# 配置ISE与Microsoft WSUS的版本1.4状态

## 目录



## 简介

本文描述如何配置思科身份服务引擎(ISE)状态功能，当集成与MS Windows服务器更新服务时(WSUS)。

> **Note**:当您访问网络时，您重定向对Cisco AnyConnect安全移动客户端版本4.1供应的ISE用状态模块，检查在WSUS的符合状态并且安装必要的更新为了站点是兼容的。一旦站点报告如兼容， ISE允许全双工网络访问。

# 先决条件

## 要求

Cisco 建议您了解以下主题：

- 思科ISE部署、验证和授权
- 关于ISE和思科AnyConnect摆代理程序姿势的方式的基础知识运行
- 思科可适应安全工具(ASA)的配置
- 基本VPN和802.1x知识
- Microsoft WSUS的配置

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows版本7
- 与WSUS版本6.3的Microsoft Windows版本2012
- Cisco ASA版本9.3.1和以上
- Cisco ISE软件版本1.3及以后

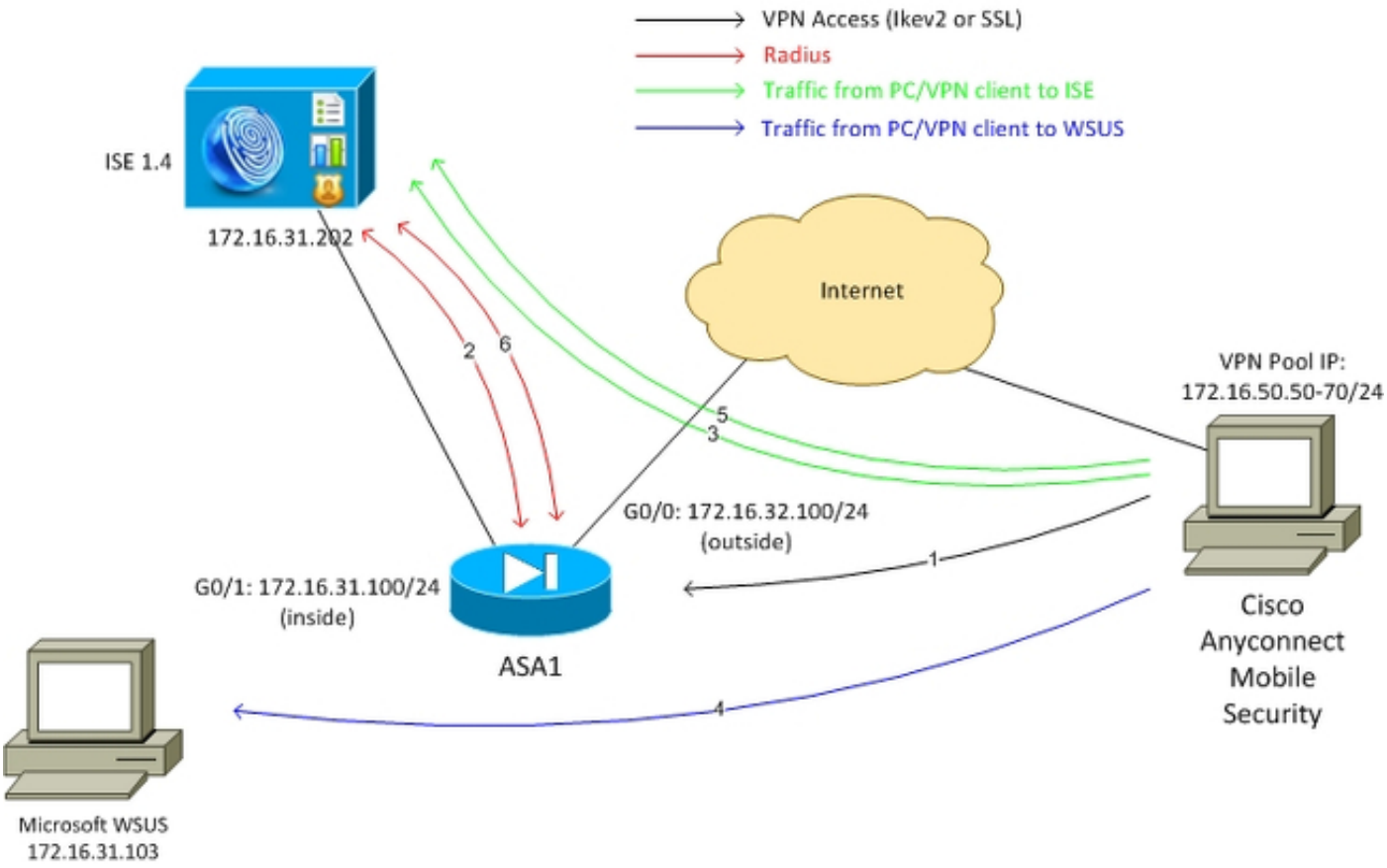
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

# 配置

此部分描述如何配置ISE和相关网元。

### 网络图

这是使用示例在本文中的拓扑：




这是通信流，如网络图所示：

1. 远程用户通过VPN访问的思科AnyConnect连接对ASA。这可以是任一种统一的访问，例如在交换机或一无线会话终止在无线局域网控制器的802.1x/MAC验证旁路(MAB)有线的会话(WLC)终止。

2. 作为认证过程的部分， ISE确认终端站的状态状况与兼容不是相等的(*ASA-VPN_quarantine*授权规则)，并且重定向属性在*Radius Access-Accept*消息返回。结果， ASA重定向所有HTTP数据流对ISE。

3. 用户打开Web浏览器并且输入所有地址。在对ISE的重定向以后，思科AnyConnect 4状态模块在站点安装。状态模块然后下载从ISE (WSUS的需求的策略)。

4. 状态模块搜索Microsoft WSUS，并且执行修正。

5. 在成功的修正以后，状态模块发送报告对ISE。

6. ISE问题Radius该的崔凡吉莱授权(CoA)提供对一个兼容VPN用户(*ASA-VPN_compliant*授权规则)的全双工网络访问。

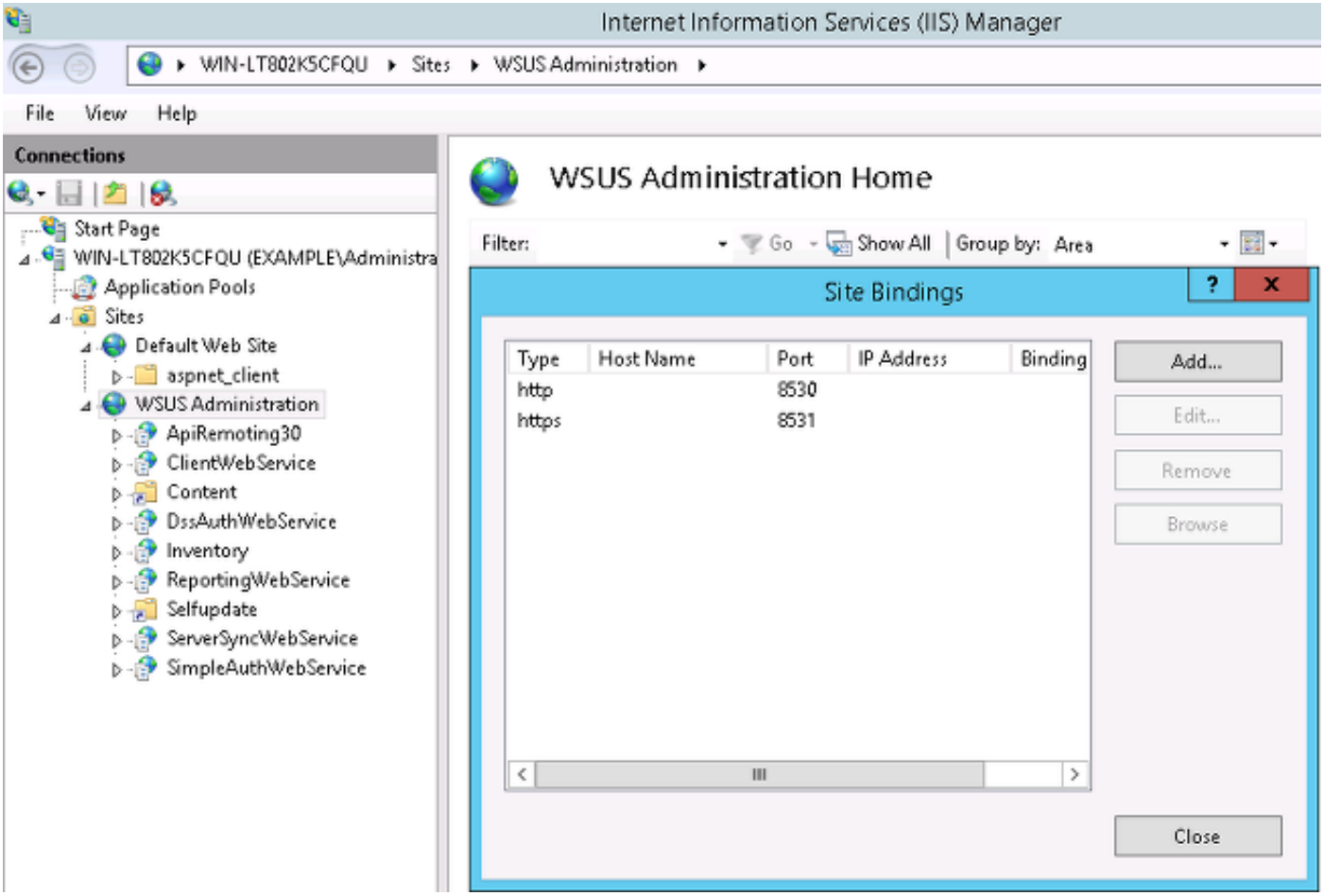
**Note**:为了修正能工作(能力安装在PC的Microsoft Windows更新)，用户应该有本地管理权限。

