

# Konfigurieren des Status ISE Version 1.4 mit Microsoft WSUS

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Microsoft WSUS](#)

[ASA](#)

[ISE](#)

[Statusbehebung für WSUS](#)

[Statusanforderung für WSUS](#)

[AnyConnect-Profil](#)

[Client-Bereitstellungsregeln](#)

[Autorisierungsprofile](#)

[Autorisierungsregeln](#)

[Überprüfen](#)

[PC mit aktualisierten GPO-Richtlinien](#)

[Genehmigen eines kritischen Updates für den WSUS](#)

[Überprüfen Sie den PC-Status auf dem WSUS.](#)

[VPN-Sitzung eingerichtet](#)

[Statusmodul empfängt Richtlinien von der ISE und führt Problembehebung durch](#)

[Vollständiger Netzwerkzugriff](#)

[Fehlerbehebung](#)

[Wichtige Hinweise](#)

[Optionsdetails für die WSUS-Bereinigung](#)

[Windows Update-Dienst](#)

[SCCM-Integration](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie die Statusfunktion der Cisco Identity Services Engine (ISE) konfiguriert wird, wenn sie in die Microsoft Windows Server Update Services (WSUS) integriert ist.

**Hinweis:** Wenn Sie auf das Netzwerk zugreifen, werden Sie zur ISE für Cisco AnyConnect Secure Mobility Client Version 4.1 umgeleitet, wobei ein Statusmodul bereitgestellt wird. Dieses prüft den Compliance-Status auf dem WSUS und installiert die erforderlichen Aktualisierungen, damit die Station den Anforderungen entspricht. Sobald die Station als konform gemeldet wurde, ermöglicht die ISE den vollständigen Netzwerkzugriff.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Bereitstellung, Authentifizierung und Autorisierung der Cisco ISE
- Grundkenntnisse der Funktionsweise der ISE und des Cisco AnyConnect-Schwachstellenagenten
- Konfiguration der Cisco Adaptive Security Appliance (ASA)
- Grundlegendes VPN und 802.1x-Wissen
- Konfiguration des Microsoft WSUS

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows Version 7
- Microsoft Windows Version 2012 mit WSUS Version 6.3
- Cisco ASA Version 9.3.1 und höher
- Cisco ISE Software Version 1.3 und höher

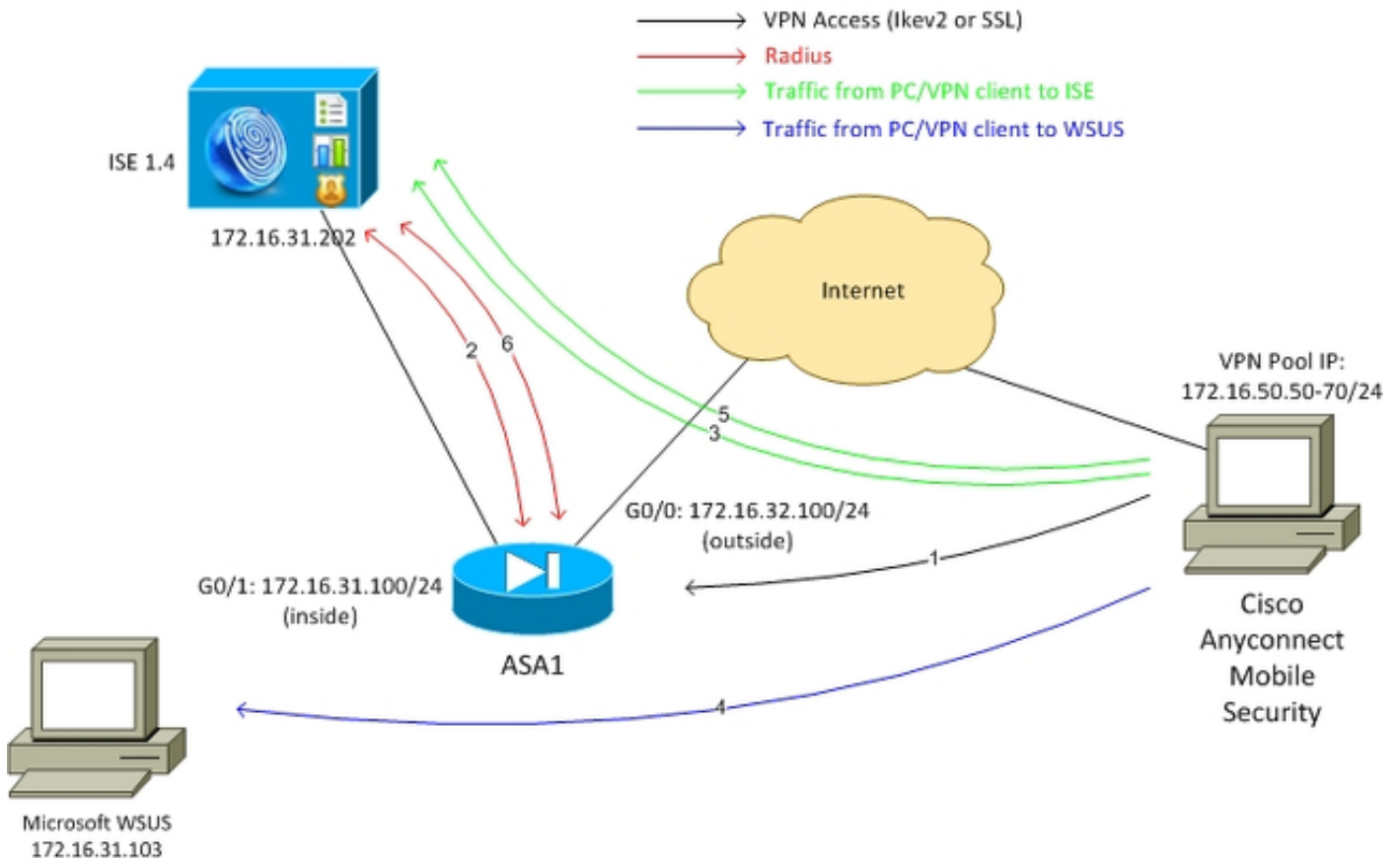
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie die ISE und die zugehörigen Netzwerkelemente konfigurieren.

