

Microsoft WSUS를 사용하여 ISE 버전 1.4 상태 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[Microsoft WSUS](#)

[ASA](#)

[ISE](#)

[WSUS에 대한 상태 개선](#)

[WSUS에 대한 상태 요구 사항](#)

[AnyConnect 프로파일](#)

[클라이언트 프로비저닝 규칙](#)

[권한 부여 프로파일](#)

[권한 부여 규칙](#)

[다음을 확인합니다.](#)

[업데이트된 GPO 정책이 있는 PC](#)

[WSUS에서 중요 업데이트 승인](#)

[WSUS에서 PC 상태 확인](#)

[VPN 세션 설정](#)

[포스처 모듈은 ISE에서 정책을 수신하고 교정 수행](#)

[전체 네트워크 액세스](#)

[문제 해결](#)

[중요 참고 사항](#)

[WSUS 교정에 대한 옵션 세부 정보](#)

[Windows 업데이트 서비스](#)

[SCCM 통합](#)

[관련 정보](#)

소개

이 문서에서는 Microsoft WSUS(Windows Server Update Services)와 통합될 때 Cisco ISE(Identity Services Engine) 상태 기능을 구성하는 방법에 대해 설명합니다.

참고:네트워크에 액세스할 때 Cisco AnyConnect Secure Mobility Client Version 4.1 프로비저

닝을 위한 ISE로 리디렉션됩니다. 포스처 모듈에서는 WSUS의 규정 준수 상태를 확인하고 스테이션 규정 준수를 위해 필요한 업데이트를 설치합니다.스테이션이 규정 준수 상태로 보고되면 ISE는 전체 네트워크 액세스를 허용합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 구축, 인증 및 권한 부여
- ISE와 Cisco AnyConnect 포스처 에이전트가 작동하는 방식에 대한 기본 지식
- Cisco ASA(Adaptive Security Appliance) 구성
- 기본 VPN 및 802.1x 지식
- Microsoft WSUS 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 버전 7
- Microsoft Windows 버전 2012(WSUS 버전 6.3 포함)
- Cisco ASA 버전 9.3.1 이상
- Cisco ISE 소프트웨어 버전 1.3 이상

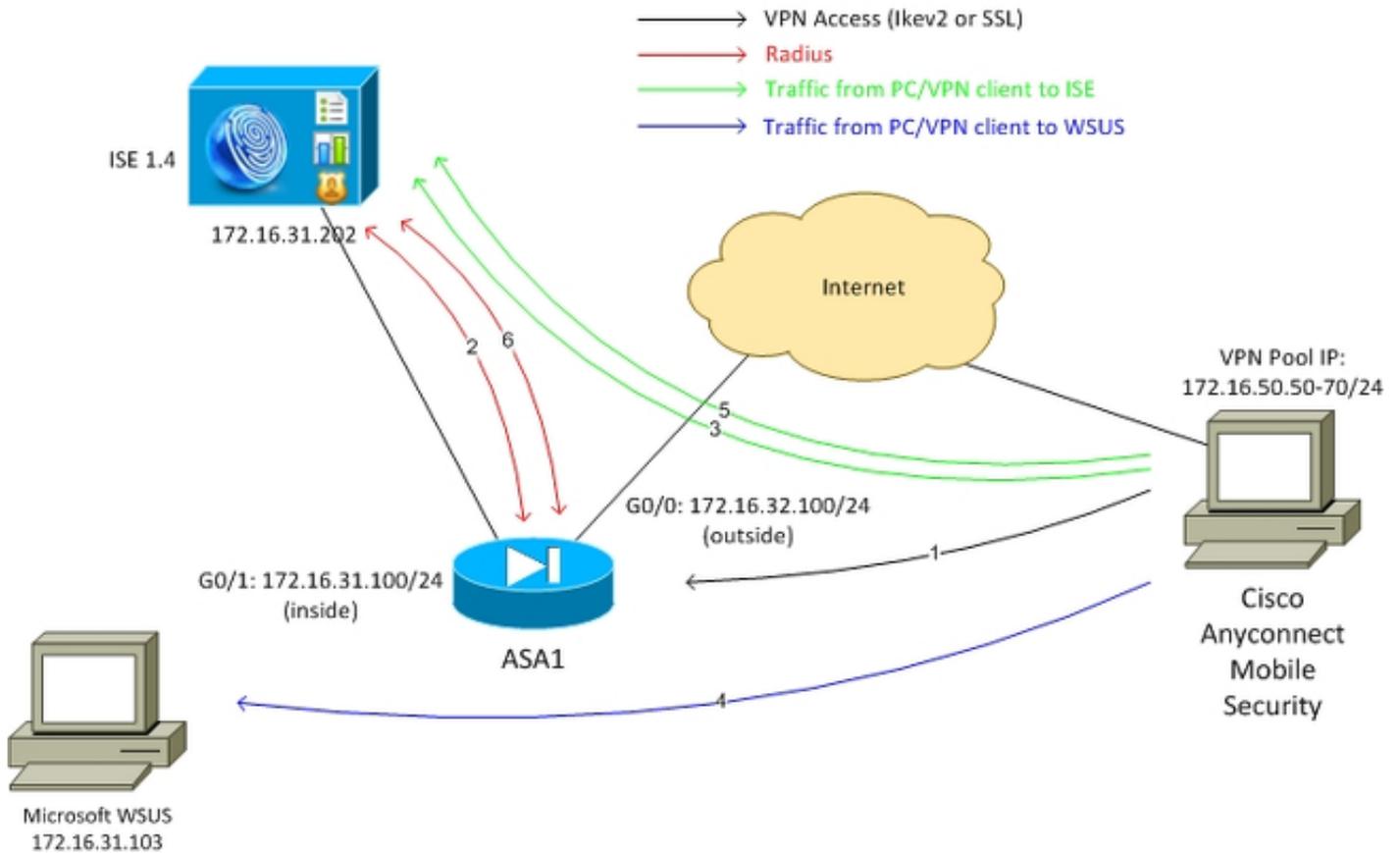
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 ISE 및 관련 네트워크 요소를 구성하는 방법에 대해 설명합니다.

네트워크 다이어그램

이 문서의 예제에 사용되는 토폴로지입니다.



다음은 네트워크 다이어그램에 표시된 트래픽 흐름입니다.