## Microsoft WSUS

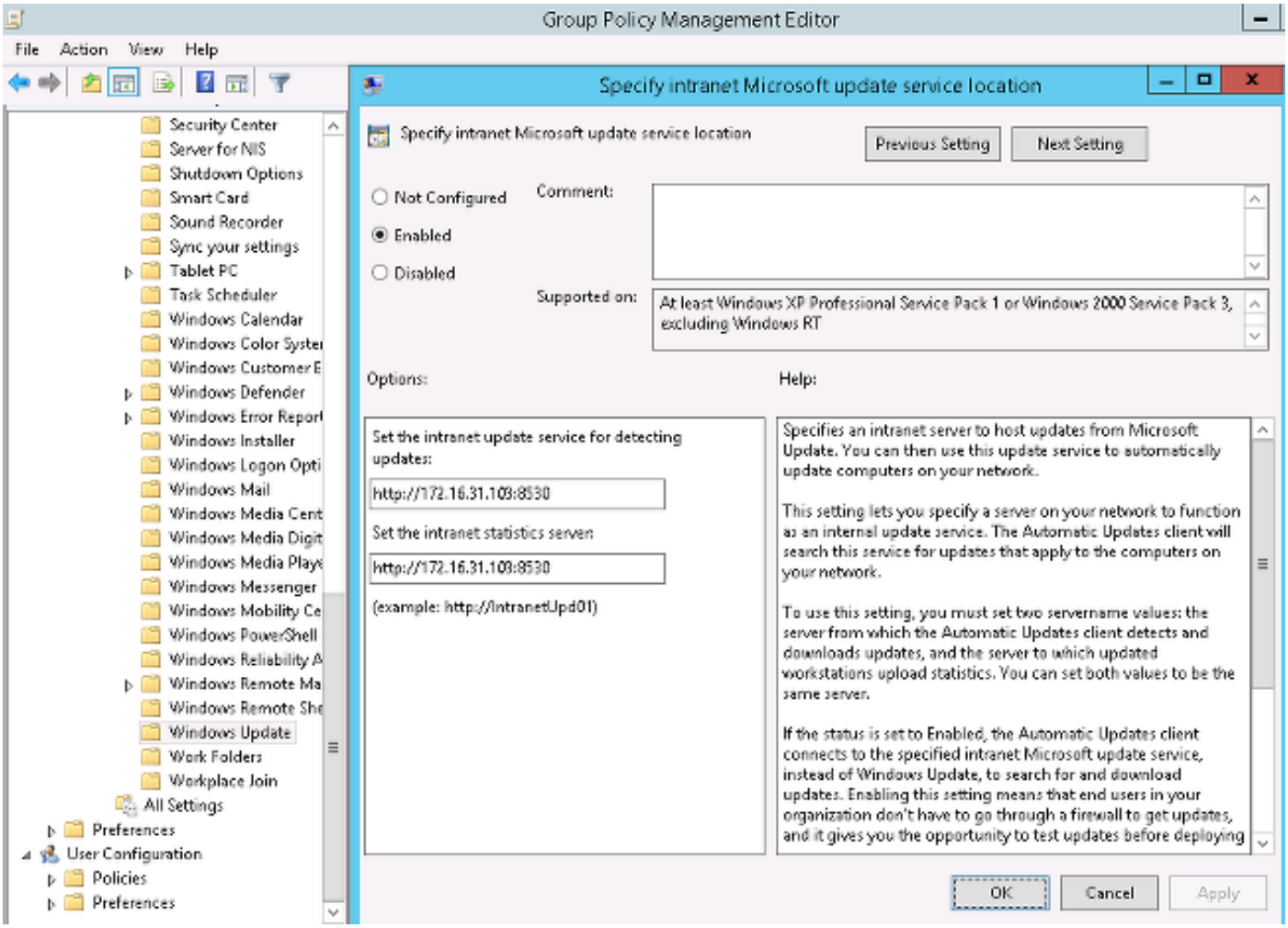
**Note**:WSUS的详细配置是超出本文的范围。关于详细信息，参考在您的组织Microsoft文档的

[部署Windows服务器更新服务](#)。

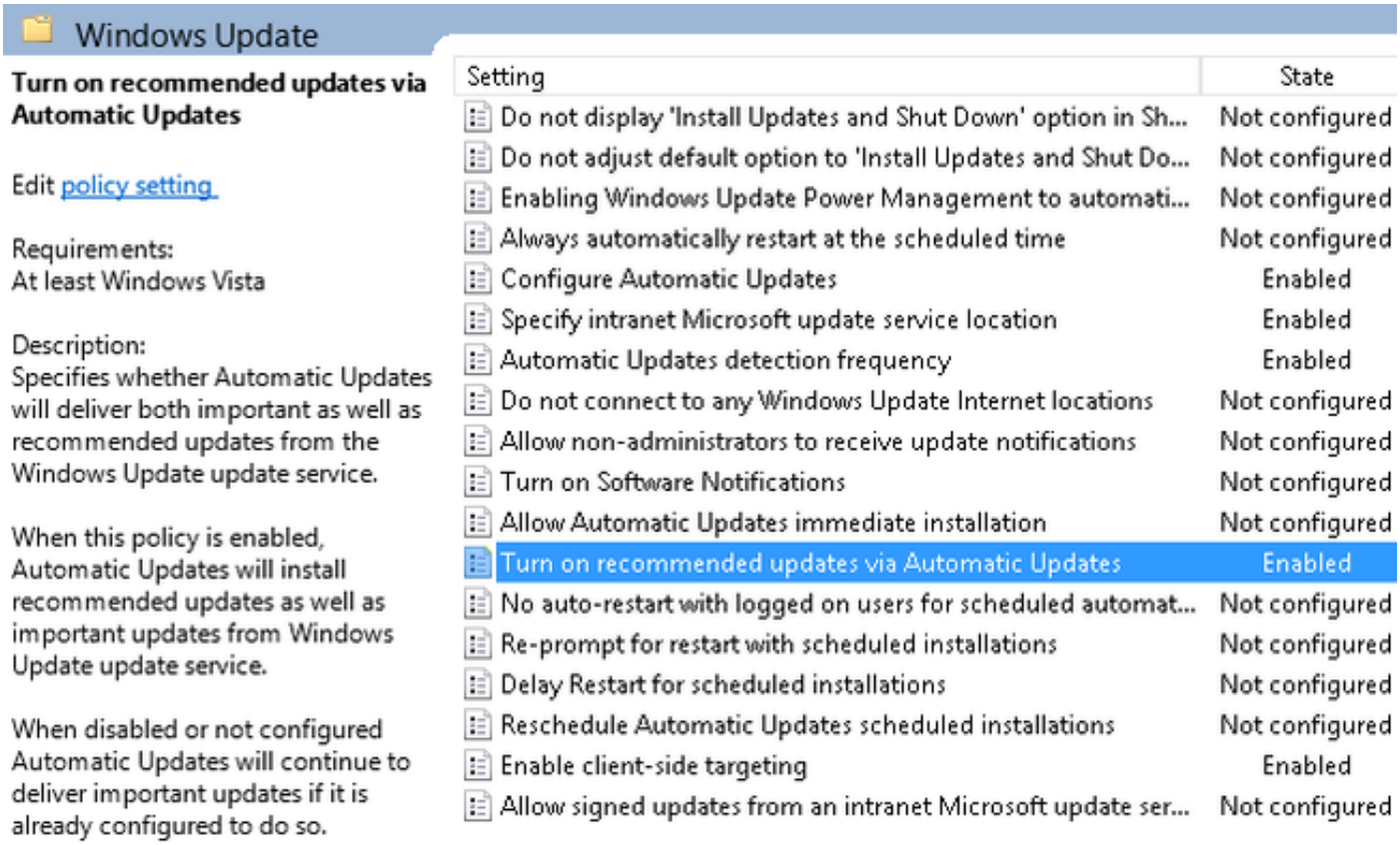
WSUS服务通过标准的TCP端口8530部署。为修正记住那，其他端口也使用是重要的。这就是为什么它是安全添加WSUS的IP地址对在ASA (描述的以后的重定向访问控制表(ACL)在本文)。