## Netzwerkdiagramm

Dies ist die Topologie, die für die Beispiele in diesem Dokument verwendet wird:



Hier ist der Datenverkehrsfluss, wie im Netzwerkdiagramm veranschaulicht:

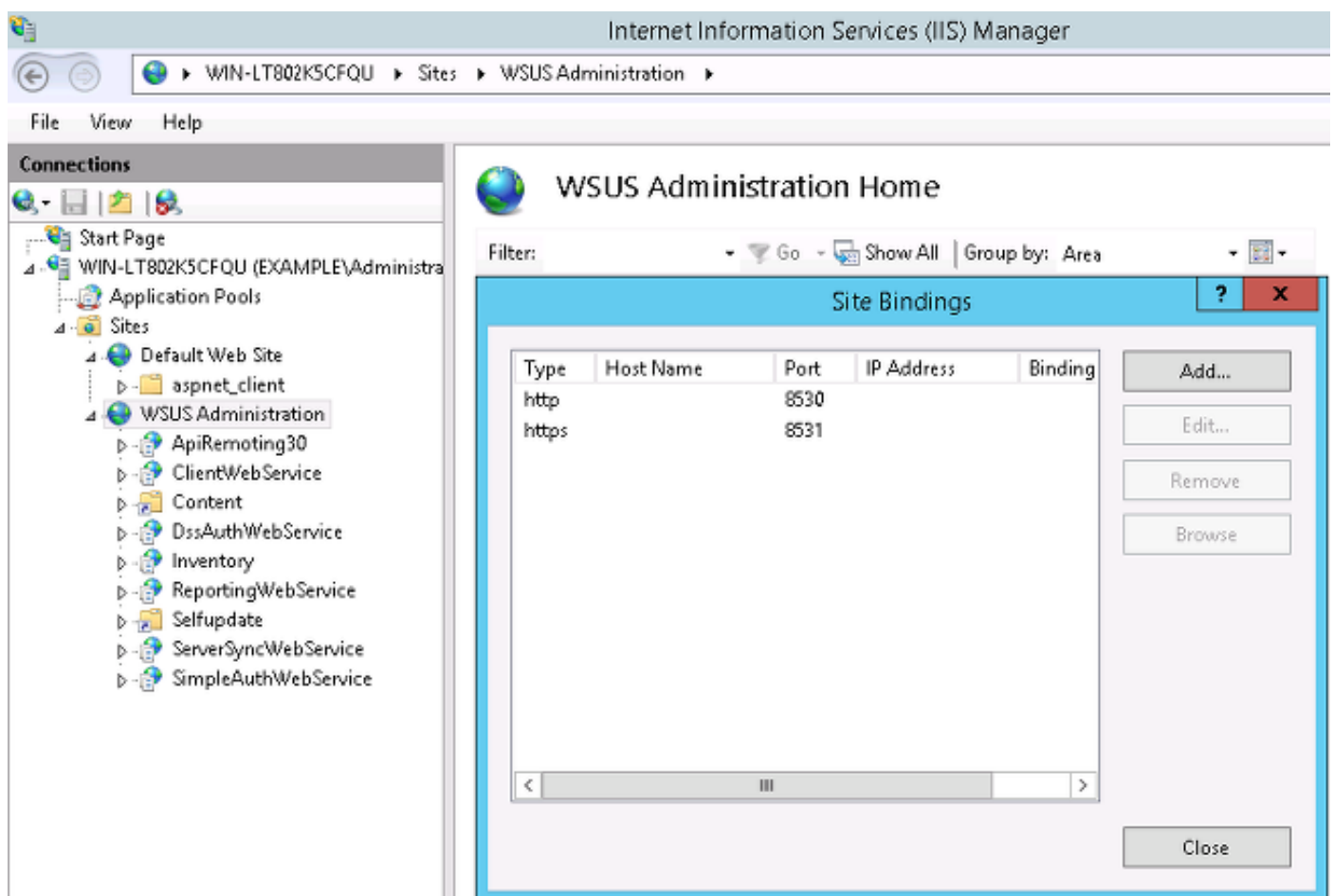
1. Der Remote-Benutzer stellt über Cisco AnyConnect eine Verbindung für den VPN-Zugriff auf die ASA her. Dabei kann es sich um eine beliebige Art von Unified Access handeln, z. B. eine verkabelte 802.1x/MAC Authentication Bypass (MAB)-Sitzung, die am Switch terminiert wird, oder eine Wireless-Sitzung, die am Wireless LAN Controller (WLC) terminiert wird.
2. Im Rahmen des Authentifizierungsprozesses bestätigt die ISE, dass der Status der Endstation nicht den Vorgaben entspricht (*ASA-VPN\_Quarantine*-Autorisierungsregel) und dass die Umleitungsattribute in der *RADIUS Access-Accept*-Nachricht zurückgegeben werden. Daher leitet die ASA den gesamten HTTP-Datenverkehr an die ISE um.
3. Der Benutzer öffnet einen Webbrowser und gibt eine beliebige Adresse ein. Nach der Umleitung zur ISE wird das Cisco AnyConnect 4-Statusmodul auf der Station installiert. Das Statusmodul lädt dann die Richtlinien von der ISE herunter (Voraussetzung für WSUS).