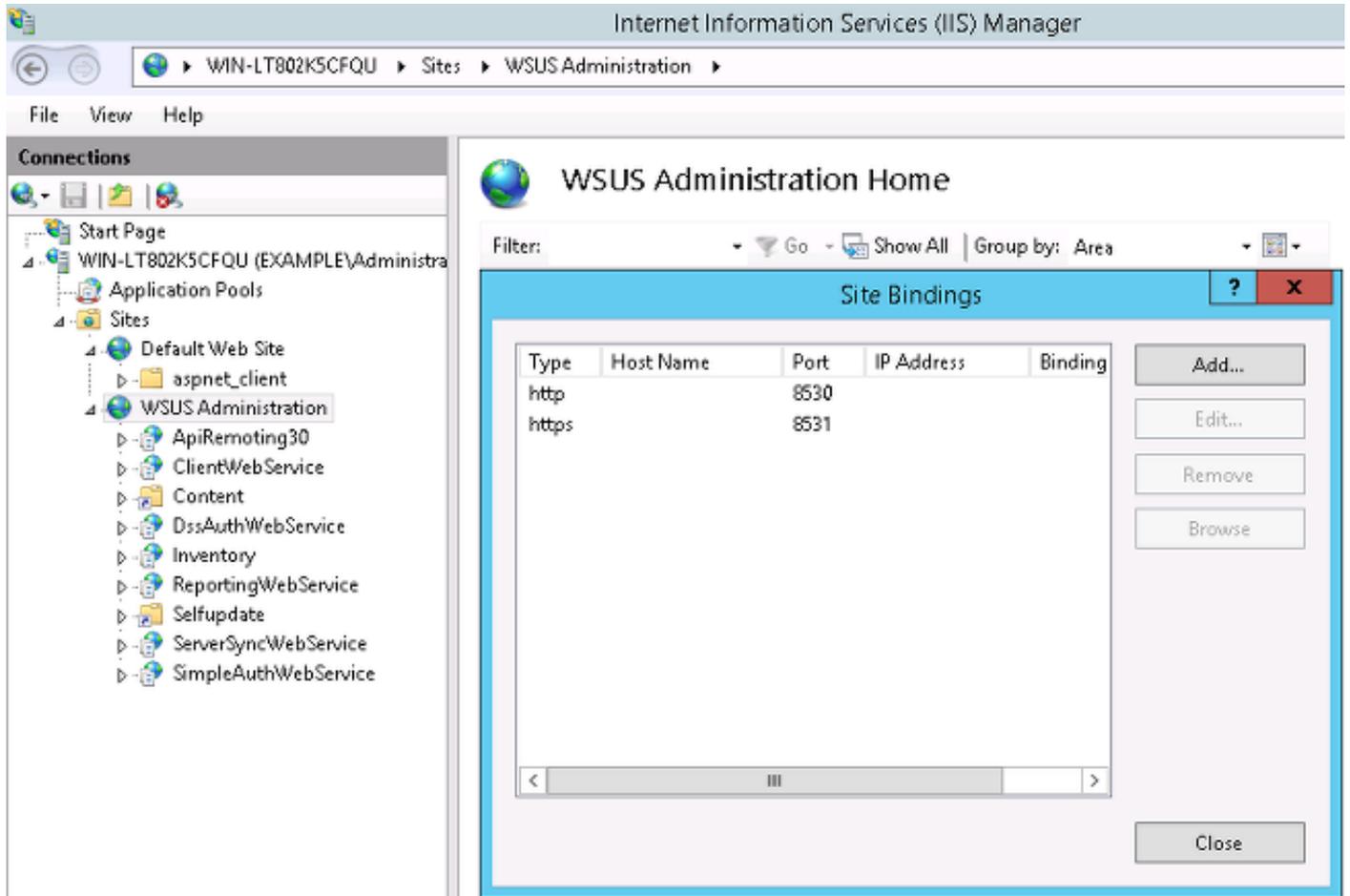
- 원격 사용자는 ASA에 대한 VPN 액세스를 위해 Cisco AnyConnect를 통해 연결합니다. 이는 스위치에서 종료되는 802.1x/MAB(MAC Authentication Bypass) 유선 세션 또는 WLC(Wireless LAN Controller)에서 종료되는 무선 세션과 같은 모든 유형의 통합 액세스가 될 수 있습니다.
- 인증 프로세스의 일부로서, ISE는 엔드 스테이션의 상태 상태가 규정 준수(ASA-VPN_quarantine 권한 부여 규칙)와 같지 않으며 리디렉션 특성이 Radius Access-Accept 메시지에 반환되는지 확인합니다. 따라서 ASA는 모든 HTTP 트래픽을 ISE로 리디렉션합니다.
- 사용자가 웹 브라우저를 열고 주소를 입력합니다. ISE로 리디렉션을 수행한 후 Cisco AnyConnect 4 포스터 모듈이 스테이션에 설치됩니다. 그런 다음 상태 모듈은 ISE에서 정책을 다운로드합니다(WSUS에 대한 요구 사항).
- 포스터 모듈은 Microsoft WSUS를 검색하고 리미디에이션을 수행합니다.
- 성공적으로 교정이 완료되면 상태 모듈이 ISE에 보고서를 보냅니다.
- ISE는 호환 VPN 사용자(ASA-VPN_호환 권한 부여 규칙)에 대한 전체 네트워크 액세스를 제공하는 CoA(Radius Change of Authorization)를 발행합니다.

참고: 교정이 작동하려면(PC에 Microsoft Windows 업데이트를 설치하는 기능) 사용자에게 로컬 관리 권한이 있어야 합니다.

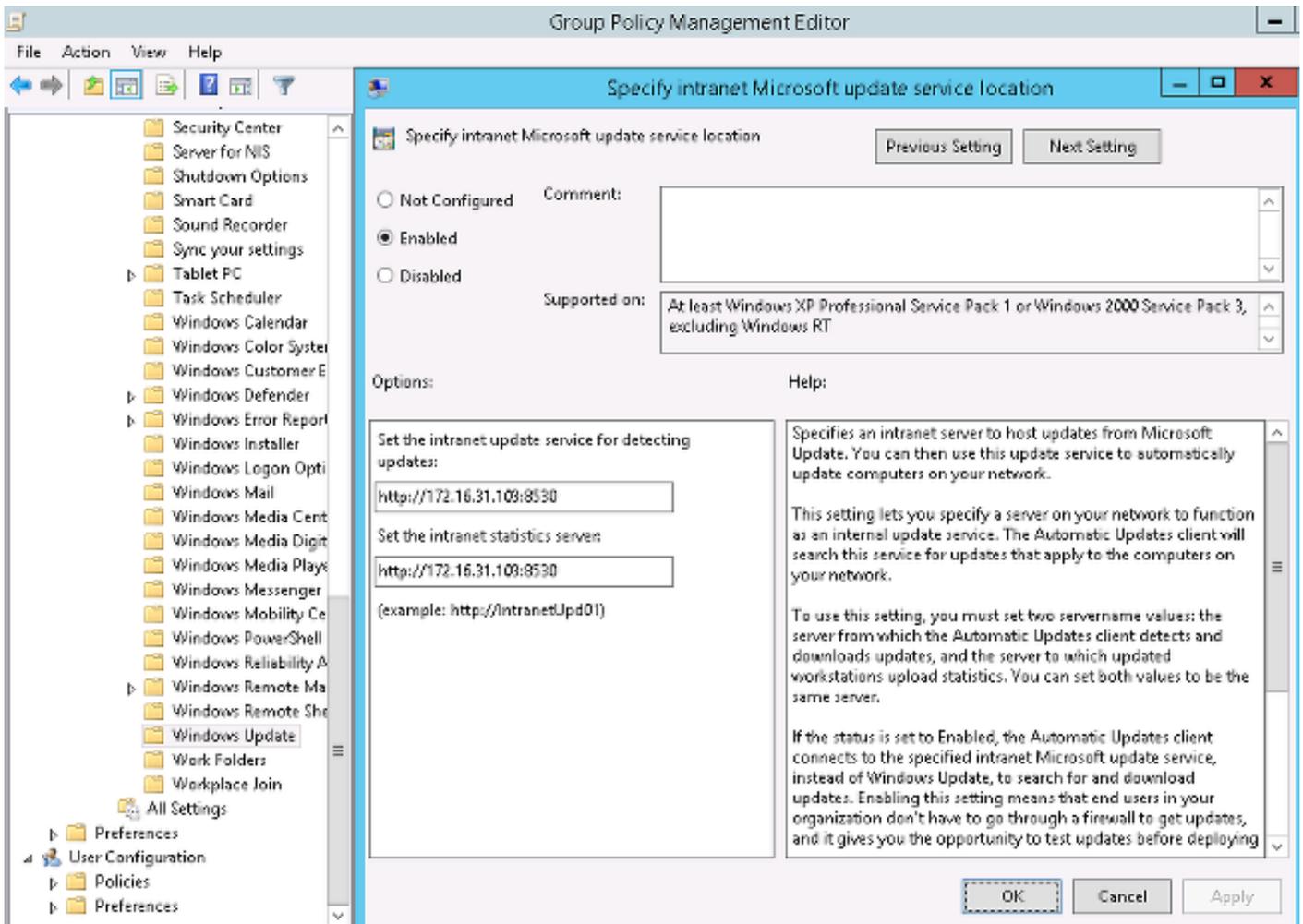
Microsoft WSUS

참고: WSUS의 자세한 구성은 이 문서의 범위를 벗어납니다. 자세한 내용은 [조직 Microsoft에서 Windows Server Update Services 배포](#) 설명서를 참조하십시오.