域的组策略为Microsoft Windows更新和点配置对本地WSUS服务器：




这些是为粒状策略启用根据不同的级别严重性的推荐的更新：




客户端瞄准允许较大适应性。ISE能使用根据不同的Microsoft Active Directory的状态策略(AD)计算

机容器。WSUS能审批根据此会员的更新。

## ASA

远程用户的简单安全套接字协议层(SSL) VPN访问被使用(详细信息是超出本文的范围)。

这是配置示例：

```
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
```

配置access-list ASA是重要的，用于为了确定流量应该重定向到ISE (为不是兼容的)的用户：

```
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
```

仅域名系统(DNS)、ISE、WSUS和互联网控制消息协议(ICMP)流量为固执的用户允许。所有另一个流量(HTTP)重定向对AnyConnect 4供应的ISE，对状态和修正负责。

## ISE

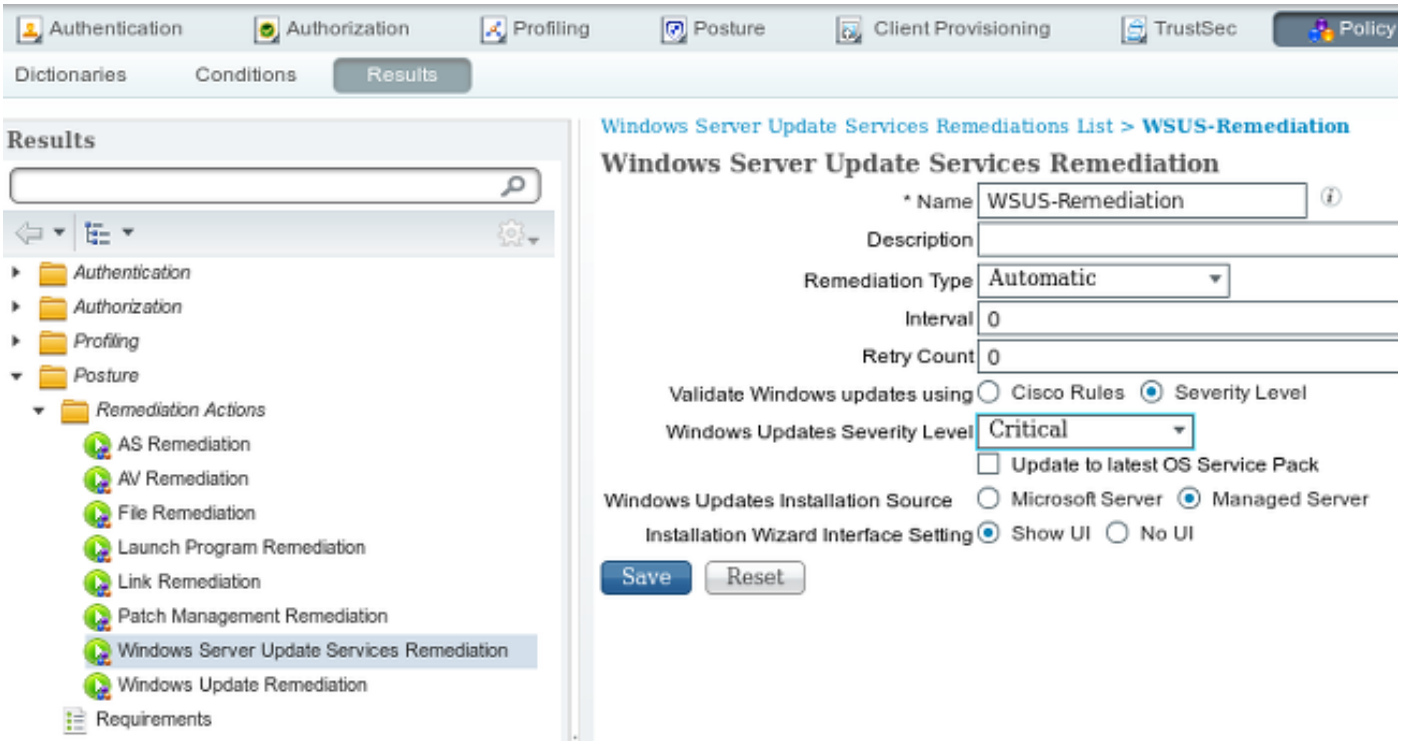
**Note**:AnyConnect 4供应和状态是超出本文的范围。参考与ISE欲了解更详细的信息版本1.3配置示例的AnyConnect 4.0集成，例如如何配置ASA作为网络设备和安装Cisco AnyConnect 7应用程序。

## WSUS的状态修正

完成这些步骤为了配置WSUS的状态修正：

1. 导航对**策略>情况>状态>修正操作> Windows服务器更新服务修正**为了创建新规则。

2. 验证*Microsoft Windows更新*设置设为**严重级别**。如果修正进程开始，这部分负责检测。Microsoft Windows更新代理程序然后连接对WSUS和检查是否有等候安装为该PC的任何*关键*更新：




## WSUS的状态需求

导航对**策略>情况>状态>需求**为了创建新规则。规则使用呼叫*pr_WSUSRule的*一个假的情况，因此意味着WSUS被接触为了检查情况，当修正是必要的时(*关键*更新)。

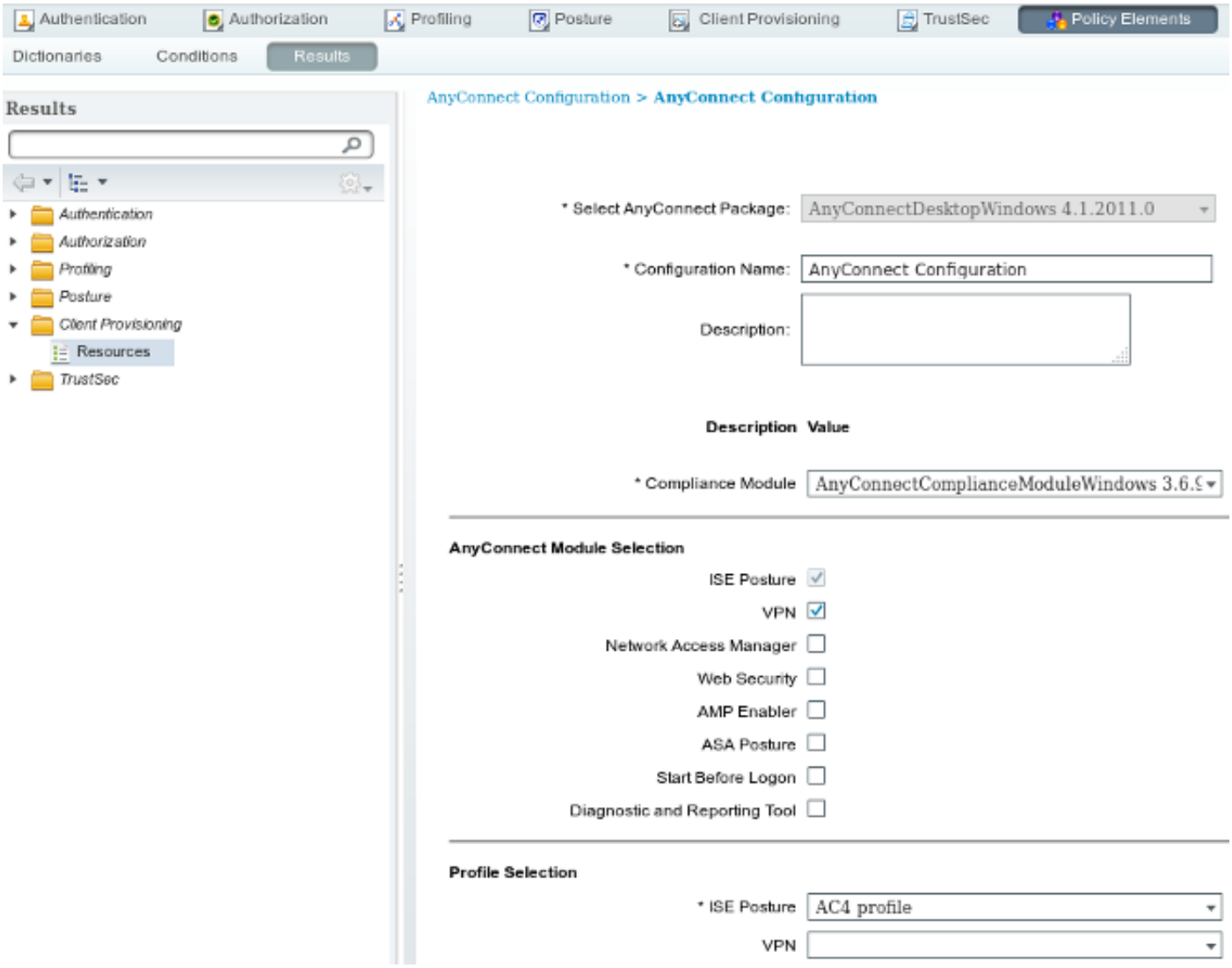
一旦此情况符合， WSUS安装为该PC配置的更新。这些能包括任一种更新，并且那些以低严重性成水平：