4. Das Statusmodul sucht nach Microsoft WSUS und führt eine Problembehebung durch.
5. Nach erfolgreicher Behebung sendet das Statusmodul einen Bericht an die ISE.
6. Die ISE gibt einen Radius Change of Authorization (CoA) aus, der vollständigen Netzwerkzugriff für einen kompatiblen VPN-Benutzer (*ASA-VPN\_compliance* Authorization Rule) bereitstellt.

**Hinweis:** Damit die Problembhebung funktioniert (Microsoft Windows-Updates können auf einem PC installiert werden), muss der Benutzer über lokale Administratorrechte verfügen.

## Microsoft WSUS

**Hinweis:** Eine detaillierte Konfiguration des WSUS wird in diesem Dokument nicht behandelt. Weitere Informationen finden Sie in der Microsoft-Dokumentation [Bereitstellung von Windows Server Update Services in Ihrer Organisation](#).

Der WSUS-Dienst wird über den standardmäßigen TCP-Port 8530 bereitgestellt. Beachten Sie, dass zur Problembhebung auch andere Ports verwendet werden. Aus diesem Grund ist es sicher, die IP-Adresse von WSUS der Umleitungszugriffskontrollliste (ACL) auf der ASA hinzuzufügen (die weiter unten in diesem Dokument beschrieben wird).