WSUS 서비스는 표준 TCP 포트 8530을 통해 구축됩니다. 교정에 다른 포트도 사용된다는 점을 기억해야 합니다. 따라서 WSUS의 IP 주소를 ASA의 리디렉션 ACL(Access Control List)에 추가해야 합니다(이 문서의 뒷부분에 설명).



도메인에 대한 그룹 정책은 Microsoft Windows 업데이트를 위해 구성되었으며 로컬 WSUS 서버를 가리킵니다.



다음은 여러 심각도 수준을 기반으로 하는 세분화된 정책에 대해 활성화된 권장 업데이트입니다.

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
Turn on recommended updates via Automatic Updates	Enabled
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

클라이언트 측 표적화는 훨씬 더 큰 유연성을 제공합니다. ISE는 다른 Microsoft AD(Active

Directory) 컴퓨터 컨테이너를 기반으로 하는 포스처 정책을 사용할 수 있습니다.WSUS는 이 구성원 자격을 기반으로 하는 업데이트를 승인할 수 있습니다.

ASA

원격 사용자에게 대한 SSL(Simple Secure Sockets Layer) VPN 액세스가 사용됩니다(자세한 내용은 이 문서의 범위를 벗어남).

다음은 컨피그레이션의 예입니다.

```
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
```

ISE로 리디렉션되어야 하는 트래픽을 확인하기 위해 사용되는 ASA에서 액세스 목록을 구성하는 것이 중요합니다(아직 규정을 준수하지 않는 사용자의 경우).

```
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
```

DNS(Domain Name System), ISE, WSUS 및 ICMP(Internet Control Message Protocol) 트래픽만 비준수 사용자에게 허용됩니다.다른 모든 트래픽(HTTP)은 AnyConnect 4 프로비저닝을 위한

ISE로 리디렉션되며, 이는 포스터 및 리미디에이션을 담당합니다.

ISE

참고: AnyConnect 4 프로비저닝 및 포스터는 이 문서의 범위를 벗어납니다. ASA를 네트워크 디바이스로 구성하고 Cisco AnyConnect 7 애플리케이션 설치 방법 등 자세한 내용은 [AnyConnect 4.0 Integration with ISE Version 1.3 Configuration Example](#)을 참조하십시오.

WSUS에 대한 상태 개선

WSUS에 대한 상태 개선을 구성하려면 다음 단계를 완료합니다.

1. 새 규칙을 생성하려면 **Policy > Conditions > Posture > Remediation Actions > Windows Server Update Services Remediation**으로 이동합니다.

2. *Microsoft Windows Updates* 설정이 Severity Level로 설정되어 있는지 **확인**합니다. 이 부품은 교정 프로세스가 시작되면 탐지를 담당합니다.

그런 다음 Microsoft Windows Update 에이전트는 WSUS에 연결하여 설치 대기 중인 PC에 대한 중요 업데이트가 있는지 확인합니다.

The screenshot shows the Cisco ISE Policy configuration interface. The top navigation bar includes 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, and Requirements. Under Remediation Actions, 'Windows Server Update Services Remediation' is selected. The main configuration area is titled 'Windows Server Update Services Remediation' and contains the following settings:

- Name: WSUS-Remediation
- Description: (empty)
- Remediation Type: Automatic
- Interval: 0
- Retry Count: 0
- Validate Windows updates using: Cisco Rules Severity Level
- Windows Updates Severity Level: Critical
- Update to latest OS Service Pack:
- Windows Updates Installation Source: Microsoft Server Managed Server
- Installation Wizard Interface Setting: Show UI No UI

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

WSUS에 대한 상태 요구 사항

새 규칙을 생성하려면 **Policy > Conditions > Posture > Requirements**로 이동합니다. 규칙은 pr_WSUSRule이라는 더미 조건을 사용합니다. 즉, 교정이 필요할 때 조건을 확인하기 위해 WSUS에 연결됩니다(중요 업데이트).

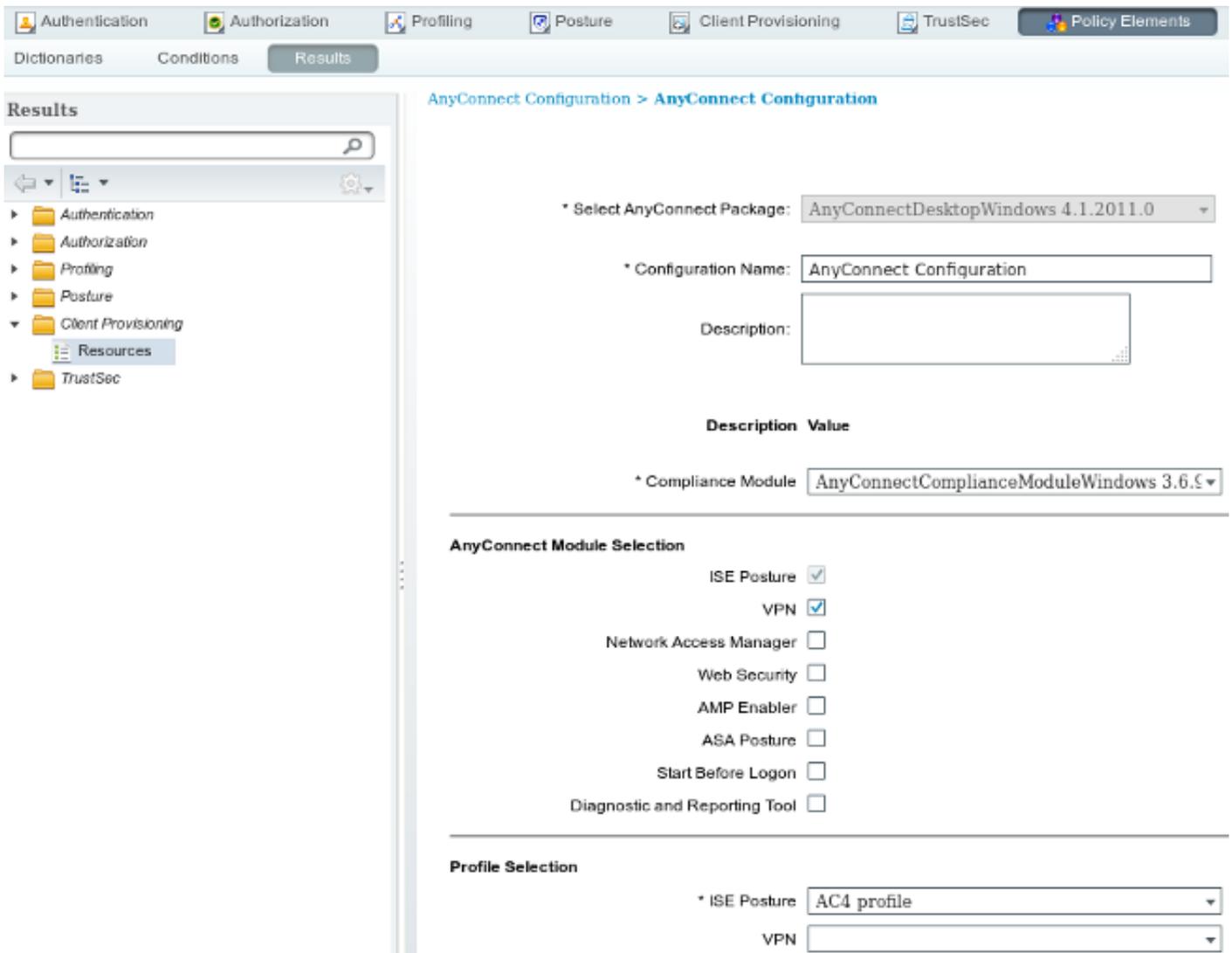
이 조건이 충족되면 WSUS는 해당 PC에 대해 구성된 업데이트를 설치합니다. 여기에는 모든 유형

의 업데이트와 심각도가 낮은 업데이트가 포함될 수 있습니다.