**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 |

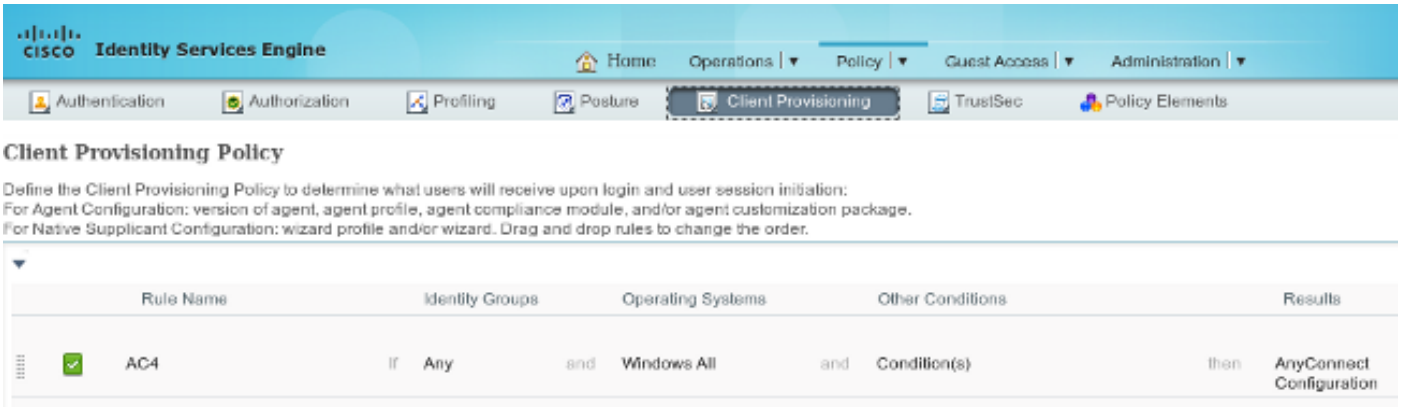
## AnyConnect配置文件

与AnyConnect 4配置文件一起配置状态模块配置文件，(正如与ISE版本1.3配置示例的AnyConnect 4.0集成所描述)：




## 客户端供应规则

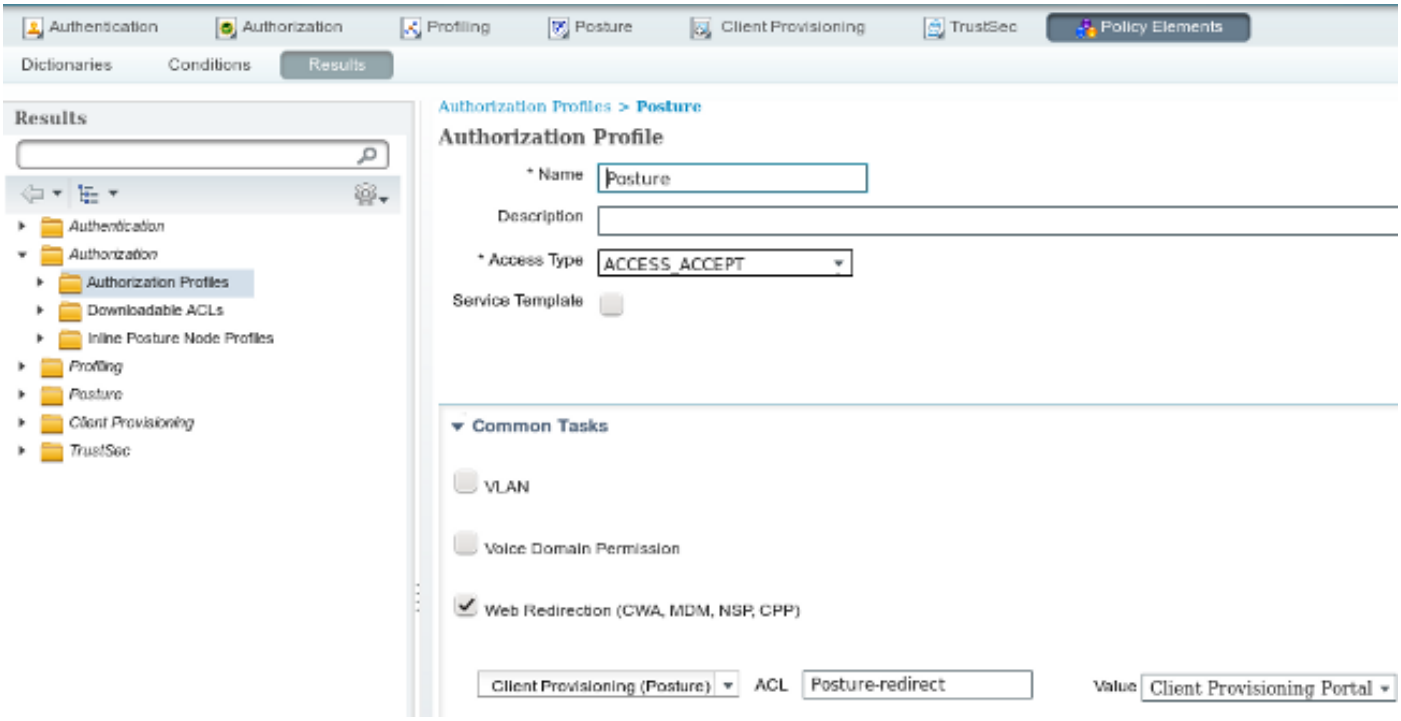
一旦AnyConnect配置文件准备好，可以从*客户端提供的策略*被参考：




整个应用程序，与配置一起，在终端安装，重定向对客户端供应入口页面。AnyConnect 4也许升级和已安装的附加模块(状态)。

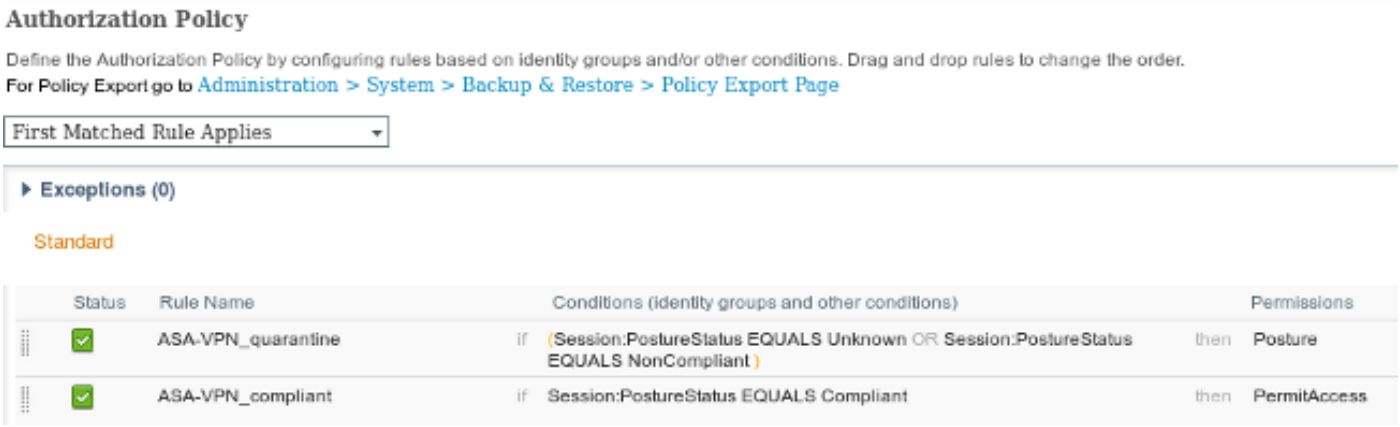
## 授权配置文件

创建重定向的一授权配置文件对客户端供应配置文件：




### 授权规则

此镜像显示授权规则：




第一次，使用*ASA-VPN_quarantine*规则。结果，*状态*授权配置文件返回，并且终端重定向到AnyConnect 4 (用状态模块)供应的客户端设置的门户。

