

ISE versie 1.4 Poststellen met Microsoft Word configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Microsoft WSUS](#)

[ASA](#)

[ISE](#)

[500 Restatie voor WSUS](#)

[Postvereisten voor WSUS](#)

[AnyConnect-profiel](#)

[Clientprovisioningregels](#)

[Verificatieprofielen](#)

[machtigingsregels](#)

[Verifiëren](#)

[Pc met bijgewerkt GPO-beleid](#)

[Een kritische update in het WSUS goedkeuren](#)

[Controleer de PC-status op het WSUS](#)

[VPN-sessie ingesteld](#)

[Postmodule Ontvang beleid van ISE en voert verbetering uit](#)

[Volledige netwerktoegang](#)

[Problemen oplossen](#)

[Belangrijke opmerkingen](#)

[Optiegegevens voor WSUS-verbetering](#)

[Windows Update Service](#)

[SCCM-integratie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de functie Cisco Identity Services Engine (ISE) kunt configureren wanneer deze is geïntegreerd in de Microsoft Windows Server Update Services (WSUS).

Opmerking: Wanneer u tot het netwerk toegang hebt, wordt u opnieuw naar ISE gericht voor

Cisco AnyConnect Secure Mobility Client versie 4.1 met een postmodule, die de nalevingsstatus op het WSUS controleert en de benodigde updates installeert om het station te conformeren. Zodra het station als compatibel is gemeld, biedt ISE volledige toegang tot het netwerk.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE-implementaties, verificatie en autorisatie
- Basiskennis van de manier waarop ISE en Cisco AnyConnect-functieagent werken
- Configuratie van de Cisco adaptieve security applicatie (ASA)
- Basiskennis van VPN en 802.1x
- Configuratie van de Microsoft WSUS-software

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows versie 7
- Microsoft Windows versie 2012 met WBS versie 6.3
- Cisco ASA versies 9.3.1 en hoger
- Cisco ISE-softwareversies 1.3 en hoger

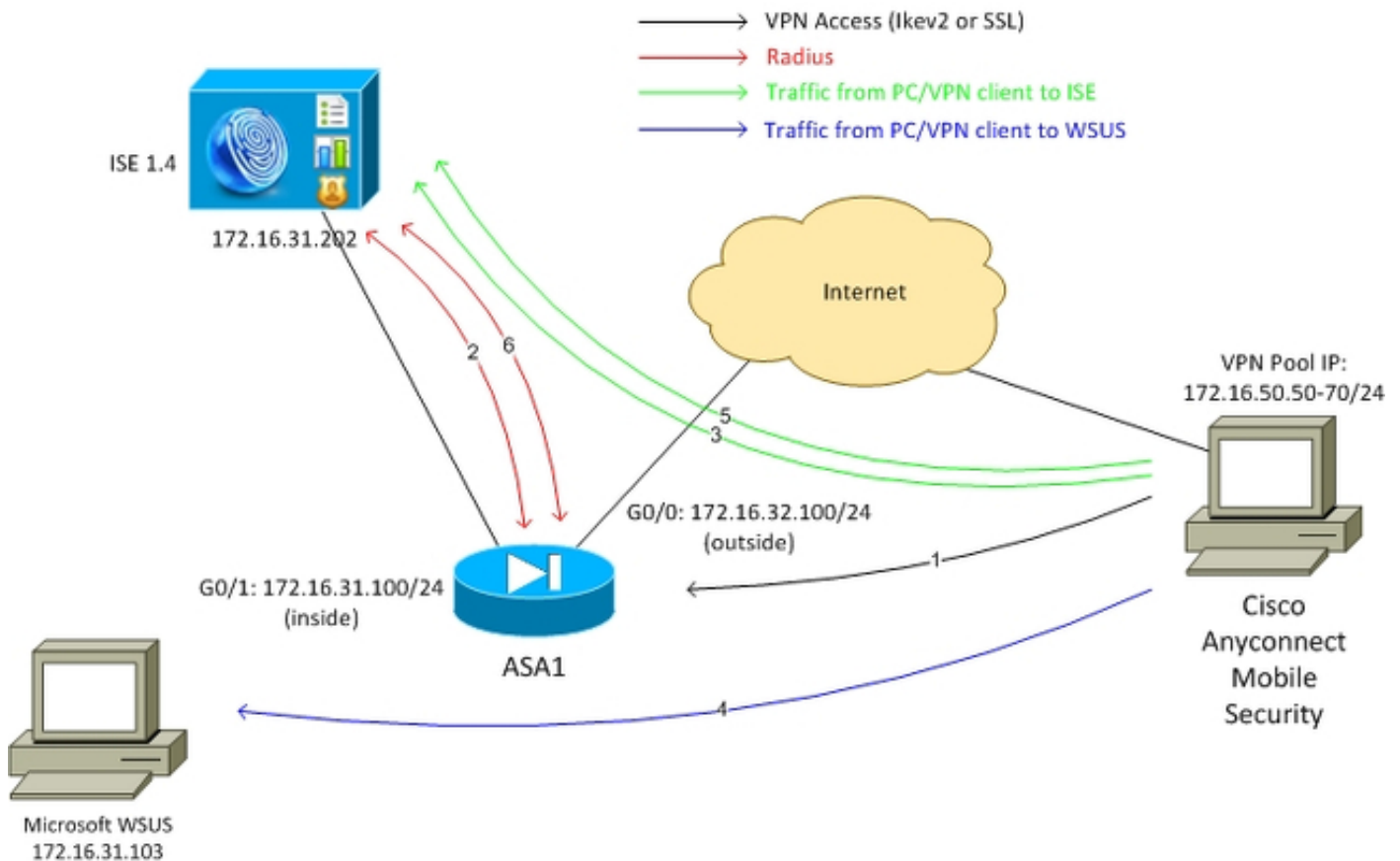
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

In deze sectie wordt beschreven hoe u de ISE en verwante netwerkelementen kunt configureren.