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

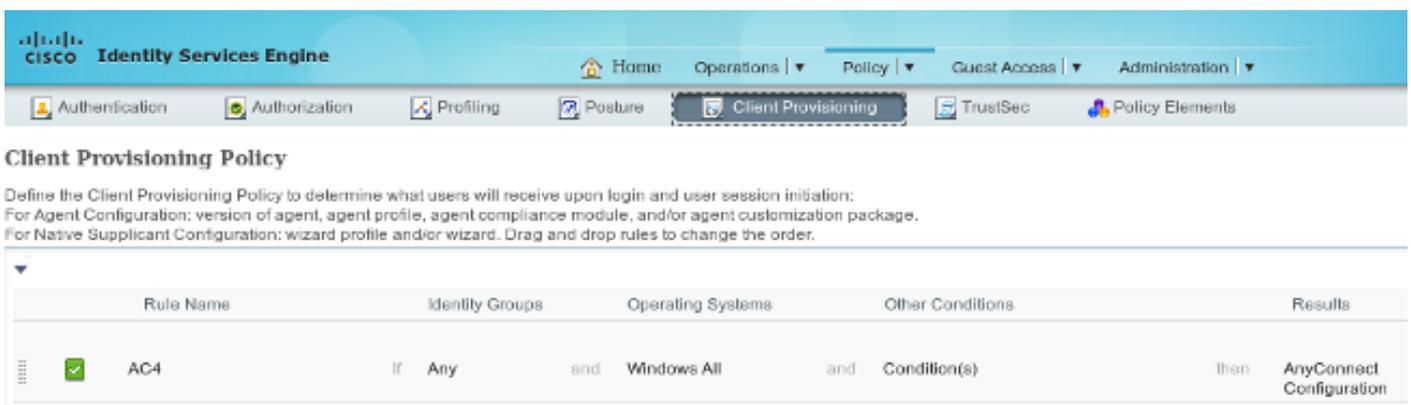
AnyConnect 프로파일

AnyConnect 4.0 Integration with ISE Version [1.3 Configuration Example](#)에 설명된 대로 AnyConnect 4 프로파일과 함께 포스터 모듈 프로파일을 구성합니다.



클라이언트 프로비저닝 규칙

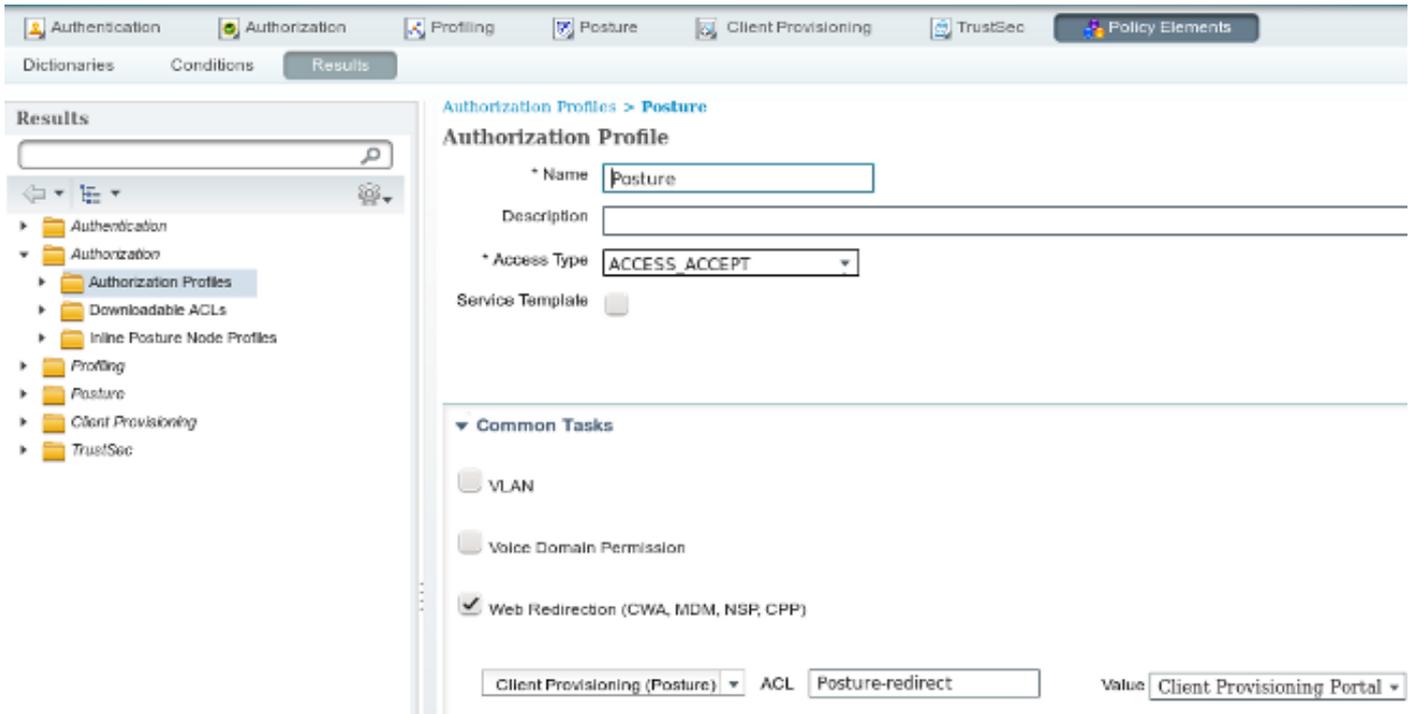
AnyConnect 프로파일이 준비되면 *클라이언트 프로비저닝* 정책에서 이를 참조할 수 있습니다.



컨피그레이션과 함께 전체 애플리케이션이 엔드포인트에 설치되며, 이는 클라이언트 프로비저닝 포털 페이지로 리디렉션됩니다. AnyConnect 4가 업그레이드되고 추가 모듈(상태)이 설치될 수 있습니다.

권한 부여 프로파일

클라이언트 프로비저닝 프로파일로 리디렉션하기 위한 권한 부여 프로파일을 만듭니다.



권한 부여 규칙

이 그림에서는 권한 부여 규칙을 보여 줍니다.

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

처음으로 *ASA-VPN_quarantine* 규칙이 사용됩니다. 따라서 *Posture* 권한 부여 프로파일이 반환되고 엔드포인트는 AnyConnect 4(포스처 모듈 포함) 프로비저닝을 위한 클라이언트 프로비저닝 포털로 리디렉션됩니다.

규정 준수가 완료되면 *ASA-VPN_compliant* 규칙이 사용되며 전체 네트워크 액세스가 허용됩니다.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

업데이트된 GPO 정책이 있는 PC

PC가 도메인에 로그인한 후 WSUS 구성이 있는 도메인 정책을 푸시해야 합니다. 이는 VPN 세션이 설정되기 전(대역 외) 또는 로그인 전 시작 기능을 사용하는 경우(802.1x 유선/무선 액세스에도 사용할 수 있음) 이후에 발생할 수 있습니다.

Microsoft Windows 클라이언트에 올바른 구성이 적용되면 Windows Update 설정에서 이를 반영할 수 있습니다.

필요한 경우 GPO(그룹 정책 개체) 새로 고침 및 Microsoft Windows Update 에이전트 서버 검색을 사용할 수 있습니다.