一旦兼容，使用*ASA-VPN_compliant*规则，并且全双工网络访问允许。

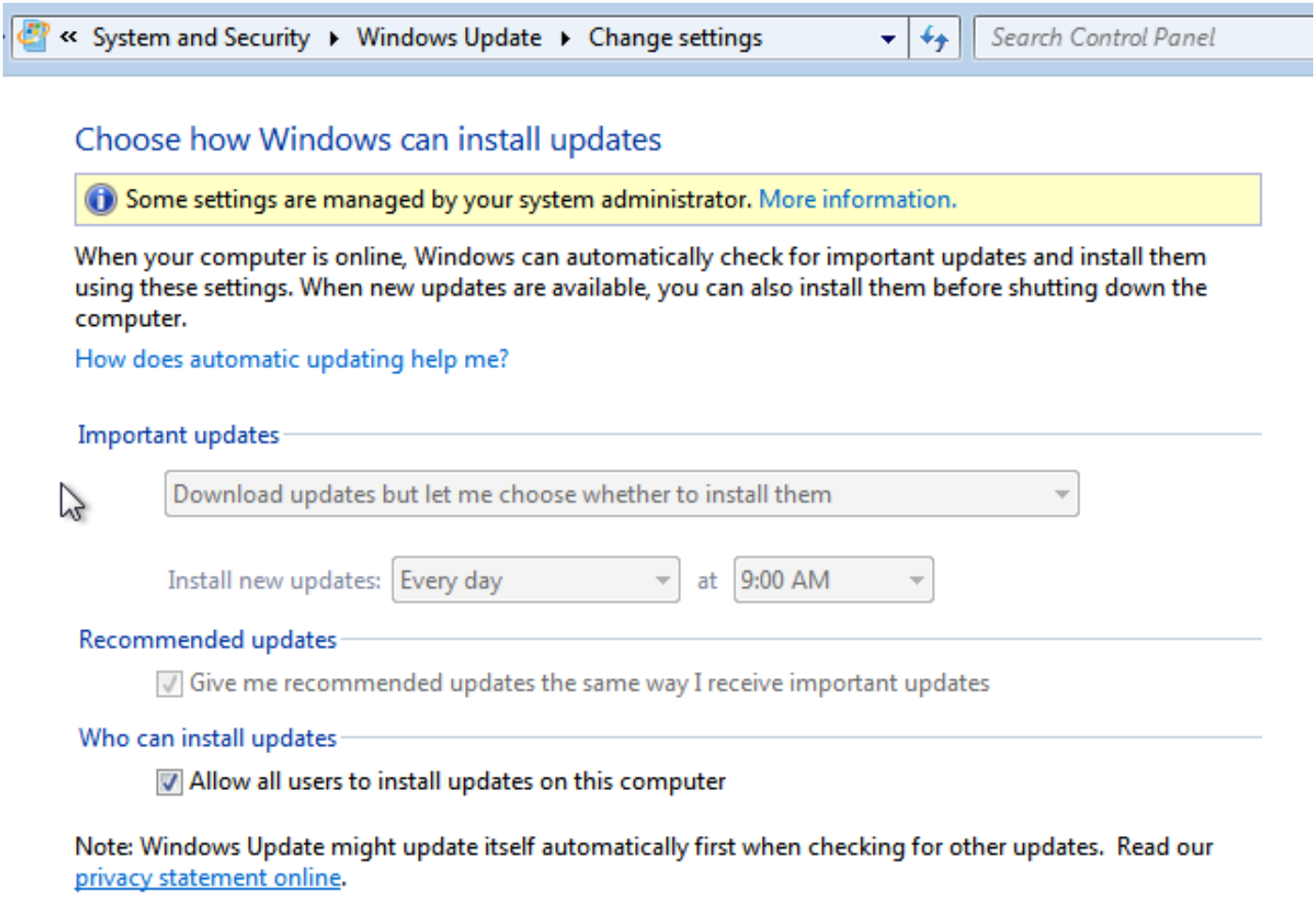
## 验证

此部分提供您能使用为了验证的信息您配置适当地工作。

### 有更新GPO策略的PC

与WSUS配置的域策略，在PC登录域后，应该推送。这能发生，在VPN会话建立前(在波段外面)或以后，如果*开始，在*使用前登录功能(它可以也用于有线的802.1x/无线访问)。

一旦Microsoft Windows客户机有正确配置，这可以从Windows更新设置反射：

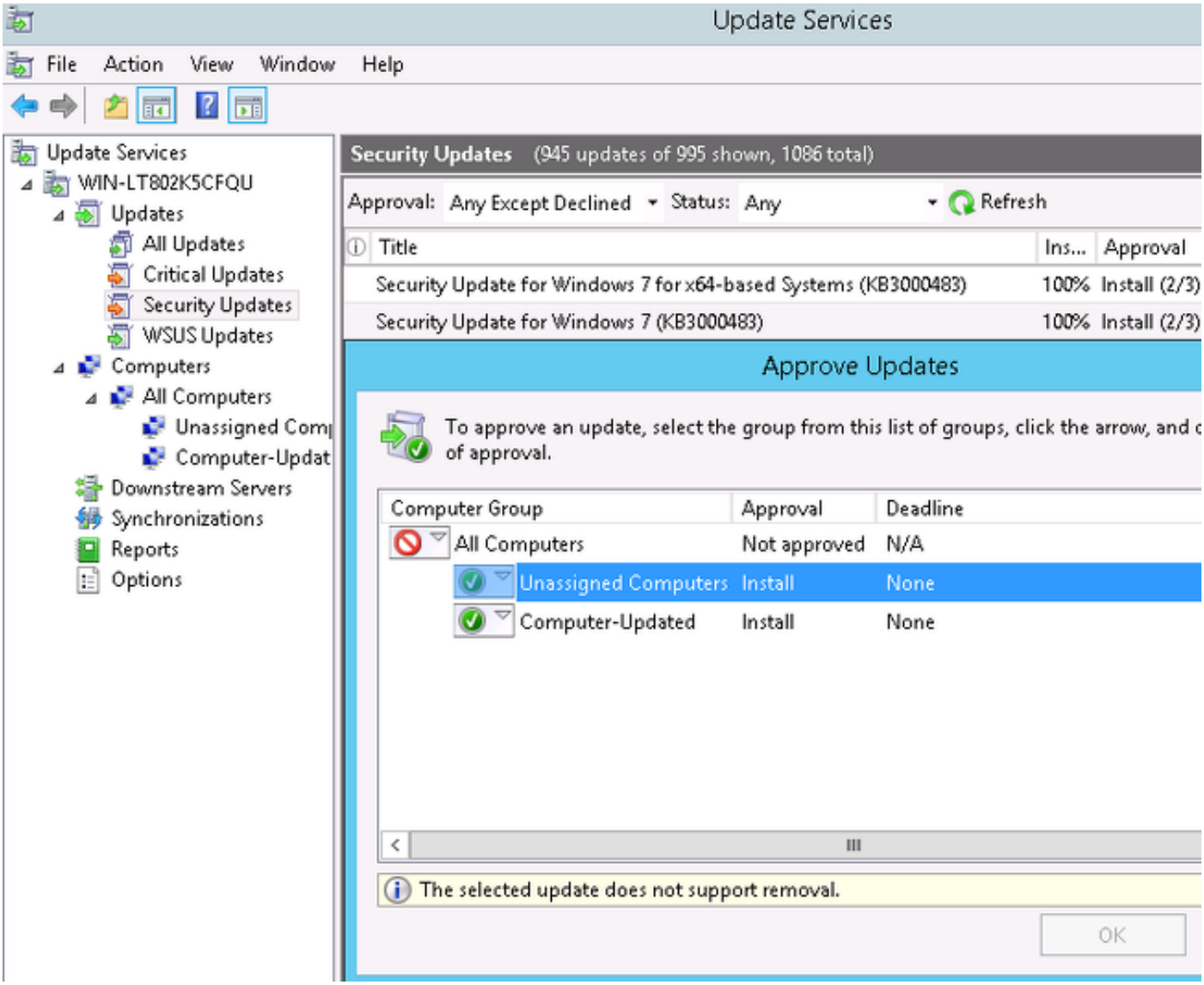



若需要，可以使用组策略对象(GPO)刷新和Microsoft Windows更新代理程序服务器发现：

```
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>
```