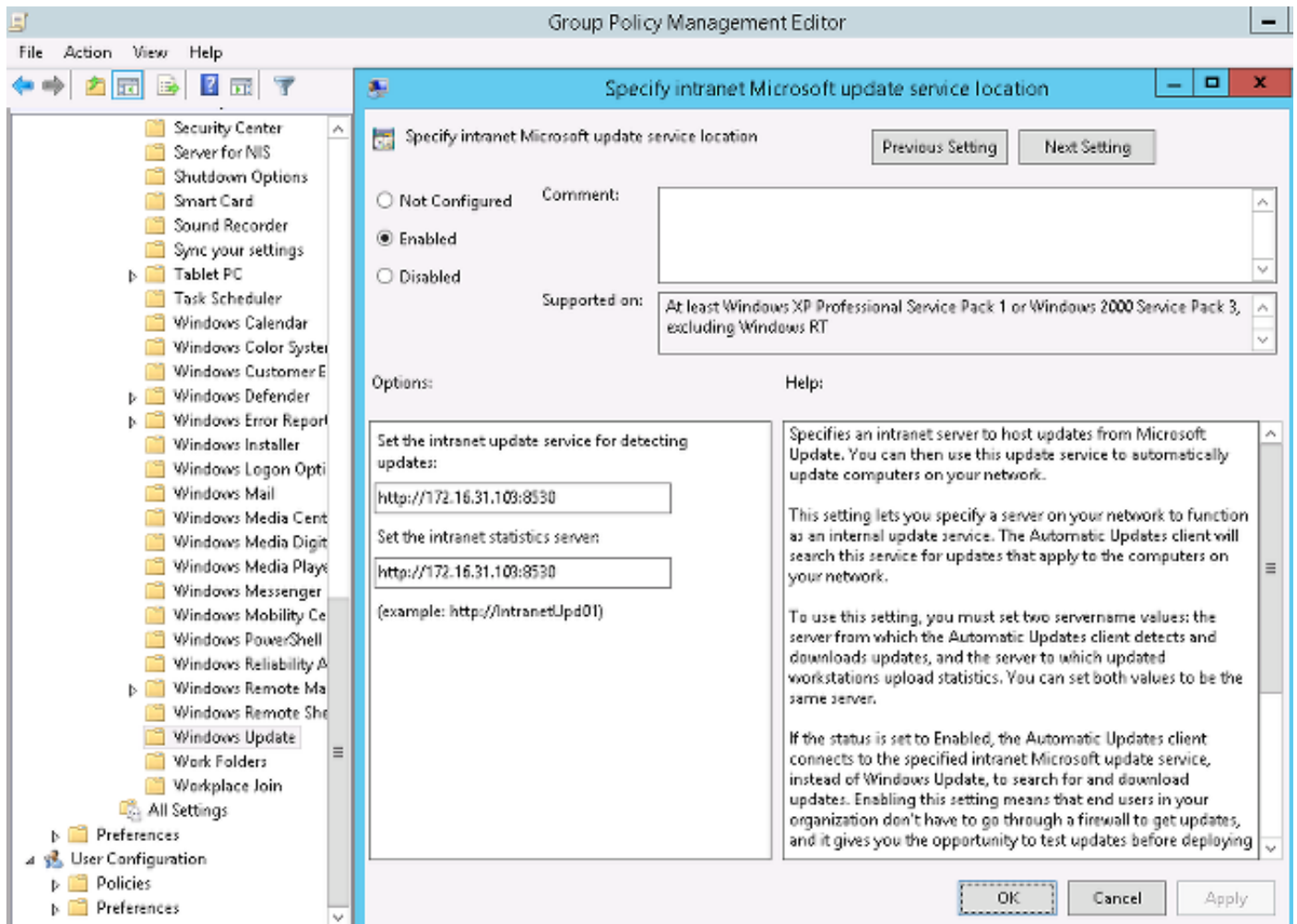


The screenshot shows the IIS Manager interface. The left pane displays the 'Connections' tree with 'WSUS Administration' selected. The main pane shows the 'WSUS Administration Home' page. A 'Site Bindings' dialog box is open, displaying the following table:

Type	Host Name	Port	IP Address	Binding
http		8530		
https		8531		

The dialog box also includes buttons for 'Add...', 'Edit...', 'Remove', 'Browse', and 'Close'.