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

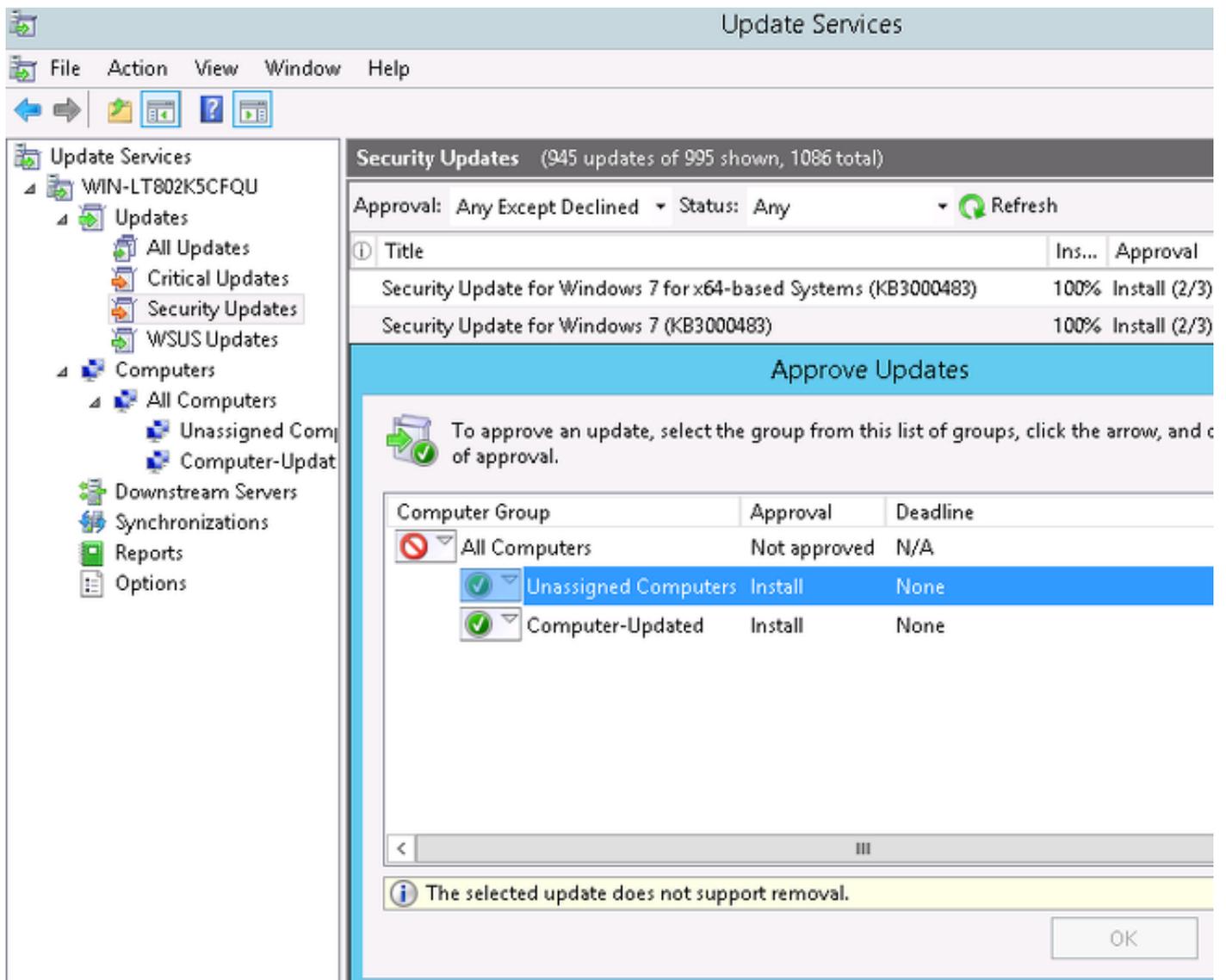
```
User Policy update has completed successfully.  
Computer Policy update has completed successfully.
```

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

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

WSUS에서 중요 업데이트 승인

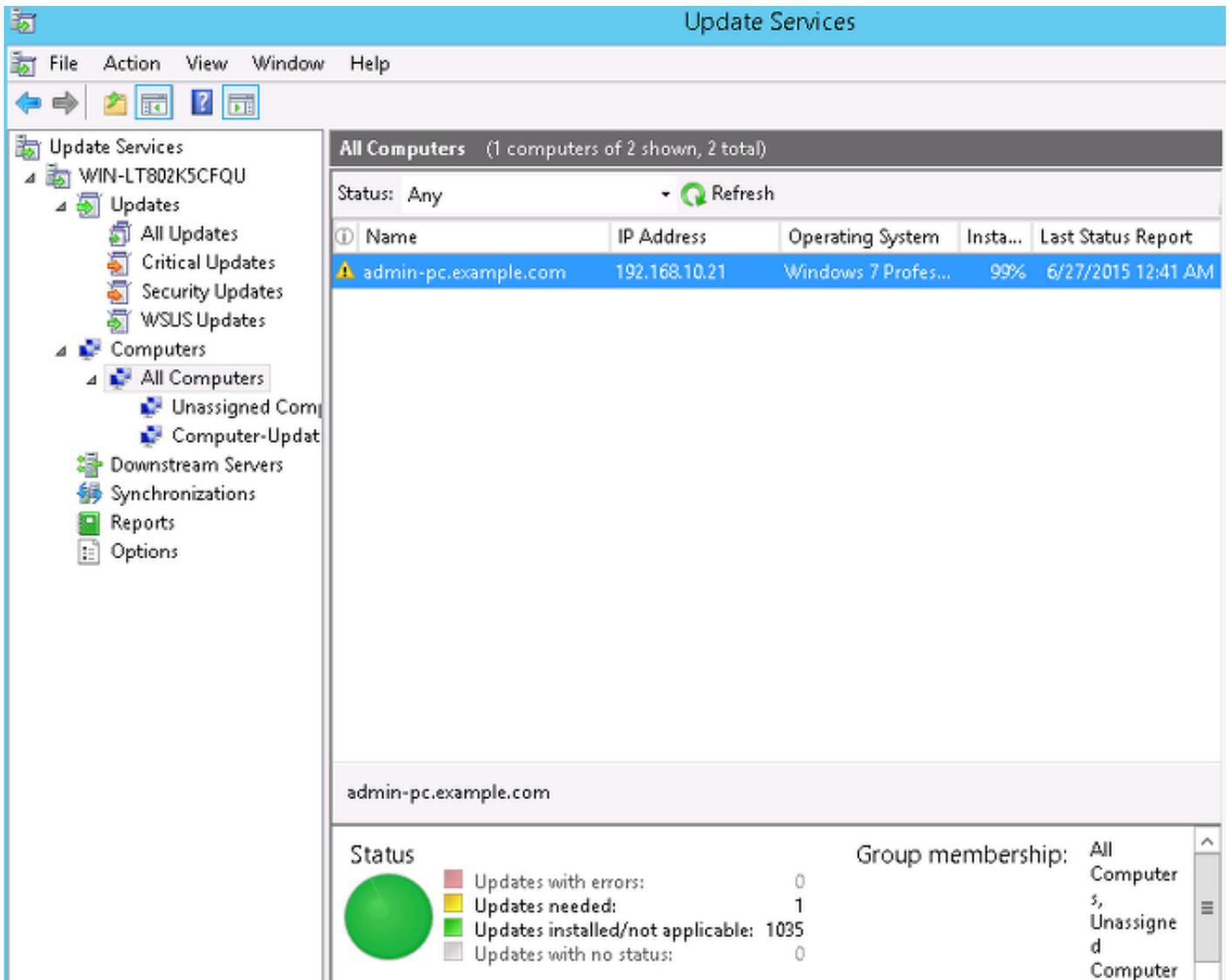
승인 프로세스는 클라이언트 사이트 대상 지정 시 다음과 같은 이점을 얻을 수 있습니다.



필요한 경우 보고서를 Wuauck으로 재전송합니다.