## 审批在WSUS的关键更新

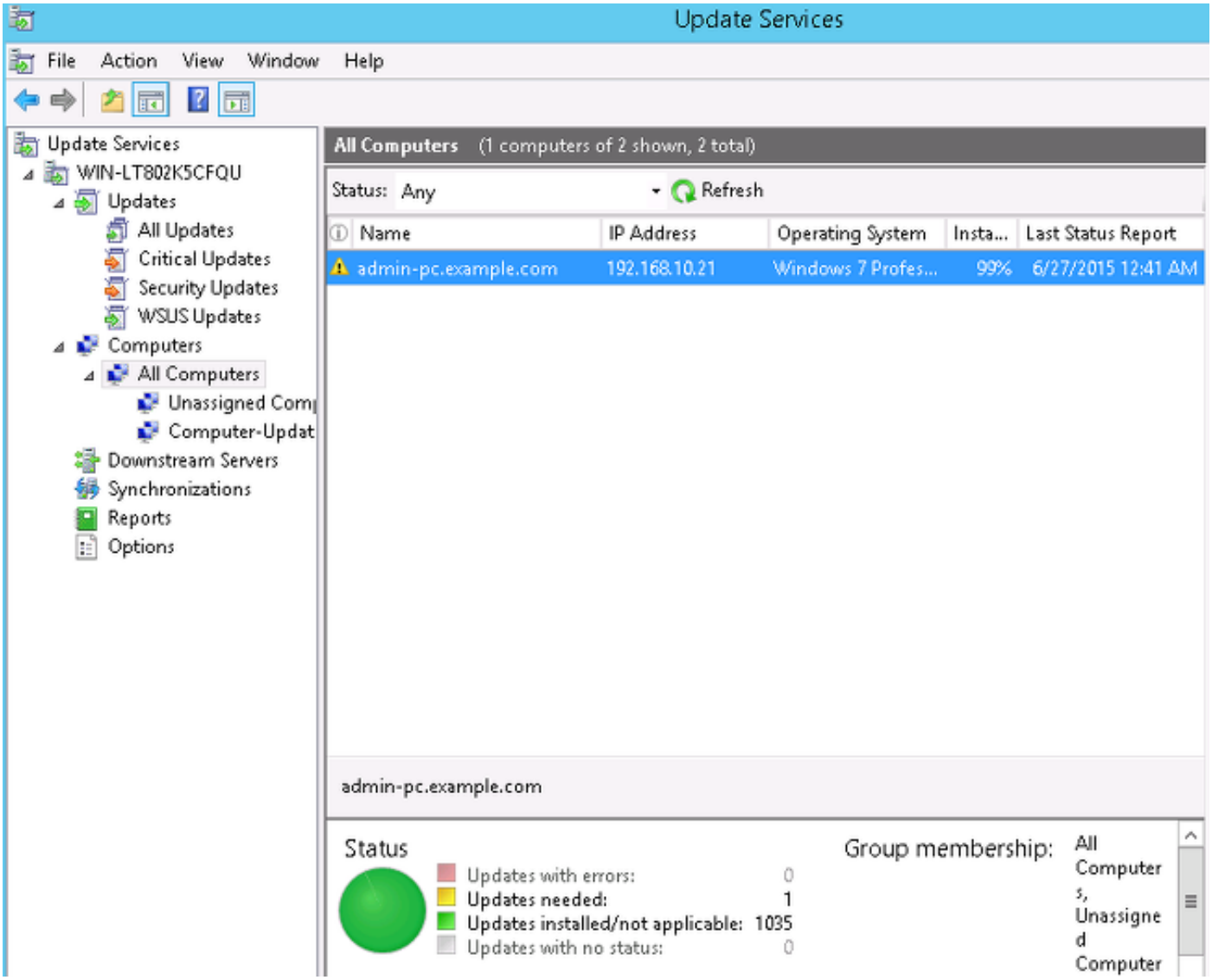
审批流程能受益于客户端站点瞄准：




若需要再发出与*wuauclt*的报告。

## 检查在WSUS的PC状态

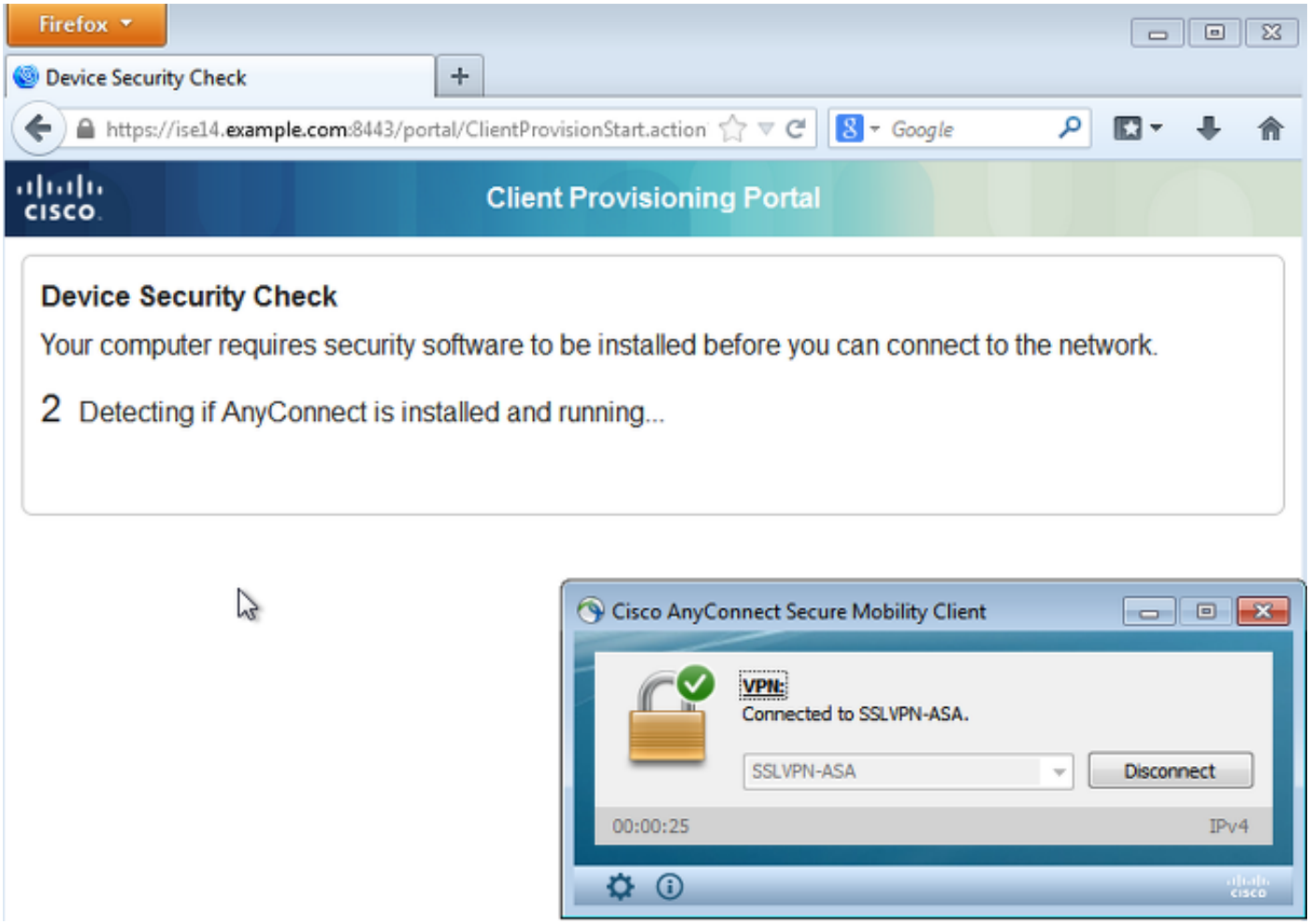
此镜像显示如何检查在WSUS的PC状态：




应该为与WSUS的下刷新安装一次更新。

## VPN会话建立

在VPN会话建立后，使用*ASA-VPN_quarantine* ISE授权规则，返回状态授权配置文件。结果，从终端的HTTP数据流为AnyConnect 4更新和状态模块供应重定向：




