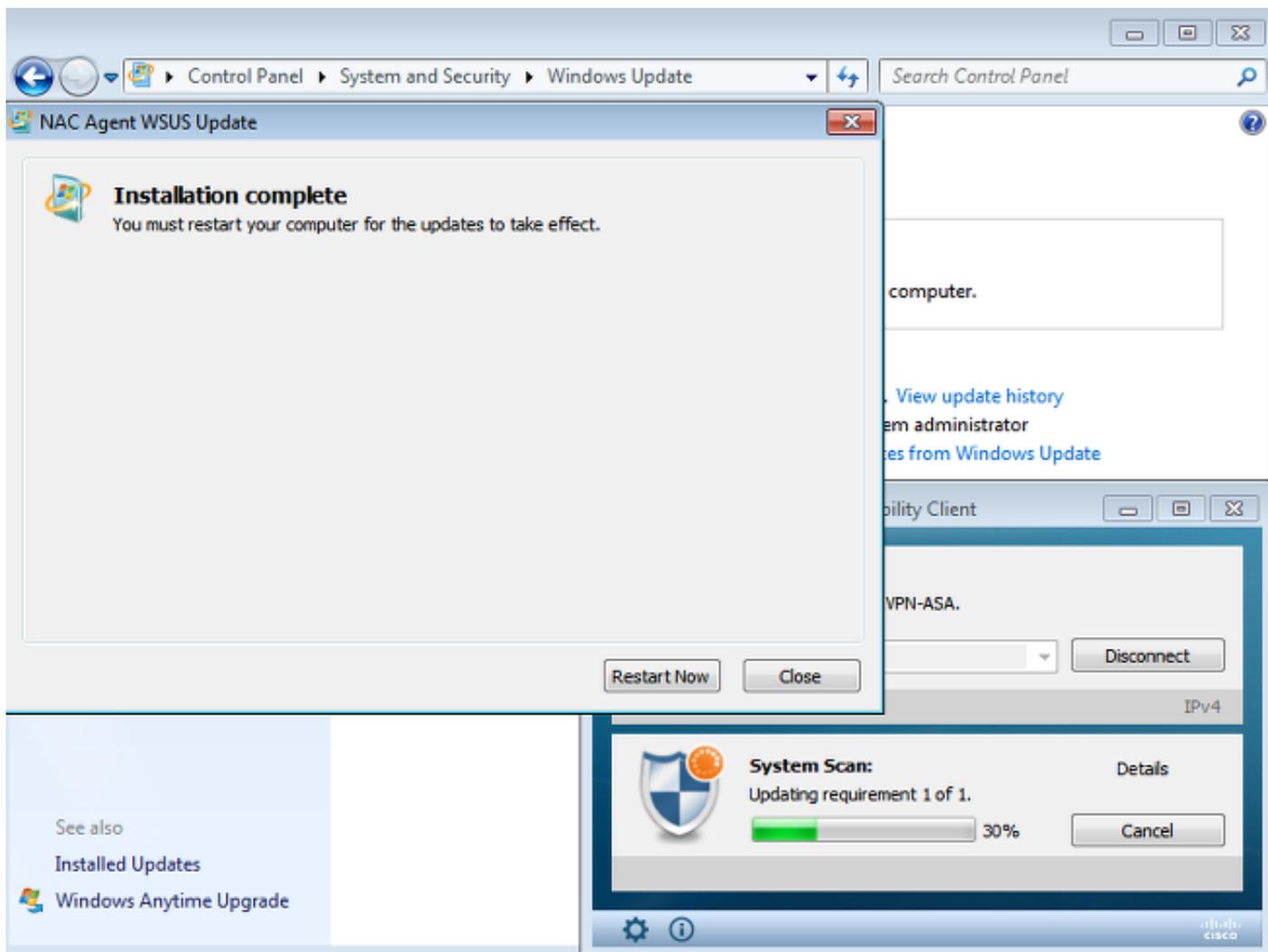
<package>
  <id>10</id>
  <name>WSUS</name>
  <version/>
  <description>This endpoint has failed check for any AS installation</description>
  <type>10</type>
  <optional>0</optional>
  <path>42#1</path>
  <remediation_type>1</remediation_type>
  <remediation_retry>0</remediation_retry>
  <remediation_delay>0</remediation_delay>
  <action>10</action>