WSUS에서 PC 상태 확인

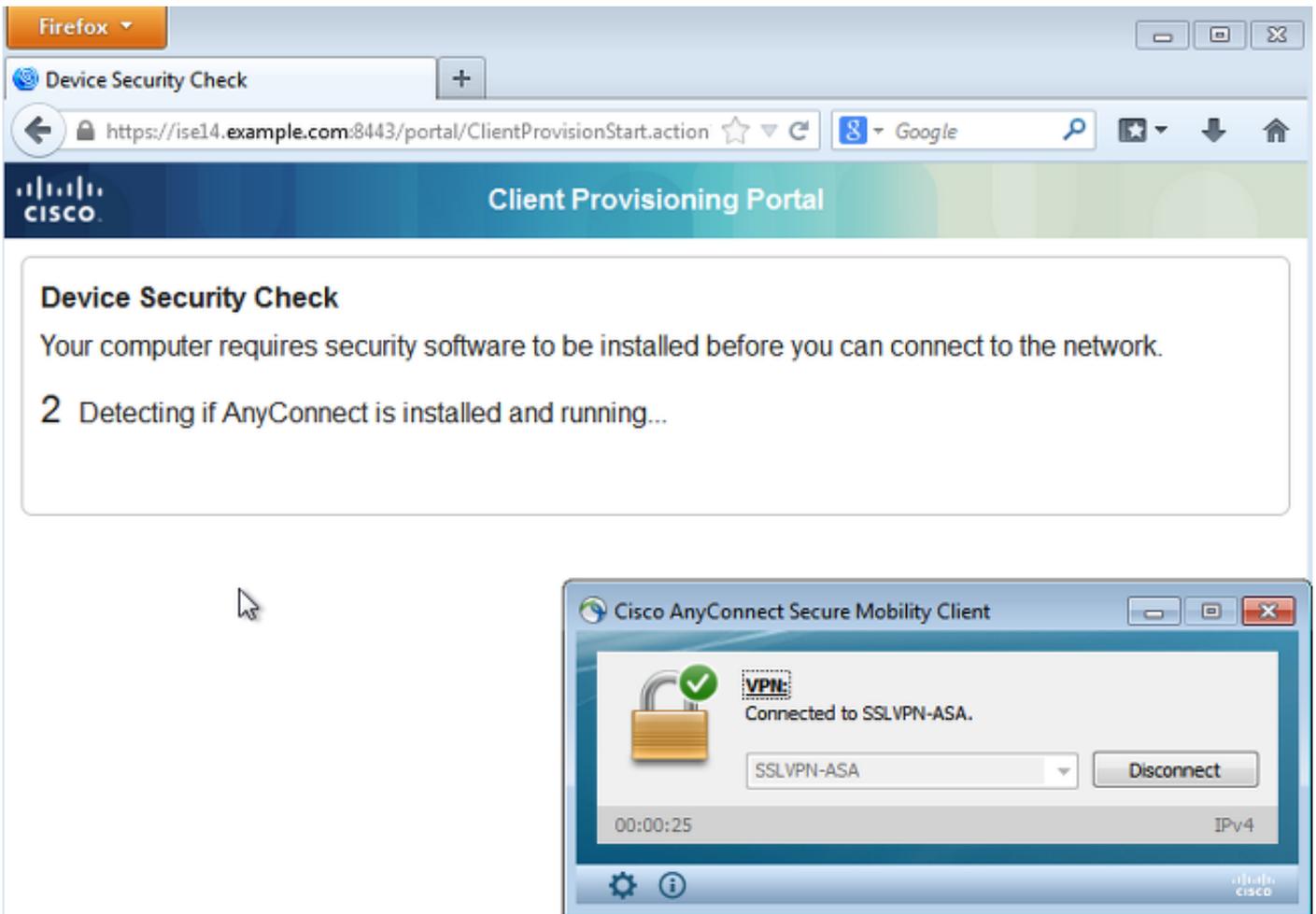
이 이미지는 WSUS에서 PC 상태를 확인하는 방법을 보여줍니다.



WSUS를 사용하여 다음 새로 고치려면 하나의 업데이트를 설치해야 합니다.

VPN 세션 설정

VPN 세션이 설정되면 *ASA-VPN_quarantine* ISE 권한 부여 규칙이 사용되며, 이 규칙은 *Posture* 권한 부여 프로파일을 반환합니다. 따라서 엔드포인트의 HTTP 트래픽은 AnyConnect 4 업데이트 및 포스처 모듈 프로비저닝을 위해 리디렉션됩니다.



이 시점에서 ASA의 세션 상태는 ISE로 HTTP 트래픽을 리디렉션하여 제한된 액세스를 나타냅니다.

```
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
```

포스처 모듈은 ISE에서 정책을 수신하고 교정 수행

포스처 모듈은 ISE에서 정책을 수신합니다. ise-psc.log 디버그는 상태 모듈에 전송되는 요구 사항을 표시합니다.

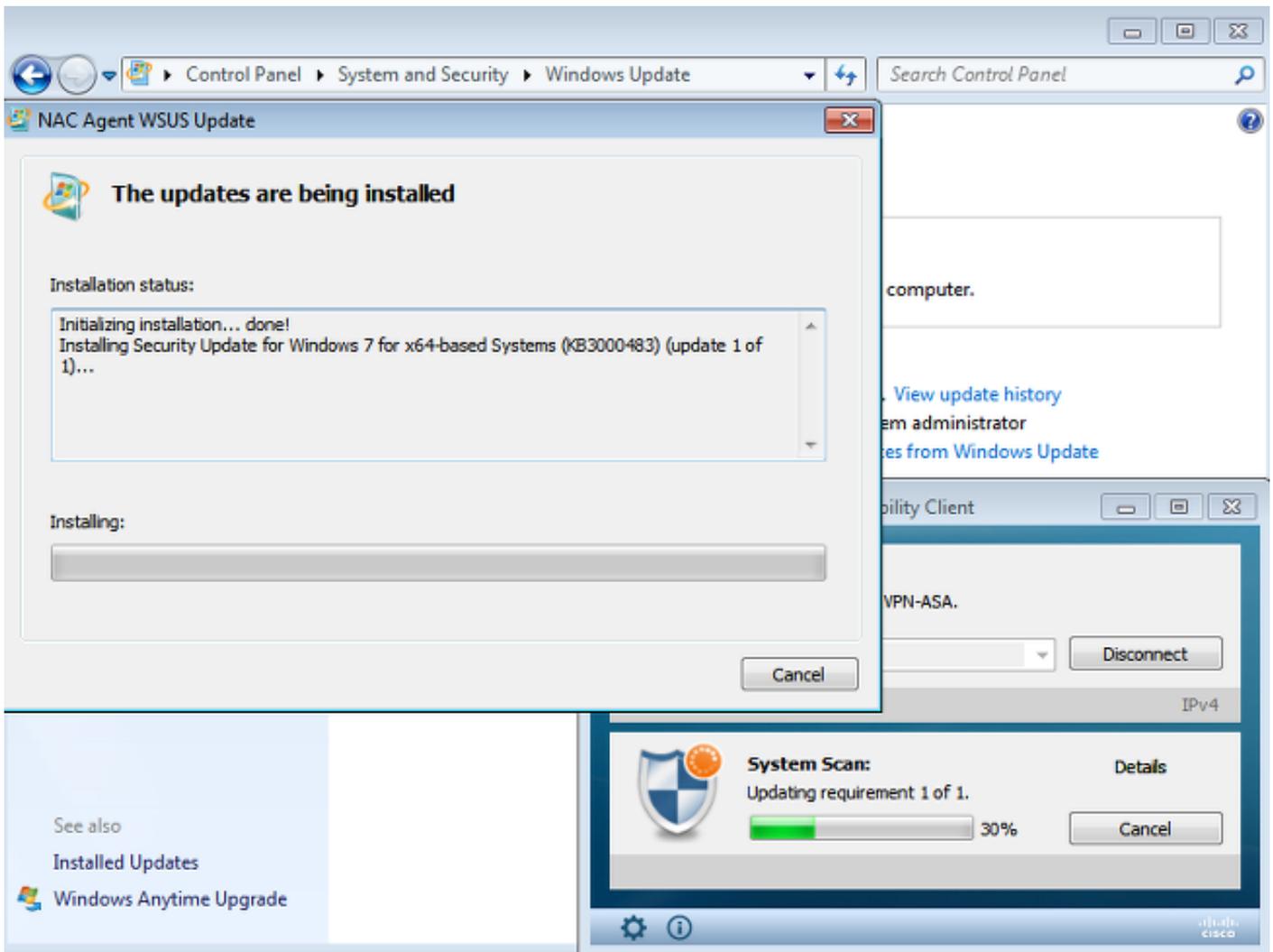
```
2015-06-05 07:33:40,493 DEBUG [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
<version>2</version>
<encryption>0</encryption>
<package>
<id>10</id>
```

```
<version/>
<description>This endpoint has failed check for any AS installation</description>
<type>10</type>
<optional>0</optional>
```