这时，在ASA的会话状态指示与HTTP数据流的重定向的有限访问对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-redirec
```

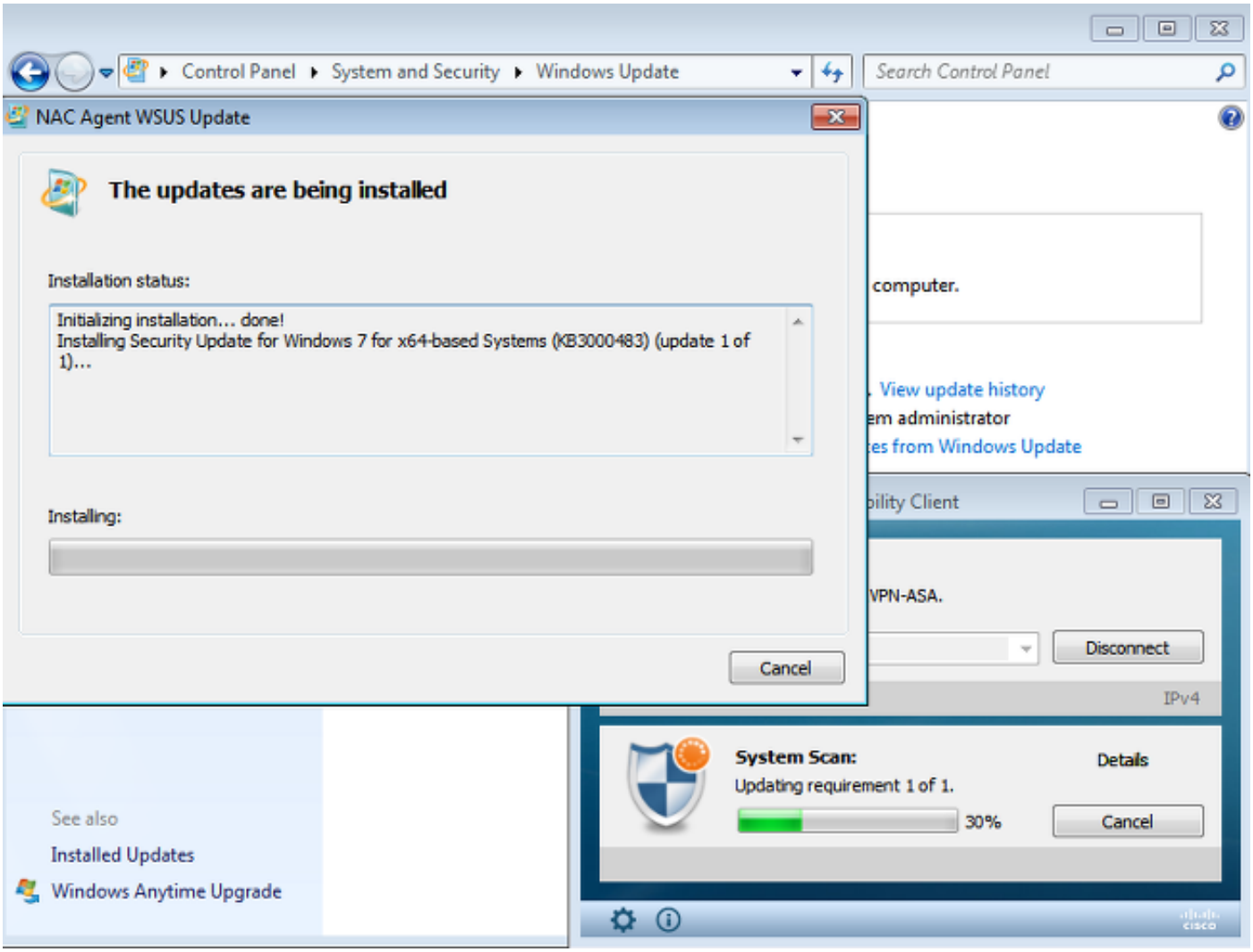
## 状态模块接收从ISE的策略并且执行修正

状态模块接收从ISE的策略。ise-psc.log调试显示发送到状态模块的要求：

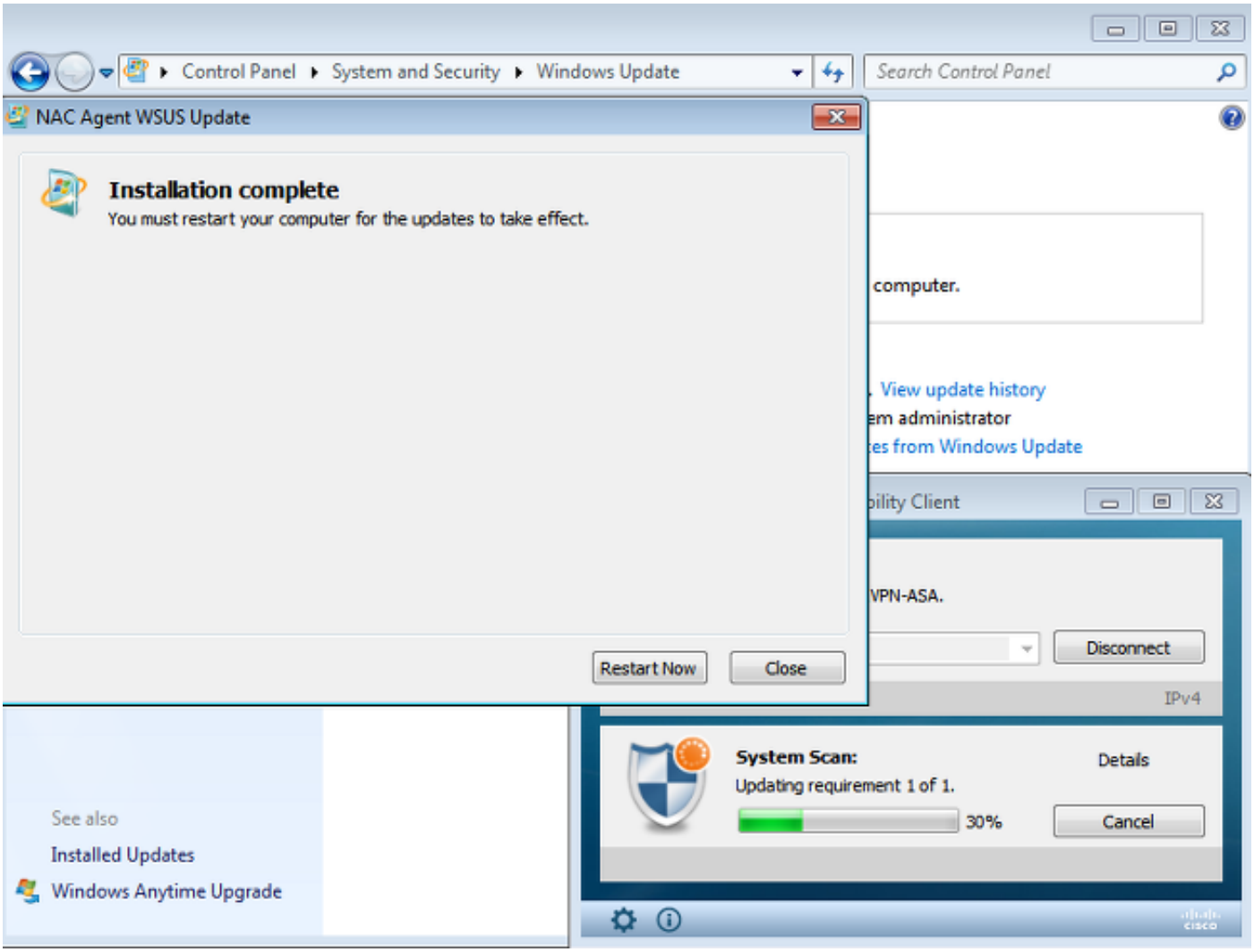
```
2015-06-05 07:33:40,493 DEBUG  [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1:::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
 <version>2</version>
 <encryption>0</encryption>
 <package>
   <id>10</id>
   <name>WSUS</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>
```

状态模块自动地触发Microsoft Windows更新代理程序连接到WSUS和下载更新如WSUS策略所配置的一样(自动全部没有任何用户干涉) ：

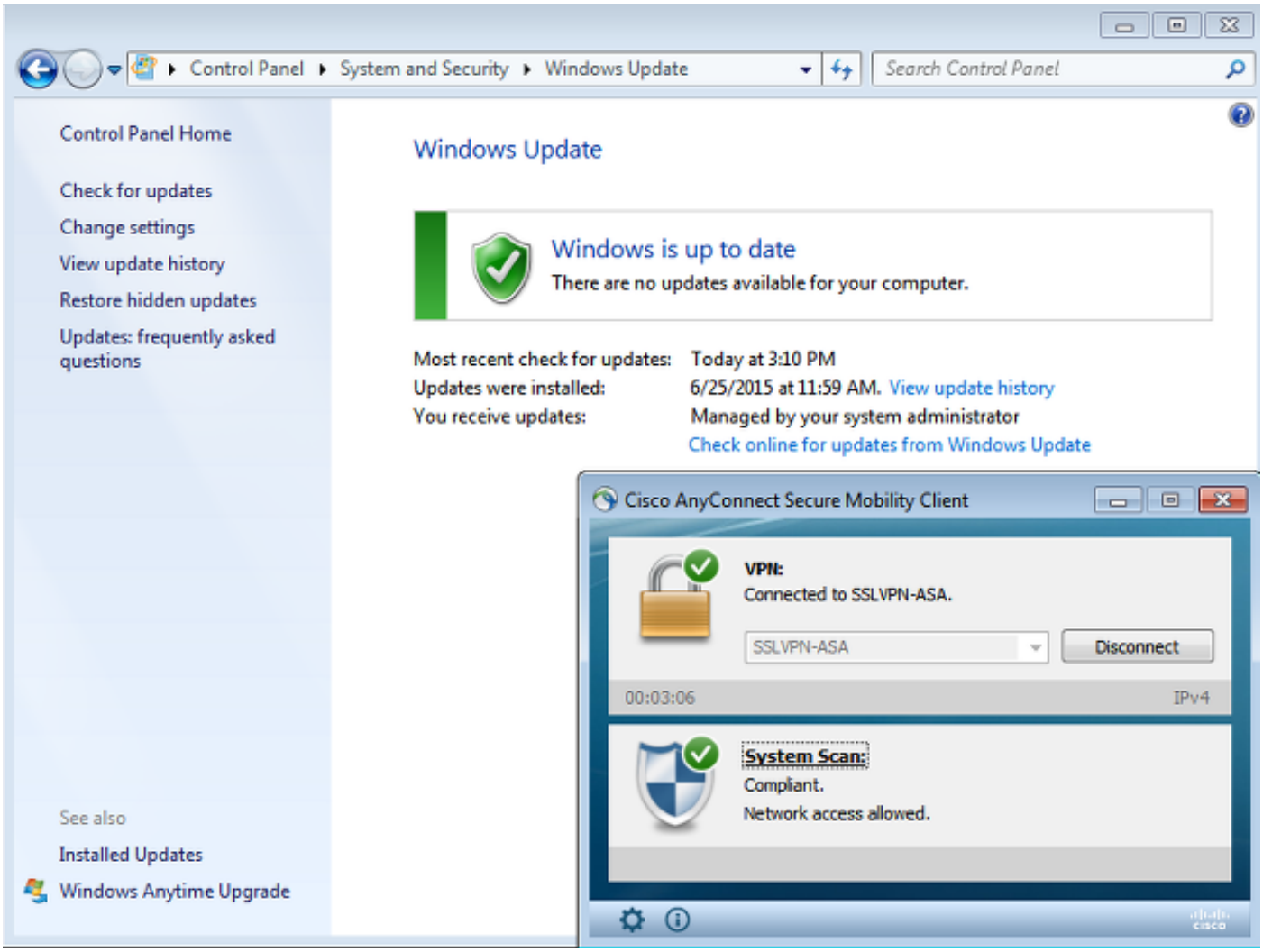



**Note**:某些更新也许要求系统重新启动。

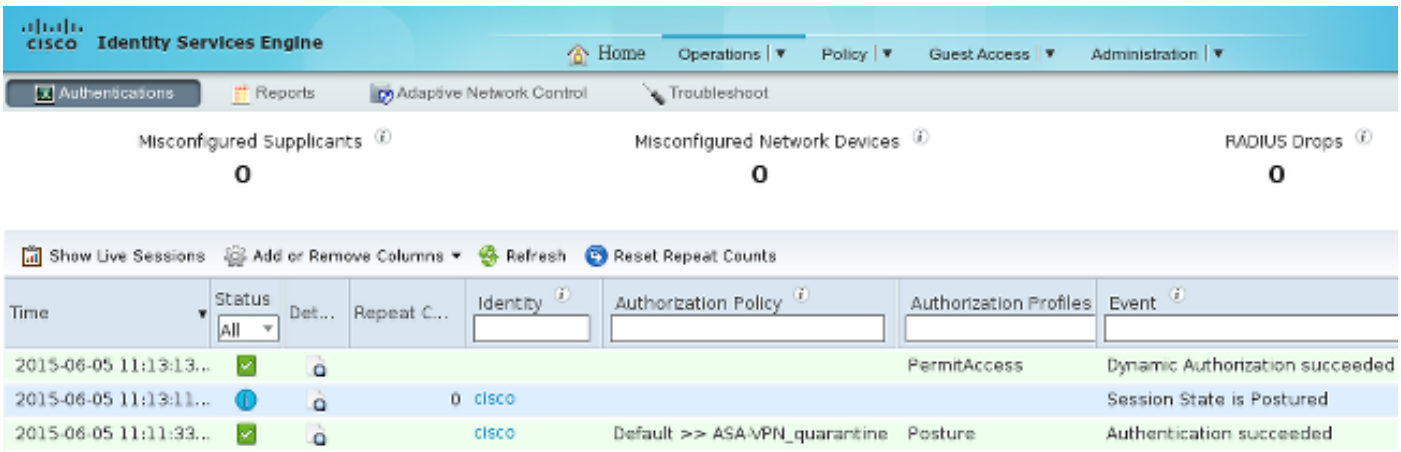



## 全双工网络访问

在站点报告如兼容由AnyConnect状态模块后，您将看到此：




报告被发送对ISE，复评策略并且点击*ASA-VPN_compliant*授权规则。这提供全双工网络访问(通过Radius CoA)。导航对**操作>认证**为了确认此：




调试(**ise-psc.log**)也确认符合状态、CoA触发和最终设置状态的：