  <check>
    <id>pr_WSUSCheck</id>
  </check>
  <criteria/>
</package>
</cleanmachines>

```

O módulo da postura provoca automaticamente o agente da atualização de Microsoft Windows para conectar ao WSUS e para transferir atualizações como configurado nas políticas WSUS (tudo automaticamente sem alguma intervenção de usuário):

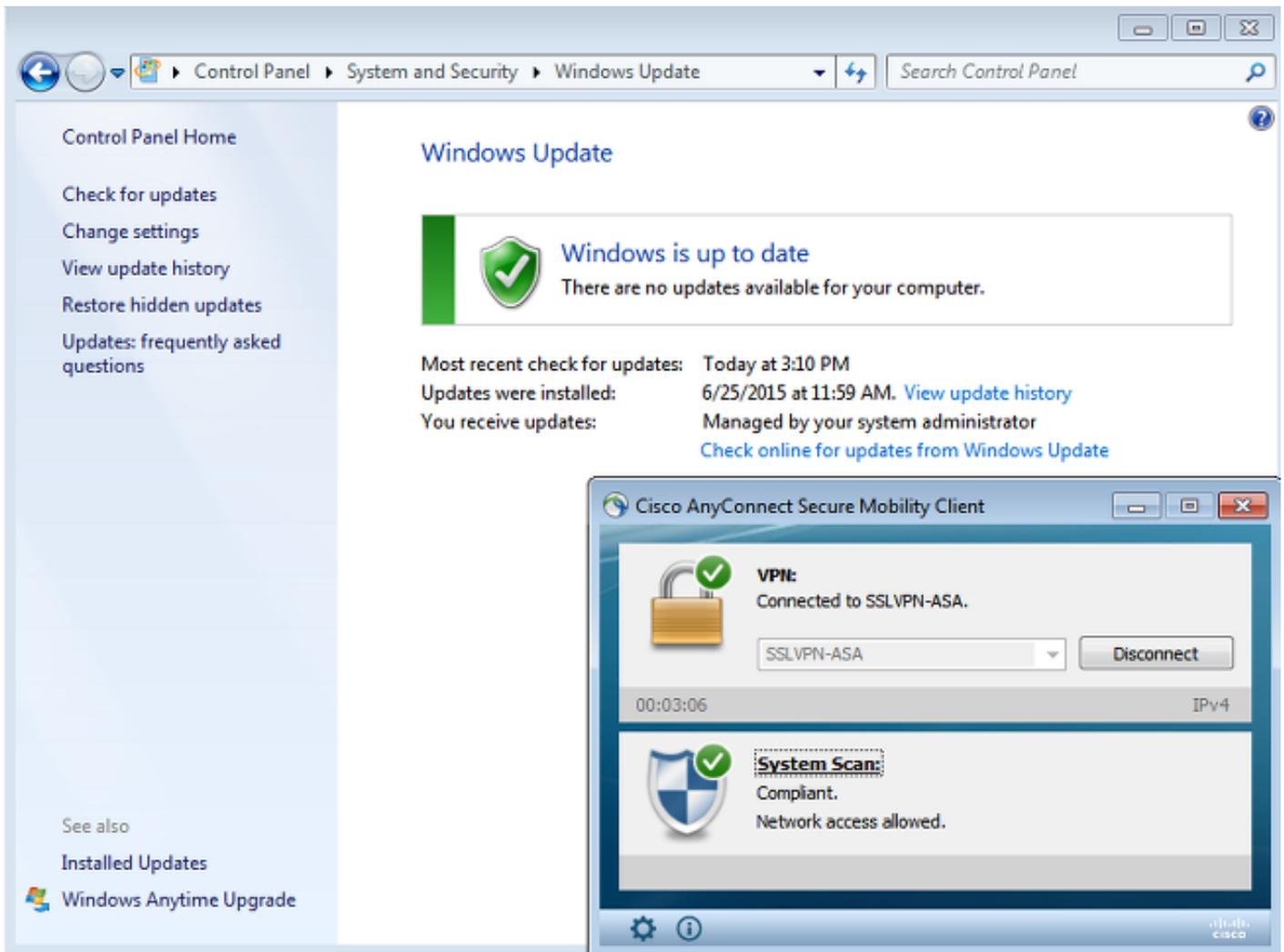