Netwerkdigram

Dit is de topologie die voor de voorbeelden door dit document wordt gebruikt:



Hier is de verkeersstroom, zoals wordt geïllustreerd in het netwerkdiagram:

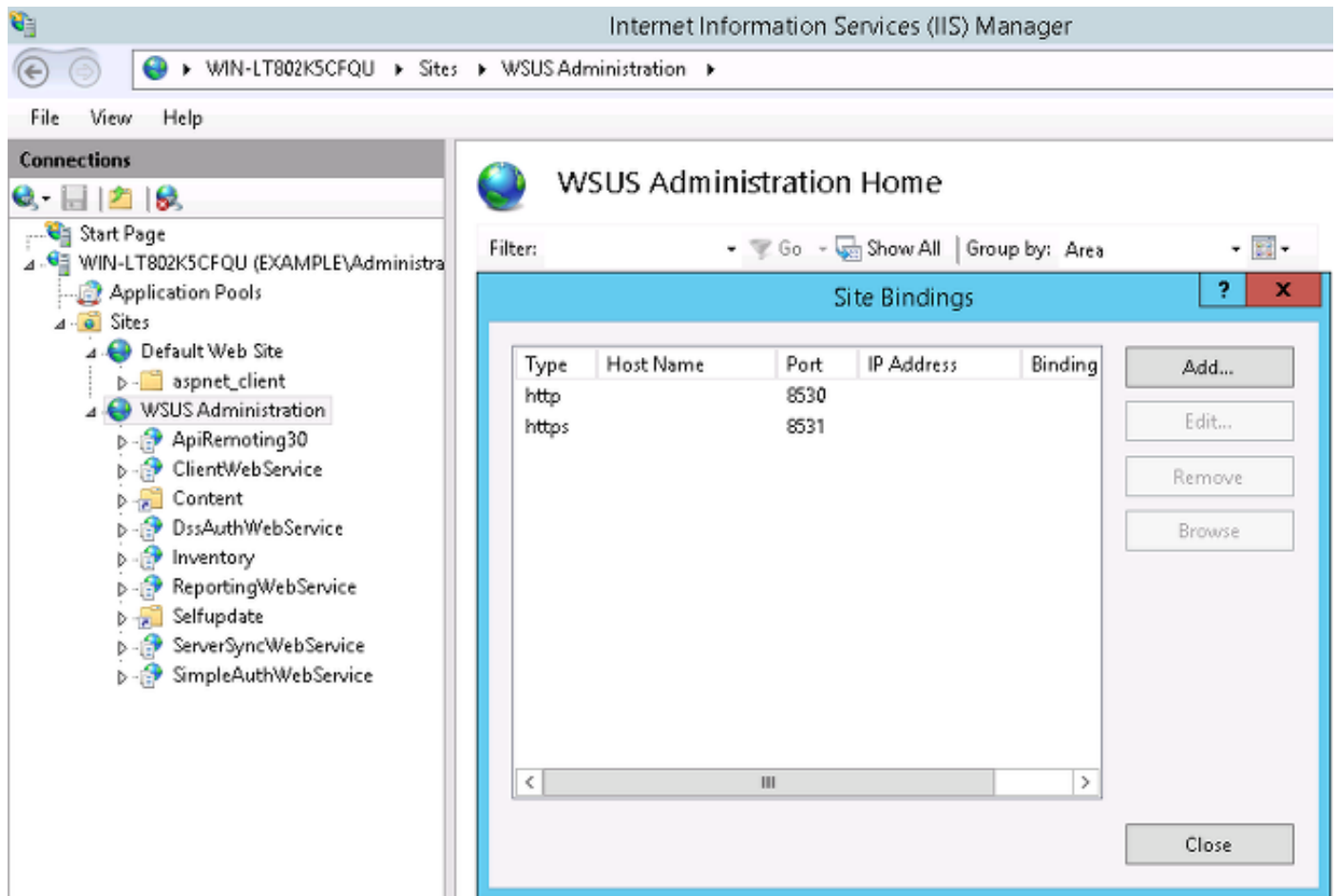
1. De externe gebruiker sluit zich aan via Cisco AnyConnect voor VPN-toegang tot de ASA. Dit kan elk type geünificeerde toegang zijn, zoals een bekabelde sessie van 802.1x/MAC-verificatie (MAB) die op de switch wordt afgesloten of een draadloze sessie die op de draadloze LAN-controller (WLC) wordt beëindigd.
2. Als onderdeel van het authenticatieproces bevestigt ISE dat de posterstatus van het eindstation niet gelijk is aan de conforme (*ASA-VPN_quarantaine* autorisatieregel) en dat de omleidingseigenschappen worden teruggegeven in het *Radius Access-Accept* bericht. Als resultaat hiervan richt de ASA al het HTTP verkeer naar ISE om.
3. De gebruiker opent een webbrowser en voert elk adres in. Nadat u de omleiding naar ISE hebt voltooid, is de Cisco AnyConnect 4 postmodule op het station geïnstalleerd. In de postmodule wordt het beleid vervolgens gedownload van de ISE (eis voor WSUS).
4. De postuur-module zoekt naar Microsoft WSUS en voert corrigerende maatregelen uit.
5. Na een geslaagde sanering stuurt de postmodule een rapport naar de ISE.
6. ISE geeft een Radius Change of Authorization (CoA) uit die volledige netwerktoegang biedt tot een conforme VPN-gebruiker (*ASA-VPN_conform* autorisatieregel).

Opmerking: De gebruiker moet lokale beheerrechten hebben, zodat het herstel kan werken (de mogelijkheid om Microsoft Windows updates op een pc te installeren).