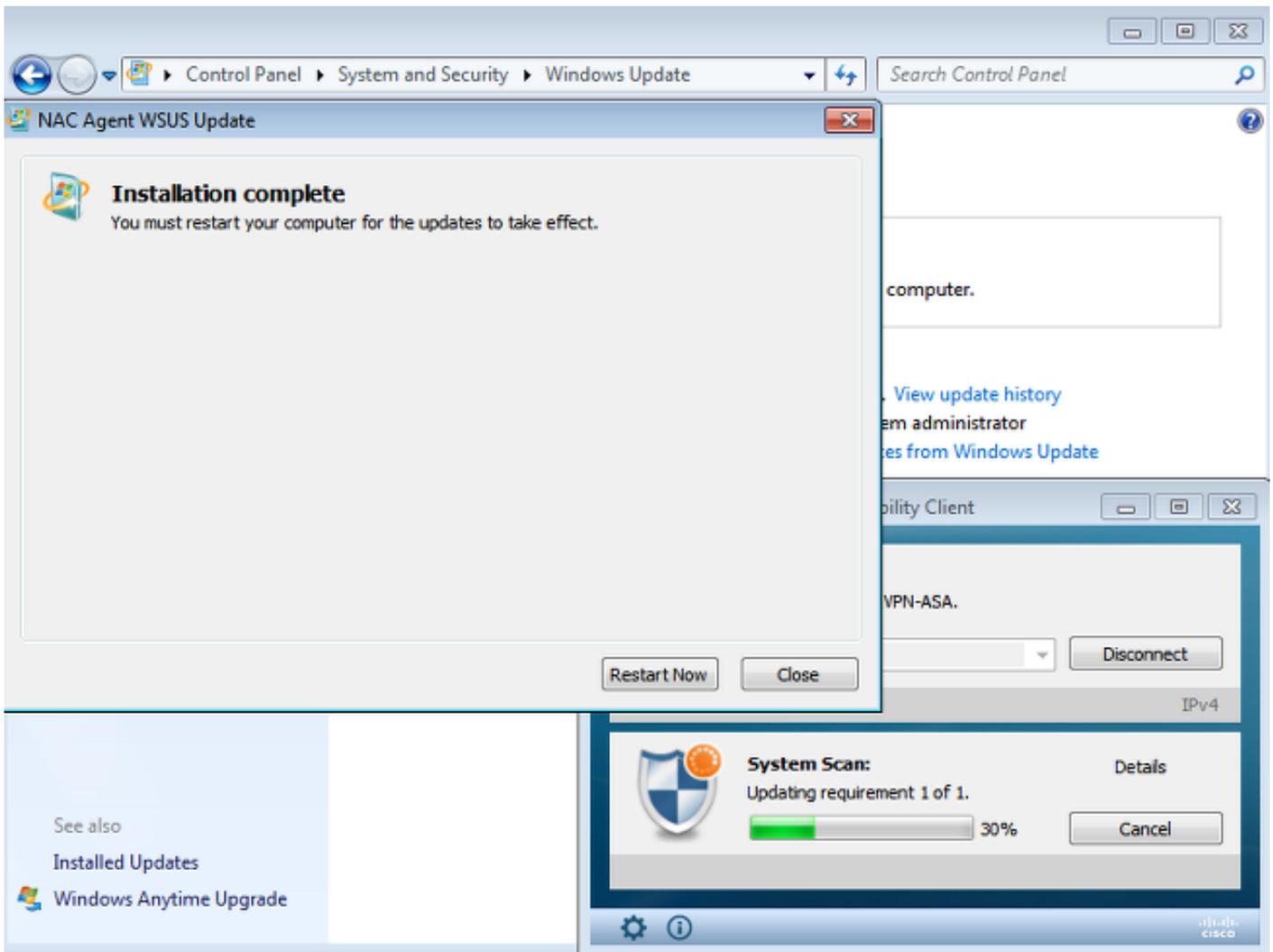
```
<remediation_type>1</remediation_type>
<remediation_retry>0</remediation_retry>
<remediation_delay>0</remediation_delay>
<action>10</action>
<check>
```

```
</check>
<criteria/>
</package>
</cleanmachines>
```

포스처 모듈은 Microsoft Windows Update 에이전트가 WSUS에 연결하도록 자동으로 트리거하고 WSUS 정책에 구성된 대로 업데이트를 다운로드합니다(사용자 개입 없이 모두 자동으로).

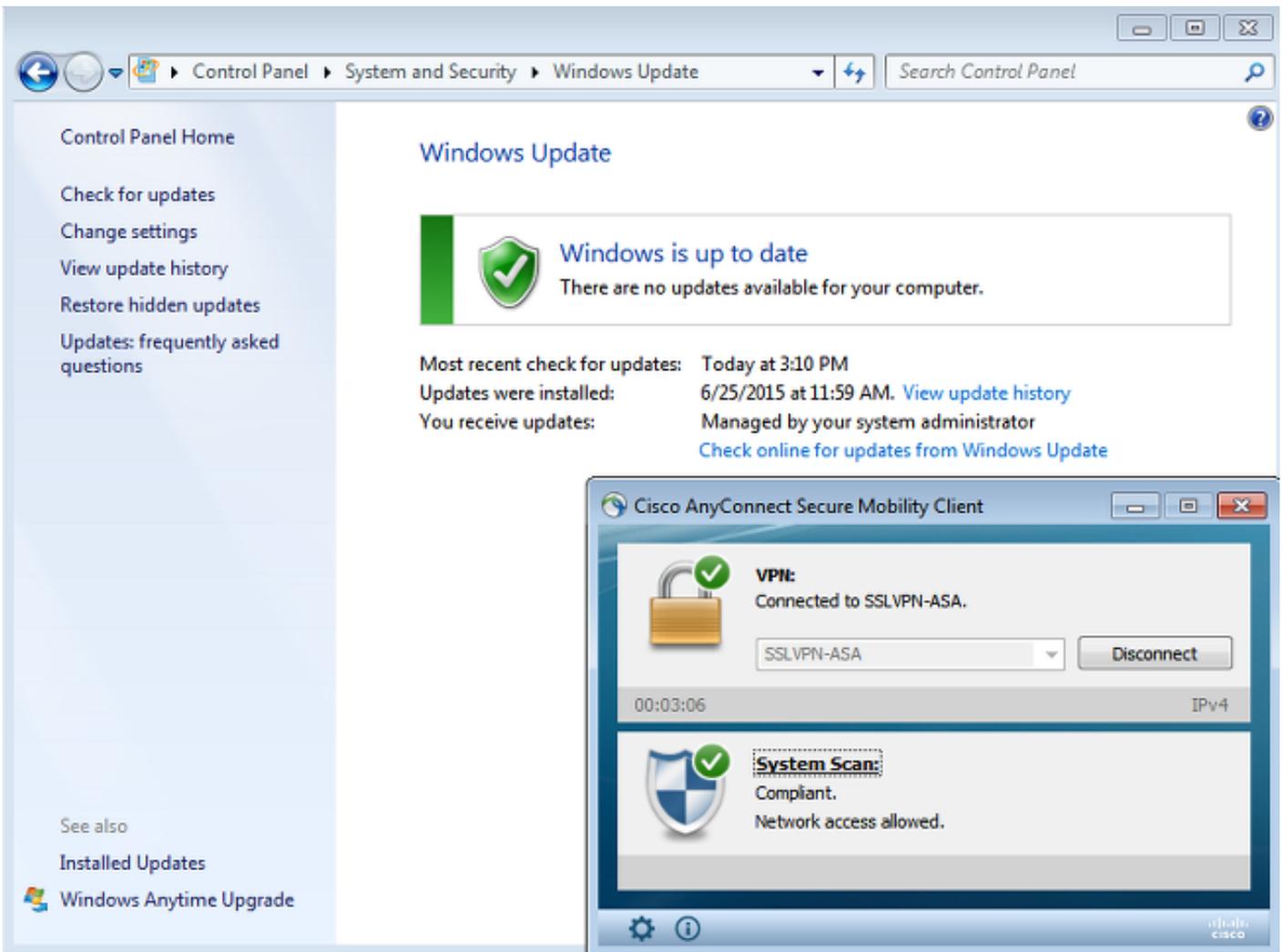


참고: 일부 업데이트는 시스템을 다시 시작해야 할 수 있습니다.