**Note:** Algumas das atualizações puderam exigir um reinício do sistema.

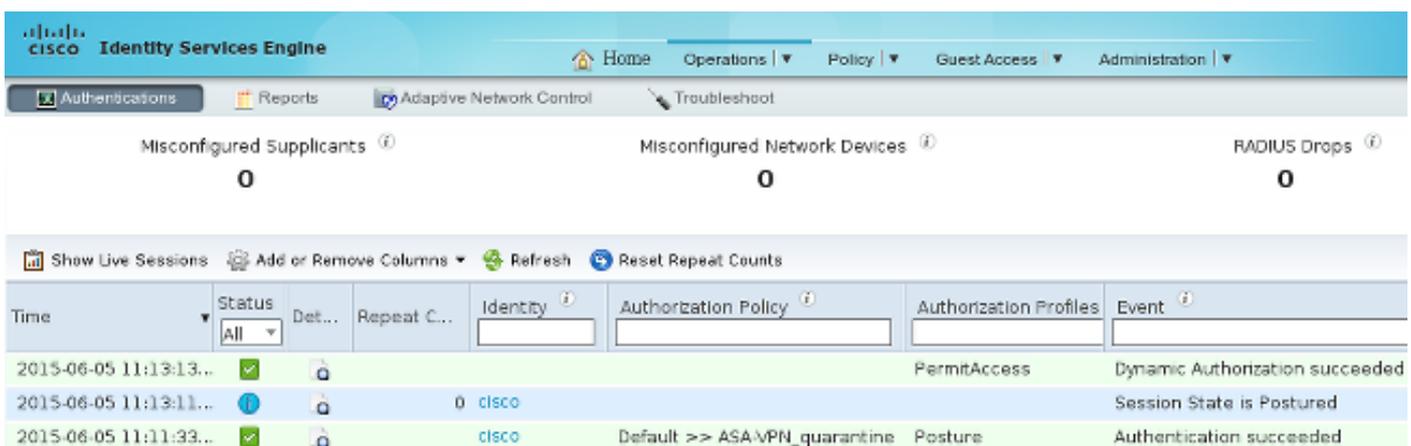


## Acesso de rede completo

Você verá este depois que a estação é relatada como complacente pelo módulo da postura de AnyConnect:



O relatório é enviado ao ISE, que reavalia a política e bate a regra da autorização de ASA-VPN\_compliant. Isto fornece o acesso de rede completo (através do CoA do raio). Navegue às operações > às autenticações a fim confirmar isto:



Debuga (ise-psc.log) igualmente confirmam o status de conformidade, o disparador CoA, e as configurações final para a postura:

```
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureManager -:cisco:
ac101f6400039000556b4200::- Posture report token for endpoint mac
08-00-27-DA-EF-AD is Healthy
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco:
ac101f6400039000556b4200::- entering triggerPostureCoA for session
```

ac101f6400039000556b4200

```
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco:ac101f6400039000556b4200::- Posture CoA is scheduled for session id [ac101f6400039000556b4200]
```

```
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:ac101f6400039000556b4200::- DM_PKG report non-AUP:html = <!--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:DA:EF:AD-->
```

```
DEBUG [pool-183-thread-1][]cisco.cpm.posture.runtime.PostureCoA -:cisco:ac101f6400036000556b3f52::- Posture CoA is triggered for endpoint [08-00-27-da-ef-ad] with session [ac101f6400039000556b4200]
```

Também, o relatório de avaliação detalhado ISE da postura confirma que a estação é complacente:

## Posture More Detail Assessment

Time Range: From 05/30/2015 12:00:00 AM to 06/05/2015 11:59:59 PM  
Generated At: 2015-06-05 20:09:00.047

### Client Details

Username:	cisco
Mac Address:	08:00:27:DA:EF:AD
IP address:	172.16.50.50
Session ID:	ac101f6400036000556b3f52
Client Operating System:	Windows 7 Professional 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.1.02011
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-PC
System Domain:	example.com
System User:	Administrator
User Domain:	EXAMPLE
AV Installed:	ClamWin Free Antivirus;0.98.5;55.20615;06/26/2015;
AS Installed:	Windows Defender;6.1.7600.16385;1.201.171.0;06/26/2015;

### Posture Report

Posture Status:	Compliant
Logged At:	2015-06-05 07:28:49.194

### Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed Conditions
WSUS	WSUS	Mandatory			Missing windows updates: 0

**Note:** O endereço de controle de acesso de mídia (MAC) exato da relação de rede física em Microsoft Windows PC é sabido devido aos Ramais de ACIDEX.