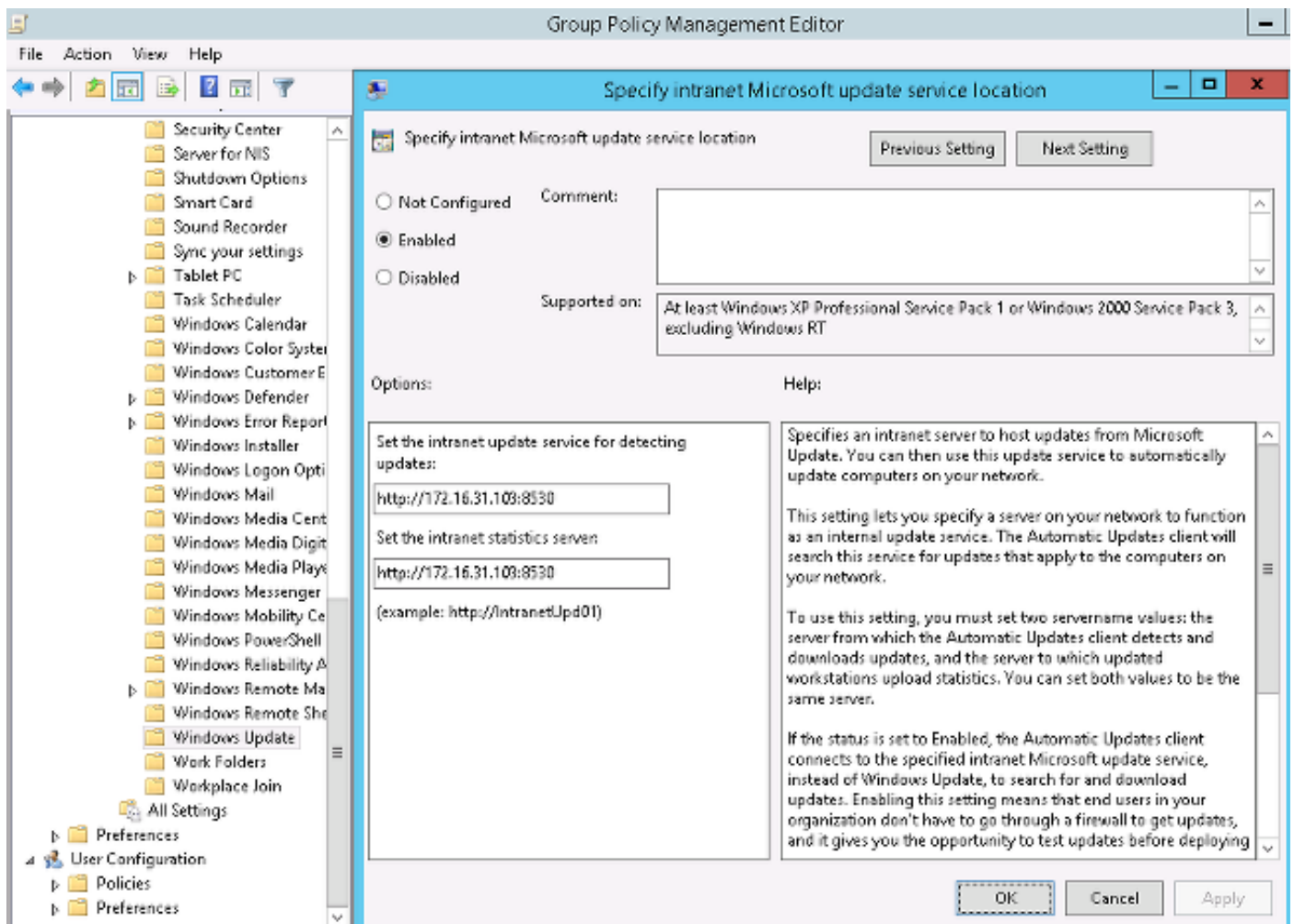
Microsoft WSUS

Opmerking: Een gedetailleerde configuratie van het WSUS is buiten het bereik van dit document. Raadpleeg de [Windows Server Update Services](#) implementeren [in uw](#) Microsoft-documentatie van [uw organisatie](#).

De WSUS-service wordt uitgevoerd via de standaard TCP-poort 8530. Het is belangrijk te bedenken dat voor sanering ook andere havens worden gebruikt. Dit is waarom het veilig is om het IP-adres van WSUS toe te voegen aan de toegangscontrolelijst (ACL) in de ASA (later beschreven in dit document).



Het groepsbeleid voor het domein is ingesteld voor Microsoft Windows-updates en wijst op de lokale WSUS-server:



Dit zijn de aanbevolen updates die beschikbaar zijn voor korrelig beleid dat gebaseerd is op verschillende niveaus van ernst:

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

De doelgerichtheid van de cliënt maakt een veel grotere flexibiliteit mogelijk. ISE kan postuur beleid gebruiken dat gebaseerd is op de verschillende Microsoft Active Directory (AD) computercontainers. Het WSUS kan updates goedkeuren die zijn gebaseerd op dit lidmaatschap.

ASA

Eenvoudige Secure Socket Layer (SSL) VPN-toegang voor de externe gebruiker wordt gebruikt (waarvan de details buiten het bereik van dit document zijn).

Hier is een voorbeeldconfiguratie:

```
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
```

Het is belangrijk om een toegangslijst op de ASA te vormen, die wordt gebruikt om het verkeer te bepalen dat naar ISE (voor gebruikers die nog niet voldoen) zou moeten worden verlegd:

```
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
```

Er is alleen ICMP-verkeer (Domain Name System), ISE, WSUS en Internet Control Message

Protocol (DNS) toegestaan voor niet-conforme gebruikers. Al het andere verkeer (HTTP) wordt naar ISE verwezen voor AnyConnect 4 provisioning, die verantwoordelijk is voor houding en herstel.

ISE

Opmerking: AnyConnect 4 provisioning en opstelling is buiten het bereik van dit document. Raadpleeg de [AnyConnect 4.0-integratie met ISE versie 1.3 Configuratievoorbeeld](#) voor meer informatie, zoals hoe u de ASA als netwerkapparaat kunt configureren en de Cisco AnyConnect 7-toepassing kunt installeren.

500 Restatie voor WSUS

Voltooi deze stappen om het herstel van de houding voor WSUS te configureren:

1. Navigeer in op **Policy > Voorwaarden > Posture > Remediation Actions > Windows Server Update Services Remediation** om een nieuwe regel te maken.
2. Controleer of de instelling *Microsoft Windows Update* op **ernst** is ingesteld. Dit onderdeel is verantwoordelijk voor de detectie als het herstelproces wordt gestart.

De Microsoft Windows Update Agent sluit zich dan aan op de WWUS en controleert of er *kritieke* updates voor die PC zijn die op installatie wachten:

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. Below this, there are sub-tabs for Dictionaries, Conditions, and Results. The main content area is titled "Windows Server Update Services Remediations List > WSUS-Remediation". The configuration form for "Windows Server Update Services Remediation" is shown with 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 visible at the bottom of the configuration form. On the left side, a tree view shows the navigation structure under "Remediation Actions", with "Windows Server Update Services Remediation" selected.

Postvereisten voor WSUS

Navigeer naar **beleid > Voorwaarden > Postvereisten** om een nieuwe regel te creëren. De regel gebruikt een dummy-voorwaarde genaamd *pr_WSUSRule*, wat betekent dat het WSUS

gecontacteerd wordt om de aandoening te controleren wanneer herstel nodig is (*Kritische updates*).

Zodra aan deze voorwaarde is voldaan, installeert het WWUS de updates die voor die PC zijn gevormd. Dit kan elk type updates omvatten, en ook updates met een lagere ernst:

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-profiel

Configureer het profiel van de postmodule met het AnyConnect 4-profiel (zoals beschreven in de [AnyConnect 4.0-integratie met ISE versie 1.3 Configuratievoorbeeld](#)):

The screenshot shows the Cisco ISE Policy Elements configuration interface. The top navigation bar includes tabs for 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 (expanded), Resources, and TrustSec. The main content area is titled 'AnyConnect Configuration > AnyConnect Configuration' and contains the following configuration fields:

- * Select AnyConnect Package: AnyConnectDesktopWindows 4.1.2011.0
- * Configuration Name: AnyConnect Configuration
- Description: (empty text area)
- * Compliance Module: AnyConnectComplianceModuleWindows 3.6.9

Below these fields is the 'AnyConnect Module Selection' section with the following options:

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

The 'Profile Selection' section includes:

- * ISE Posture: AC4 profile
- VPN: (empty dropdown)