```
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:ac
101f6400039000556b4200:::- 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]**

并且，ISE选派了状态评估报告确认站点是兼容的：

## 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**:物理网络接口的确切的MAC控制(MAC)地址在Microsoft Windows PC的知道由于ACIDEX扩展。

# 故障排除

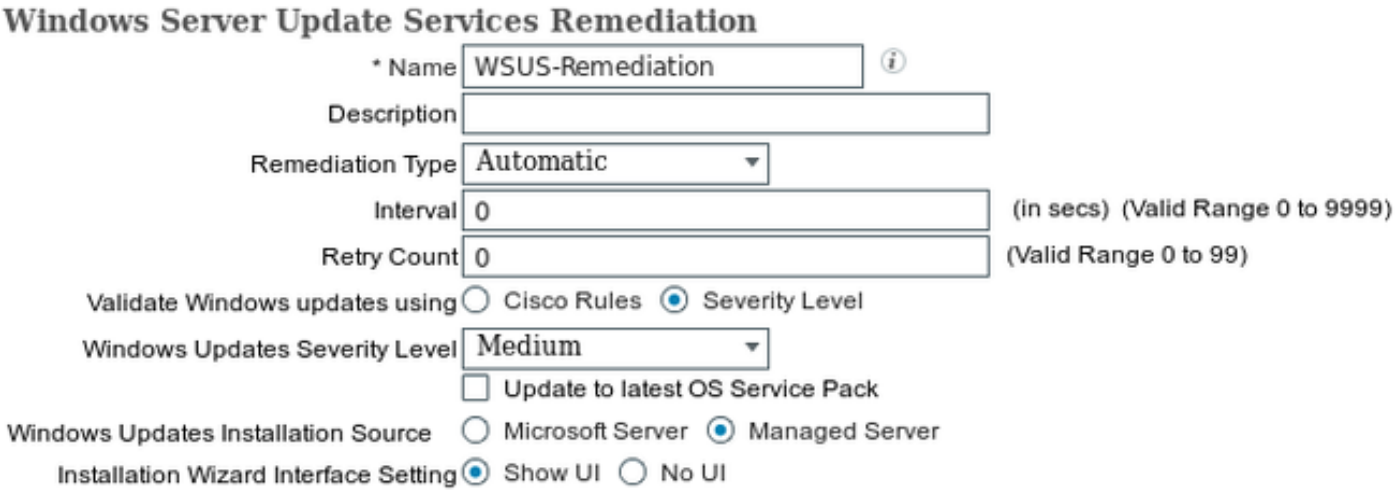
当前没有此配置的故障排除信息联机。

# 重要说明

此部分提供关于在本文描述的配置的一些重要信息。

## WSUS修正的选项详细信息

区分从修正的需求条件是重要的。AnyConnect触发Microsoft Windows更新代理程序检查标准，从属在*验证Windows更新使用*修正设置。



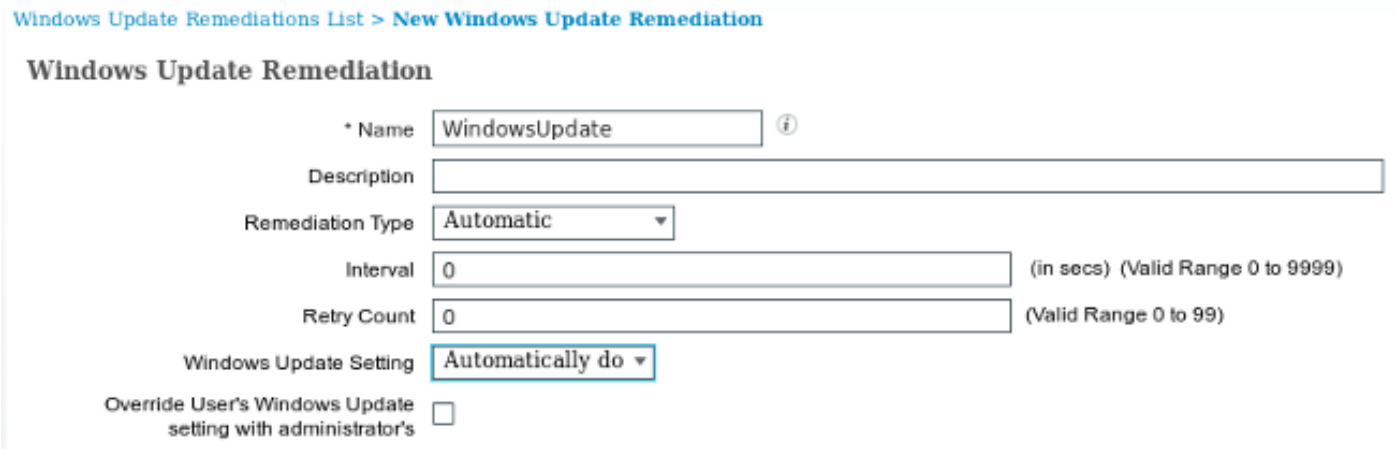

对于此示例，使用*严重级别*。使用*关键*设置， Microsoft Windows代理程序证实是否有其中任一待定(不已安装)关键更新。如果有，则修正开始。

修正进程也许然后安装根据WSUS配置的所有关键和较不重要更新(为特定计算机审批的更新)。

使用*验证Windows更新使用*集作为**思科规定**，在需求被选派决定的条件站点是否是兼容的。

## Windows更新服务

对于没有WSUS服务器的部署，有能使用呼叫*Windows Update修正的*另一个修正类型：




此修正类型允许对Microsoft Windows更新设置的控制并且使您执行立即更新。使用与此修正类型的一个典型的情况是*pc_AutoUpdateCheck*。这允许您证实Microsoft Windows更新设置是否在终端启用。否则，您可启用它和执行更新。

### SCCM集成

呼叫*补丁程序管理的*ISE版本1.4的一新特性允许与许多第三方供应商的集成。从属在供应商，多个选项为条件和补救是可用的。

对于Microsoft，支持系统管理服务器(SMS)和系统中心配置管理器(SCCM)。

## 相关信息

- 在思科ISE配置指南的状态服务
- 思科身份服务引擎管理员指南，版本1.4
- 思科身份服务引擎管理员指南，版本1.3
- 部署Windows服务器在您的组织的更新服务
- 技术支持和文档 - Cisco Systems