## Troubleshooting

Não há atualmente nenhuma informação de Troubleshooting disponível para esta configuração.

## Notas importantes

Esta seção fornece alguma informação importante sobre a configuração que é descrita neste documento.

## Detalhes da opção para a remediação WSUS

É importante diferenciar a condição da exigência da remediação. AnyConnect provoca o agente da atualização de Microsoft Windows para verificar a conformidade, dependente das *atualizações de Windows da validação usando o ajuste da remediação*.

### Windows Server Update Services Remediation

\* Name  ⓘ

Description

Remediation Type

Interval  (in secs) (Valid Range 0 to 9999)

Retry Count  (Valid Range 0 to 99)

Validate Windows updates using  Cisco Rules  Severity Level

Windows Updates Severity Level

Update to latest OS Service Pack

Windows Updates Installation Source  Microsoft Server  Managed Server

Installation Wizard Interface Setting  Show UI  No UI

Para este exemplo, o *nível de seriedade* é usado. Com o ajuste *crítico*, o agente de Microsoft Windows verifica se haja () umas atualizações críticas não instaladas pendentes. Se há, a seguir a remediação começa.

O processo da remediação pôde então instalar todas as atualizações críticas e menos importantes baseadas na configuração WSUS (atualizações aprovadas para a máquina específica).

Com *Windows da validação as atualizações que usam o grupo como Cisco ordenam*, as circunstâncias que são detalhadas na exigência decidem se a estação é complacente.

## Serviço de Windows Update

Para disposições sem um server WSUS, há um outro tipo da remediação que possa ser usado chame a *remediação de Windows Update*:

[Windows Update Remediations List > New Windows Update Remediation](#)

### Windows Update Remediation

\* Name  ⓘ

Description

Remediation Type

Interval  (in secs) (Valid Range 0 to 9999)

Retry Count  (Valid Range 0 to 99)

Windows Update Setting

Override User's Windows Update setting with administrator's

Este tipo da remediação permite o controle sobre os ajustes da atualização de Microsoft Windows e permite-o de executar atualizações imediatas. Uma condição típica que seja usada com este

tipo da remediação é *pc\_AutoUpdateCheck*. Isto permite que você verifique se o ajuste da atualização de Microsoft Windows esteja permitido no valor-limite. Se não, você pode permiti-lo e executar a atualização.

## Integração SCCM

Uns novos recursos para a versão 1.4 ISE chamada *gerenciamento de patches* permitem a integração com muitos fornecedores de terceira parte. O dependente em cima do vendedor, opções múltiplas está disponível para as circunstâncias e remediações.

Para Microsoft, o server do gerenciamento de sistema (SMS) e o gerenciador de configuração de System Center (SCCM) são apoiados.

## Informações Relacionadas

- [Serviços da postura no manual de configuração de Cisco ISE](#)
- [Guia do administrador do Cisco Identity Services Engine, liberação 1.4](#)
- [Guia do administrador do Cisco Identity Services Engine, liberação 1.3](#)
- [Distribua serviços da atualização de Windows Server em sua organização](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)