Clientprovisioningregels

Zodra het AnyConnect-profiel klaar is, kan er verwezen worden naar het beleid voor clientprovisioning:

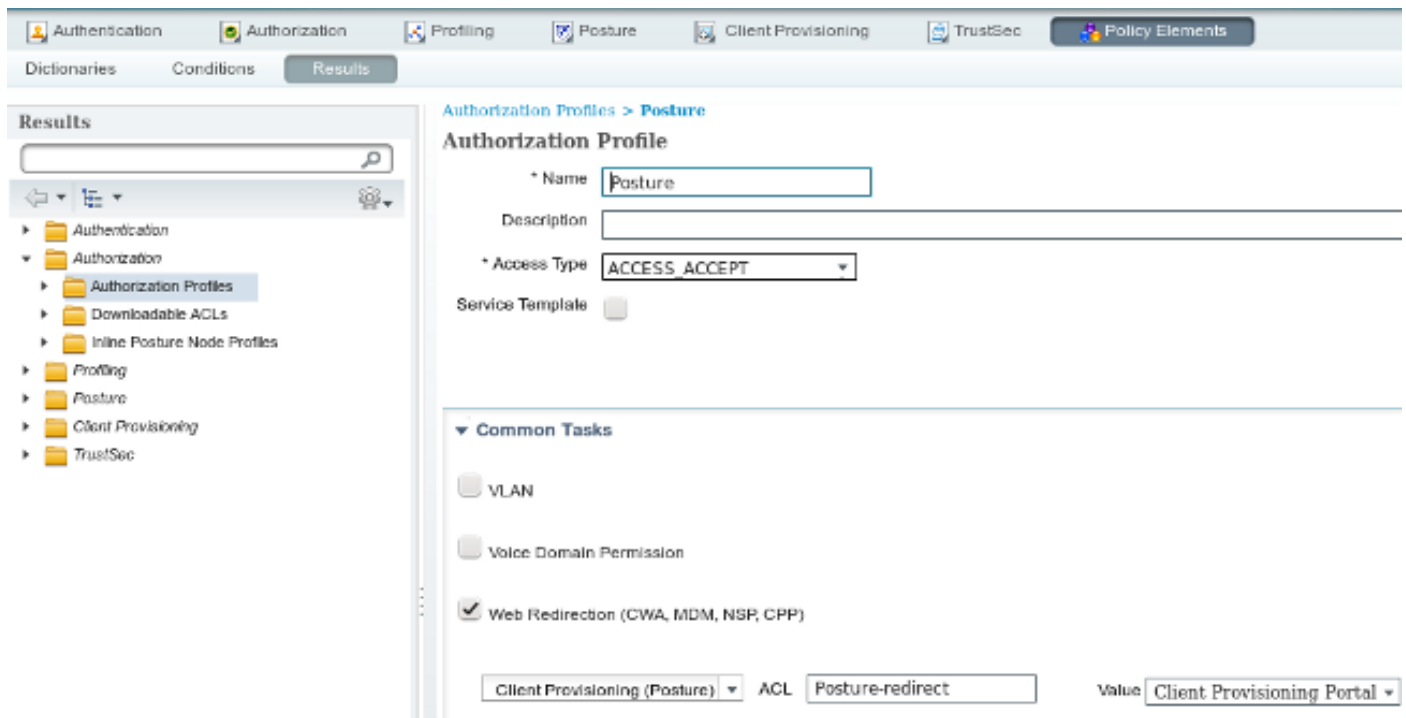
The screenshot shows the Cisco ISE Client Provisioning Policy configuration page. The top navigation bar includes tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning (selected), TrustSec, and Policy Elements. The page title is 'Client Provisioning Policy'. Below the title is a description: 'Defines 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

De gehele toepassing wordt samen met de configuratie geïnstalleerd op het eindpunt, dat wordt herleid naar de pagina van de Provisioning van de client. AnyConnect 4 kan worden bijgewerkt en er kan een extra module (functie) worden geïnstalleerd.

Verificatieprofielen

Maak een autorisatieprofiel voor omleiding naar het clientprovisioningprofiel:



machtigingsregels

Op deze afbeelding zijn de toelatingsregels te zien:

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

Voor het eerst wordt de *ASA-VPN_quarantaineregel* gebruikt. Als gevolg daarvan wordt het vergunningprofiel voor *Posture* teruggegeven en wordt het eindpunt verwezen naar het Customer Provisioning Portal voor AnyConnect 4 (met postmodule).

Zodra dit *is* gebeurd, wordt de *ASA-VPN_compatibele* regel gebruikt en is volledige netwerktoegang toegestaan.

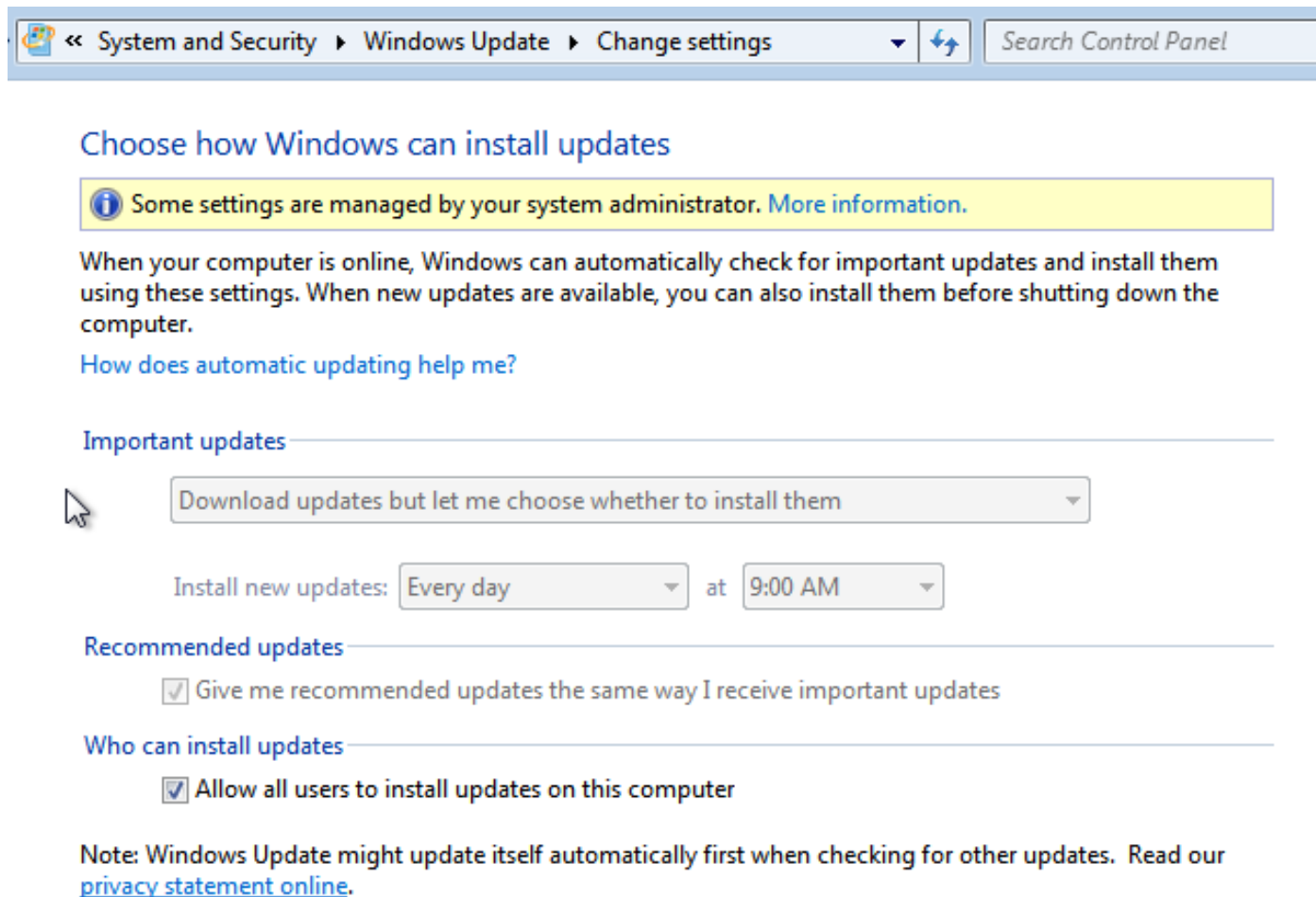
Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te controleren of de configuratie correct werkt.