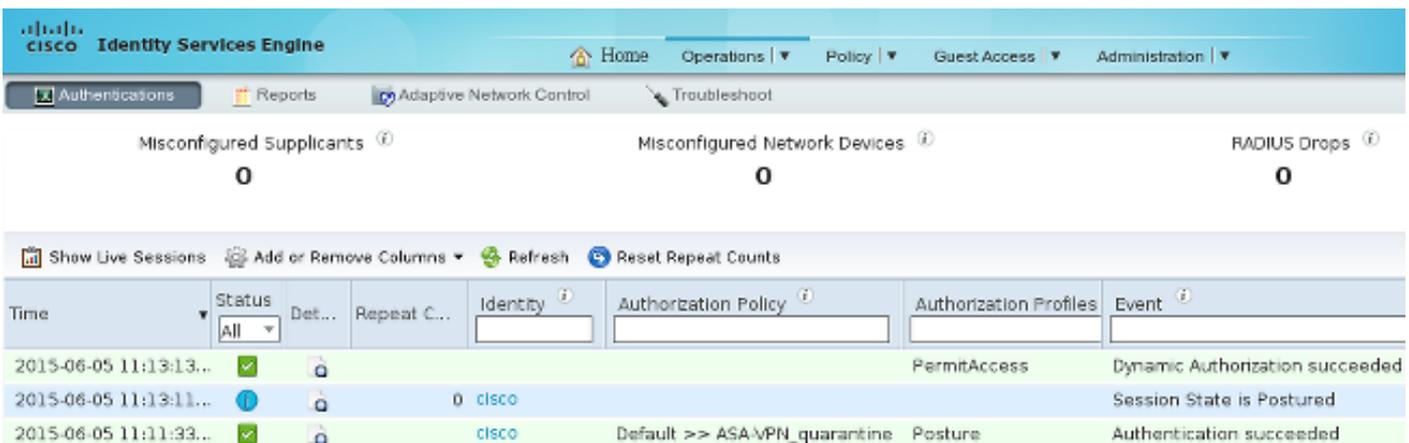


전체 네트워크 액세스

스테이션이 AnyConnect 포스터 모듈에 의해 규정 준수 상태로 보고되면 다음과 같이 표시됩니다.



보고서는 정책을 재평가하고 ASA-VPN_compliant 권한 부여 규칙에 도달하는 ISE로 전송됩니다. 이렇게 하면 전체 네트워크 액세스(Radius CoA를 통해)가 제공됩니다. Operations(운영) > Authentications(인증)로 이동하여 확인합니다.



디버그(ise-psc.log)는 또한 규정 준수 상태, CoA 트리거 및 상태에 대한 최종 설정을 확인합니다.

```
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]
```

또한 ISE Detailed Posture Assessment 보고서에서는 스테이션이 규정을 준수함을 확인합니다.

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

참고:Microsoft Windows PC의 물리적 네트워크 인터페이스의 정확한 MAC(Media Access Control) 주소는 ACIDEX 확장으로 알려져 있습니다.

문제 해결

현재 이 구성에 사용할 수 있는 문제 해결 정보가 없습니다.

중요 참고 사항

이 섹션에서는 이 문서에 설명된 구성에 대한 몇 가지 중요한 정보를 제공합니다.

WSUS 교정에 대한 옵션 세부 정보

요구 사항 조건을 교정과 구분하는 것이 중요합니다.AnyConnect는 *Validate Windows updates using remediation* 설정에 따라 Microsoft Windows Update Agent가 규정 준수를 확인하도록 트리거합니다.

Windows Server Update Services Remediation

* Name	<input type="text" value="WSUS-Remediation"/>	
Description	<input type="text"/>	
Remediation Type	<input type="text" value="Automatic"/>	
Interval	<input type="text" value="0"/>	(in secs) (Valid Range 0 to 9999)
Retry Count	<input type="text" value="0"/>	(Valid Range 0 to 99)
Validate Windows updates using	<input type="radio"/> Cisco Rules <input checked="" type="radio"/> Severity Level	
Windows Updates Severity Level	<input type="text" value="Medium"/>	
	<input type="checkbox"/> Update to latest OS Service Pack	
Windows Updates Installation Source	<input type="radio"/> Microsoft Server <input checked="" type="radio"/> Managed Server	
Installation Wizard Interface Setting	<input checked="" type="radio"/> Show UI <input type="radio"/> No UI	

이 예에서는 *Severity Level*이 사용됩니다.중요 설정을 사용하면 Microsoft Windows 에이전트가 보류 중인 중요 업데이트가 있는지 확인합니다.있는 경우 교정이 시작됩니다.

그런 다음 리미디에이션 프로세스는 WSUS 컨피그레이션에 따라 중요하며 덜 중요한 모든 업데이트를 설치할 수 있습니다(특정 시스템에 대해 승인된 업데이트).

Validate Windows updates using set as **Cisco Rules**(Cisco 규칙으로 설정을 사용하여 Validate Windows 업데이트를 사용할 경우, 요구 사항에 자세히 나와 있는 조건이 스테이션의 준수 여부를 결정합니다.

Windows 업데이트 서비스

WSUS 서버가 없는 구축의 경우 *Windows Update Remediation*이라고 할 수 있는 다른 교정 유형이 있습니다.

Windows Update Remediation

* Name	<input type="text" value="WindowsUpdate"/>	i
Description	<input type="text"/>	
Remediation Type	<input type="text" value="Automatic"/>	
Interval	<input type="text" value="0"/>	(in secs) (Valid Range 0 to 9999)
Retry Count	<input type="text" value="0"/>	(Valid Range 0 to 99)
Windows Update Setting	<input type="text" value="Automatically do"/>	
Override User's Windows Update setting with administrator's	<input type="checkbox"/>	

이 교정 유형을 사용하면 Microsoft Windows Update 설정을 제어할 수 있으며 즉시 업데이트를 수행할 수 있습니다. 이 교정 유형과 함께 사용되는 일반적인 조건은 *pc_AutoUpdateCheck*입니다. 이렇게 하면 엔드포인트에서 Microsoft Windows Update 설정이 활성화되어 있는지 확인할 수 있습니다. 그렇지 않은 경우 이를 활성화하고 업데이트를 수행할 수 있습니다.

SCCM 통합

ISE 버전 1.4의 새로운 기능인 *패치 관리*를 사용하면 많은 타사 공급업체와 통합할 수 있습니다. 공급업체에 따라 여러 가지 옵션을 조건 및 교정에 사용할 수 있습니다.

Microsoft의 경우 SMS(System Management Server) 및 SCCM(System Center Configuration Manager)이 모두 지원됩니다.

관련 정보

- [Cisco ISE 컨피그레이션 가이드의 포스터 서비스](#)
- [Cisco Identity Services Engine 관리자 가이드, 릴리스 1.4](#)
- [Cisco Identity Services Engine 관리자 가이드, 릴리스 1.3](#)
- [조직에 Windows Server Update Services 배포](#)
- [기술 지원 및 문서 - Cisco Systems](#)