Pc met bijgewerkt GPO-beleid

Het domeinbeleid met de configuratie van het WSUS moet worden geduwd nadat de PC zich in het domein inlogt. Dit kan voorkomen voordat de VPN-sessie wordt ingesteld (buiten de band) of nadat de *Start Voordat Logon*-functie wordt gebruikt (deze kan ook worden gebruikt voor 802.1x bekabelde/draadloze toegang).

Nadat de Microsoft Windows-client de juiste configuratie heeft, kan dit worden weerspiegeld in de Windows Update-instellingen:



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 contains the text 'Search Control Panel'. The main heading is 'Choose how Windows can install updates'. Below this is a yellow information box stating: 'Some settings are managed by your system administrator. More information.' The introductory text says: 'When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.' A link 'How does automatic updating help me?' is provided. Under the 'Important updates' section, the dropdown menu is set to 'Download updates but let me choose whether to install them'. The 'Install new updates' section is set to 'Every day' at '9:00 AM'. Under the 'Recommended updates' section, the checkbox 'Give me recommended updates the same way I receive important updates' is checked. Under the 'Who can install updates' section, the checkbox 'Allow all users to install updates on this computer' is checked. A note at the bottom states: 'Note: Windows Update might update itself automatically first when checking for other updates. Read our [privacy statement online](#).'

Indien nodig kan een Group Policy Object (GPO) worden opgefrist en kan de serverontdekking van Microsoft Windows Update Agent worden gebruikt:

```
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>
```

Een kritische update in het WSUS goedkeuren

Het goedkeuringsproces kan profiteren van de gerichtheid op de plaats van ontvangst:

The screenshot shows the WSUS console interface. The left pane displays the tree view with 'Update Services' expanded to 'Security Updates'. The right pane shows a list of security updates, with two updates for Windows 7 (KB3000483) listed. Below this, the 'Approve Updates' dialog box is open, displaying a table of computer groups and their approval status.

Computer Group	Approval	Deadline
All Computers	Not approved	N/A
Unassigned Computers	Install	None
Computer-Updated	Install	None

At the bottom of the dialog box, a message states: "The selected update does not support removal." An "OK" button is visible in the bottom right corner.

Herhaal het rapport indien nodig met de *mond*.

Controleer de PC-status op het WSUS

Deze afbeelding toont hoe de PC-status in het WSUS moet worden gecontroleerd:

The screenshot shows the WSUS Update Services console. The left pane shows the tree view with 'All Computers' selected under 'Computers'. The main pane displays a table of computers with the following data:

Name	IP Address	Operating System	Insta...	Last Status Report
admin-pc.example.com	192.168.10.21	Windows 7 Profes...	99%	6/27/2015 12:41 AM

Below the table, the status summary for the selected computer is shown:

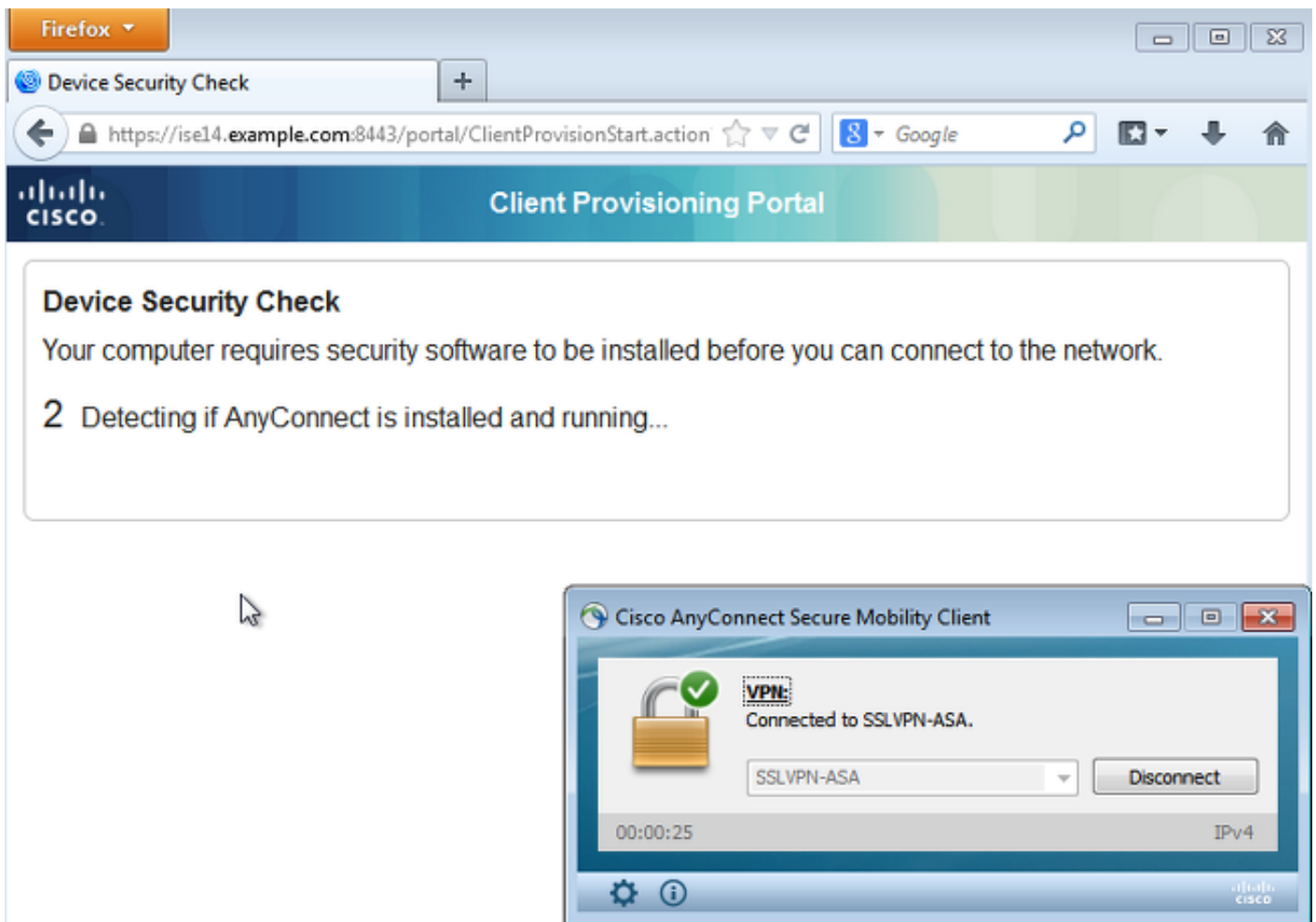
Status	Count
Updates with errors:	0
Updates needed:	1
Updates installed/not applicable:	1035
Updates with no status:	0

The group membership for the selected computer is listed as 'All Computer s, Unassigne d Computer'.

Eén update moet worden geïnstalleerd voor de volgende verfrissing met het WSUS.

VPN-sessie ingesteld

Nadat de VPN-sessie is vastgesteld, wordt de *ASA-VPN_quarantaine* ISE autorisatieregeling gebruikt, die het *Posture* autorisatieprofiel teruggeeft. Als resultaat hiervan wordt het HTTP-verkeer van het eindpunt opnieuw gericht voor de AnyConnect 4 update en posture module provisioning:



Op dit punt geeft de sessiestatus van de ASA beperkte toegang aan met de omleiding van het HTTP-verkeer naar de 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
```

Postmodule Ontvang beleid van ISE en voert verbetering uit

De postmodule ontvangt het beleid van de ISE. De uiteinden `ise-psc.log` tonen de vereiste aan die naar de postmodule wordt gestuurd:

```
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>
```

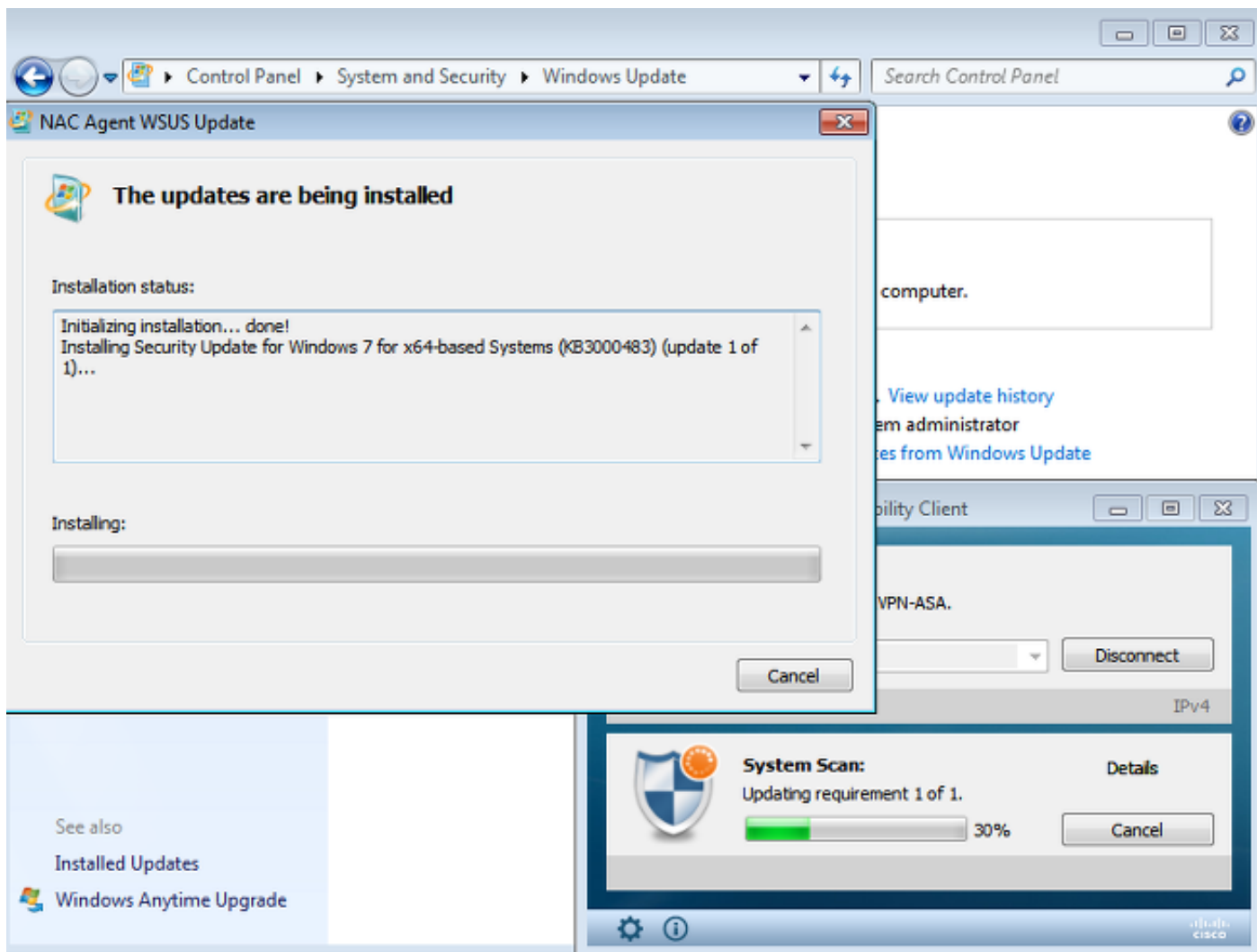
```
<package>  
  <id>10</id>
```

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

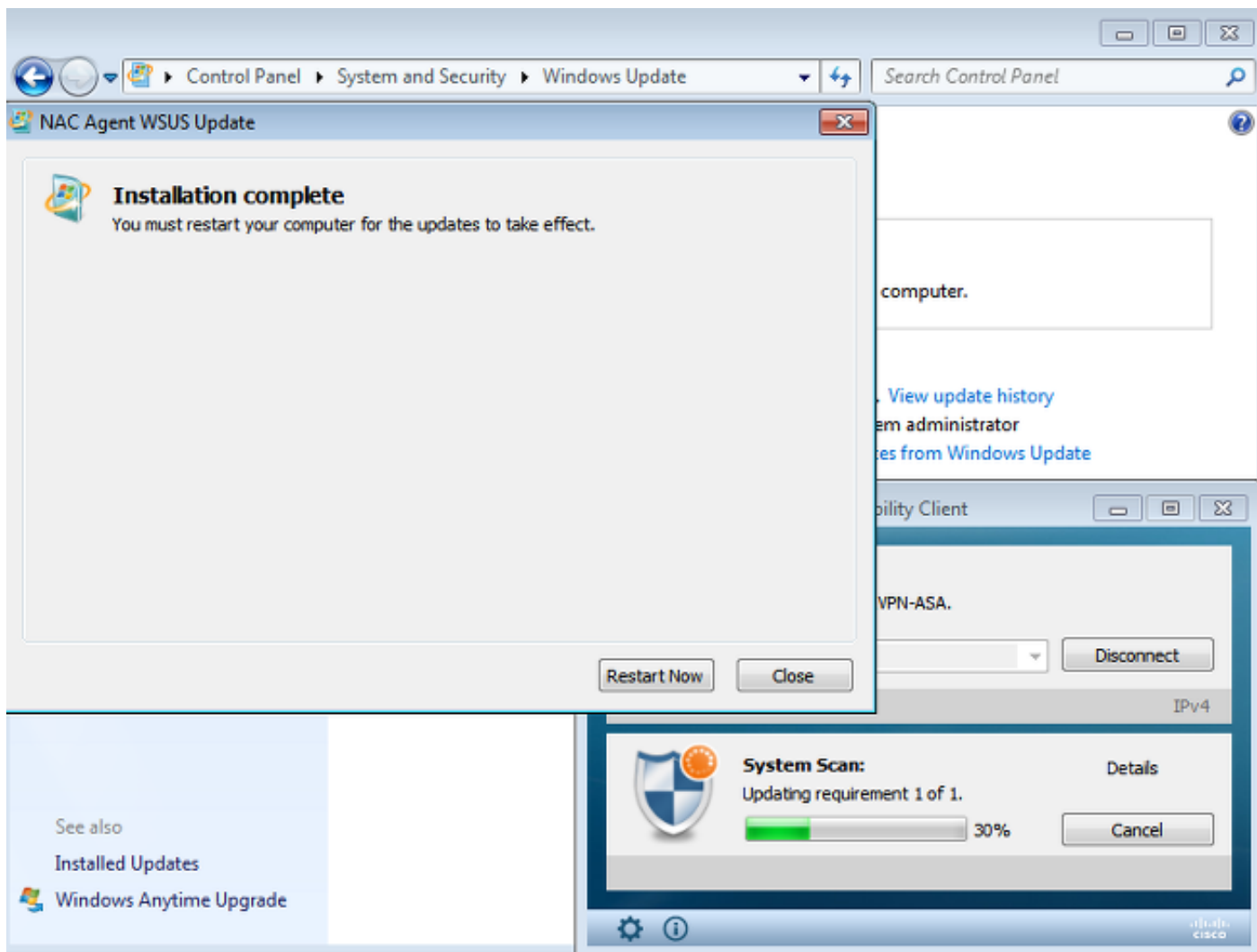
```
<remediation_type>1</remediation_type>  
<remediation_retry>0</remediation_retry>  
<remediation_delay>0</remediation_delay>  
<action>10</action>  
<check>
```

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

De postmodule start automatisch de Microsoft Windows Update Agent om verbinding te maken met de WSUS en download updates zoals ingesteld in het WSUS-beleid (allemaal automatisch zonder enige gebruikersinterventie):

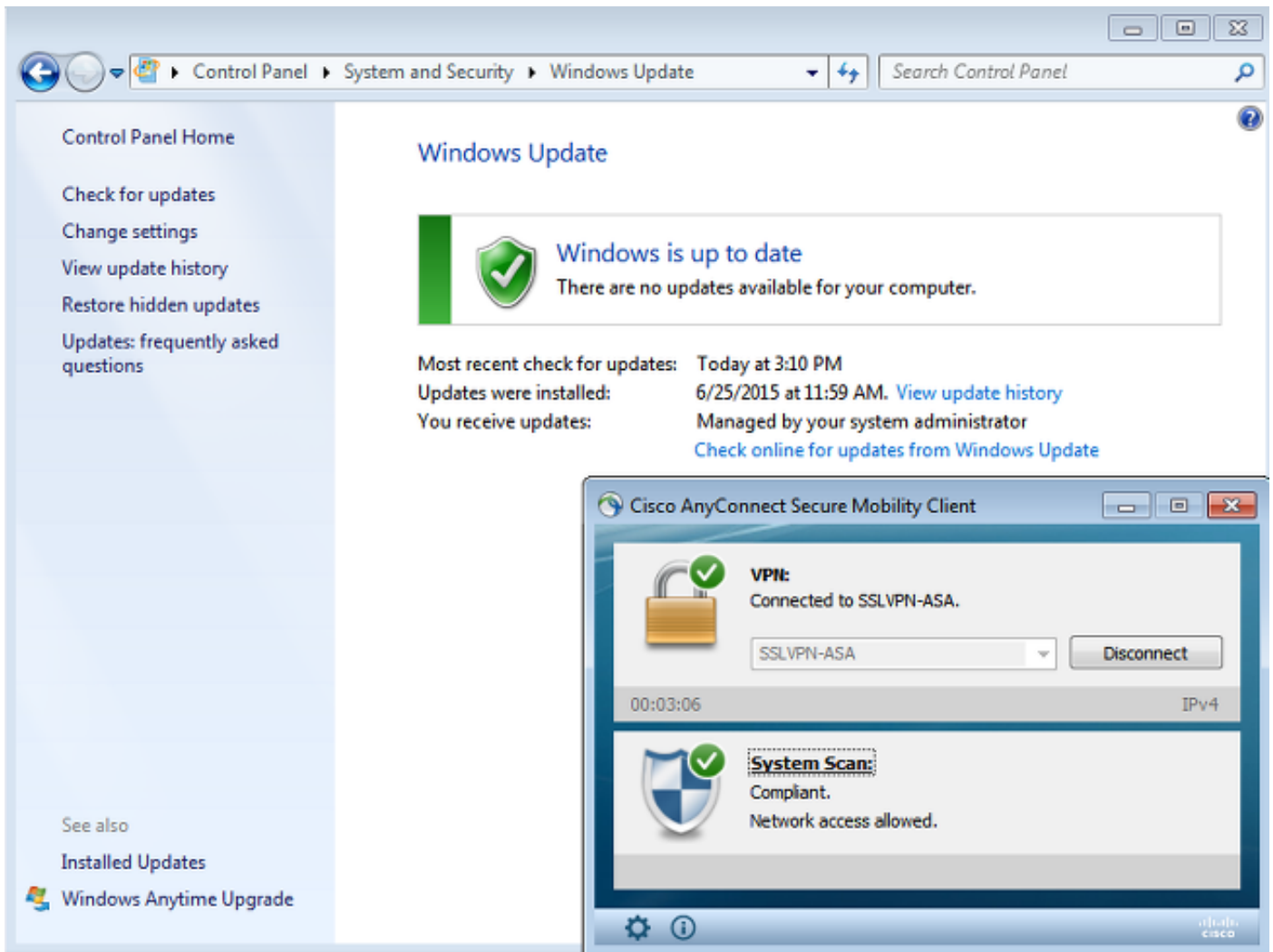


Opmerking: Voor sommige updates zou een systeemherstart nodig kunnen zijn.

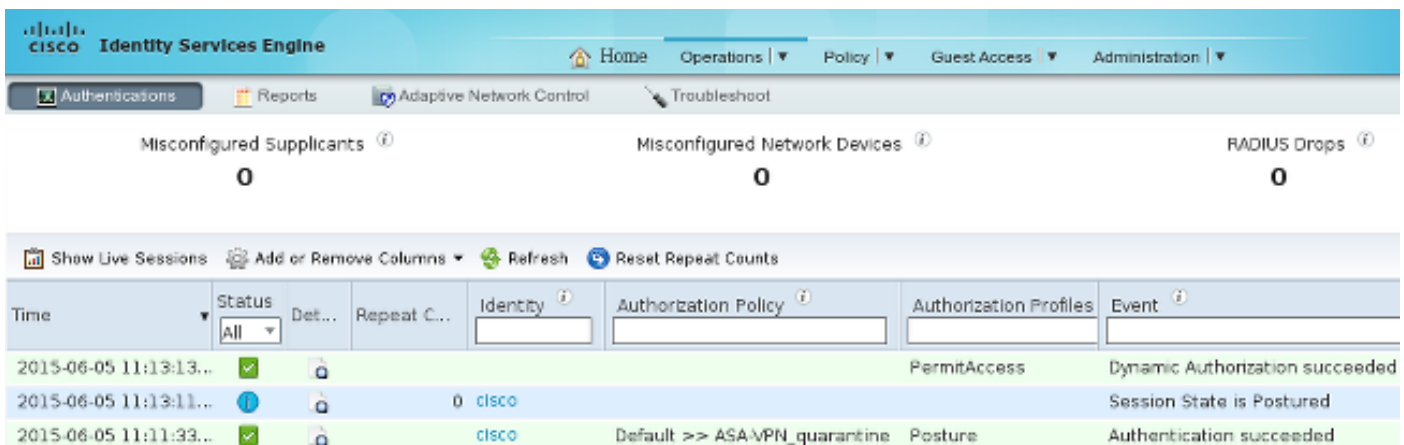


Volledige netwerktoegang

U ziet dit nadat het station is gemeld als compatibel met de AnyConnect-postmodule:



Het rapport wordt verstuurd naar ISE, die het beleid herevalueert en de autorisatieregel *ASA-VPN_compliance* raakt. Dit biedt volledige netwerktoegang (via de Radius CoA). Navigeer naar **Operations > Authenticaties** om dit te bevestigen:



De **debugs (ise-psc.log)** bevestigen ook de compliance status, de CoA-trigger en de definitieve instellingen voor de functie:

```
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]
```

Ook bevestigt het rapport van de ISE, dat het station voldoet aan:

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

Opmerking: Het exacte adres van Media Access Control (MAC) van de fysieke netwerkinterface op Microsoft Windows PC is bekend vanwege de ACIDEX-uitbreidingen.

Problemen oplossen

Er is momenteel geen informatie over probleemoplossing beschikbaar voor deze configuratie.

Belangrijke opmerkingen

Deze sectie verschaft belangrijke informatie over de configuratie die in dit document wordt beschreven.

Optiegegevens voor WSUS-verbetering

Het is belangrijk de vereiste conditie te onderscheiden van de sanering. AnyConnect brengt de Microsoft Windows Update Agent in werking om de naleving te controleren, afhankelijk van de *Windows-updates valideren met corrigerende instellingen*.

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

Bij dit voorbeeld wordt het *ernst-niveau* gebruikt. Met de *kritieke* instelling controleert de Microsoft Windows Agent of er hangende (niet geïnstalleerde) kritische updates zijn. Als er iets is, dan begint het herstel.

Het herstelproces zou dan alle kritische en minder belangrijke updates op basis van de WSUS-configuratie kunnen installeren (updates goedgekeurd voor de specifieke machine).

Met de *redactie van Windows updates die als Cisco Regels* gebruiken, besluiten de voorwaarden die in de vereiste gedetailleerd zijn of het station voldoet.

Windows Update Service

Voor implementaties zonder een WSUS-server is er een ander hersteltype dat kan worden gebruikt met de naam *Windows Update Remediation*:

[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

Dit type herstel maakt controle mogelijk over de instellingen voor Microsoft Windows Update en stelt u in staat onmiddellijke updates uit te voeren. Een typische voorwaarde die met dit hersteltype wordt gebruikt is *pc_AutoUpdateCheck*. Hiermee kunt u controleren of de instelling

Microsoft Windows Update op het eindpunt is ingeschakeld. Als dit niet het geval is, kunt u dit activeren en het update uitvoeren.

SCCM-integratie

Een nieuwe functie voor de ISE versie 1.4, *patchbeheer* genaamd, maakt integratie met veel derden mogelijk. Afhankelijk van de verkoper zijn er meerdere opties beschikbaar voor zowel de omstandigheden als de oplossingen.

Voor Microsoft worden zowel de System Management Server (sms) als de System Center Configuration Manager (SCCM) ondersteund.

Gerelateerde informatie

- [Postservices in de Cisco ISE Configuration Guide](#)
- [Administrator-gids voor Cisco Identity Services Engine, release 1.4](#)
- [Administrator-gids voor Cisco Identity Services Engine, release 1.3](#)
- [Windows Server Update Services implementeren in uw organisatie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)