Die Gruppenrichtlinie für die Domäne ist für Microsoft Windows-Updates konfiguriert und verweist auf den lokalen WSUS-Server:



Dies sind die empfohlenen Updates, die für detaillierte Richtlinien aktiviert werden, die auf unterschiedlichen Schweregraden basieren:

📁 **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

Die Client-seitige Ausrichtung ermöglicht eine deutlich größere Flexibilität. Die ISE kann Statusrichtlinien verwenden, die auf den verschiedenen Microsoft Active Directory (AD)-Computercontainern basieren. Der WSUS kann Updates genehmigen, die auf dieser Mitgliedschaft basieren.

## ASA

Es wird ein Simple Secure Sockets Layer (SSL)-VPN-Zugriff für den Remote-Benutzer verwendet (dessen Details nicht in diesem Dokument enthalten sind).

Hier ein Beispiel für eine Konfiguration:

```
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
```

Es ist wichtig, eine Zugriffsliste auf der ASA zu konfigurieren, die verwendet wird, um den Datenverkehr zu bestimmen, der an die ISE umgeleitet werden soll (für Benutzer, die noch nicht konform sind):

```
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

Nur Domain Name System (DNS)-, ISE-, WSUS- und Internet Control Message Protocol (ICMP)-Datenverkehr ist für nicht konforme Benutzer zulässig. Der gesamte andere Datenverkehr (HTTP) wird für die AnyConnect 4-Bereitstellung an die ISE umgeleitet, die für den Status und die Problembeseitigung verantwortlich ist.

## ISE

**Hinweis:** Bereitstellung und Status von AnyConnect 4 sind nicht Bestandteil dieses Dokuments. Weitere Informationen zum Konfigurieren der ASA als Netzwerkgerät und zum Installieren der Cisco AnyConnect 7-Anwendung finden Sie im [Konfigurationsbeispiel](#) für die [AnyConnect 4.0-Integration mit der ISE Version 1.3](#).

## Statusbehebung für WSUS

Gehen Sie wie folgt vor, um die Statussanierung für WSUS zu konfigurieren:

1. Navigieren Sie zu **Richtlinien > Bedingungen > Status > Remediation Actions > Windows Server Update Services Remediation**, um eine neue Regel zu erstellen.
2. Überprüfen Sie, ob die Einstellung *Microsoft Windows Updates* auf **Schweregrad** eingestellt ist. Dieser Teil ist für die Erkennung verantwortlich, wenn der Beseitigungsprozess initiiert wird.

Der Microsoft Windows Update Agent stellt dann eine Verbindung mit dem WSUS her und überprüft, ob *kritische* Updates für diesen PC vorliegen, die auf die Installation warten:

The screenshot displays the Cisco ISE configuration interface. At the top, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy. Below these 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 includes the following fields and options:

- 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

At the bottom of the form are "Save" and "Reset" buttons. On the left side, a "Results" pane shows a tree view of the configuration hierarchy, with "Remediation Actions" expanded to show various remediation types, including "Windows Server Update Services Remediation" which is currently selected.

## Statusanforderung für WSUS

Navigieren Sie zu **Richtlinien > Bedingungen > Status > Anforderungen**, um eine neue Regel zu erstellen. Die Regel verwendet eine Dummy-Bedingung namens *pr\_WSUSRule*, d. h., dass der WSUS kontaktiert wird, um zu prüfen, ob bei Bedarf eine Problembehebung erforderlich ist (*kritische Updates*).

Sobald diese Bedingung erfüllt ist, installiert der WSUS die für diesen PC konfigurierten Updates. Diese können jede Art von Aktualisierungen sowie Updates mit niedrigerem Schweregrad umfassen:

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-Profil

Konfigurieren Sie das Status-Modulprofil zusammen mit dem AnyConnect 4-Profil (wie im [Konfigurationsbeispiel](#) für die [Integration von AnyConnect 4.0 in ISE Version 1.3](#) beschrieben):



The screenshot shows the 'AnyConnect Configuration' page in the Cisco ISE Policy Elements interface. The left sidebar shows a tree view with 'Results' selected. 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 box)
- \* 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)

## Client-Bereitstellungsregeln

Wenn das AnyConnect-Profil fertig ist, kann auf es in der *Client Provisioning*-Richtlinie verwiesen werden:

The screenshot shows the 'Client Provisioning Policy' configuration page in the Cisco ISE Policy Elements interface. The page title is 'Client Provisioning Policy' and it includes the following text:

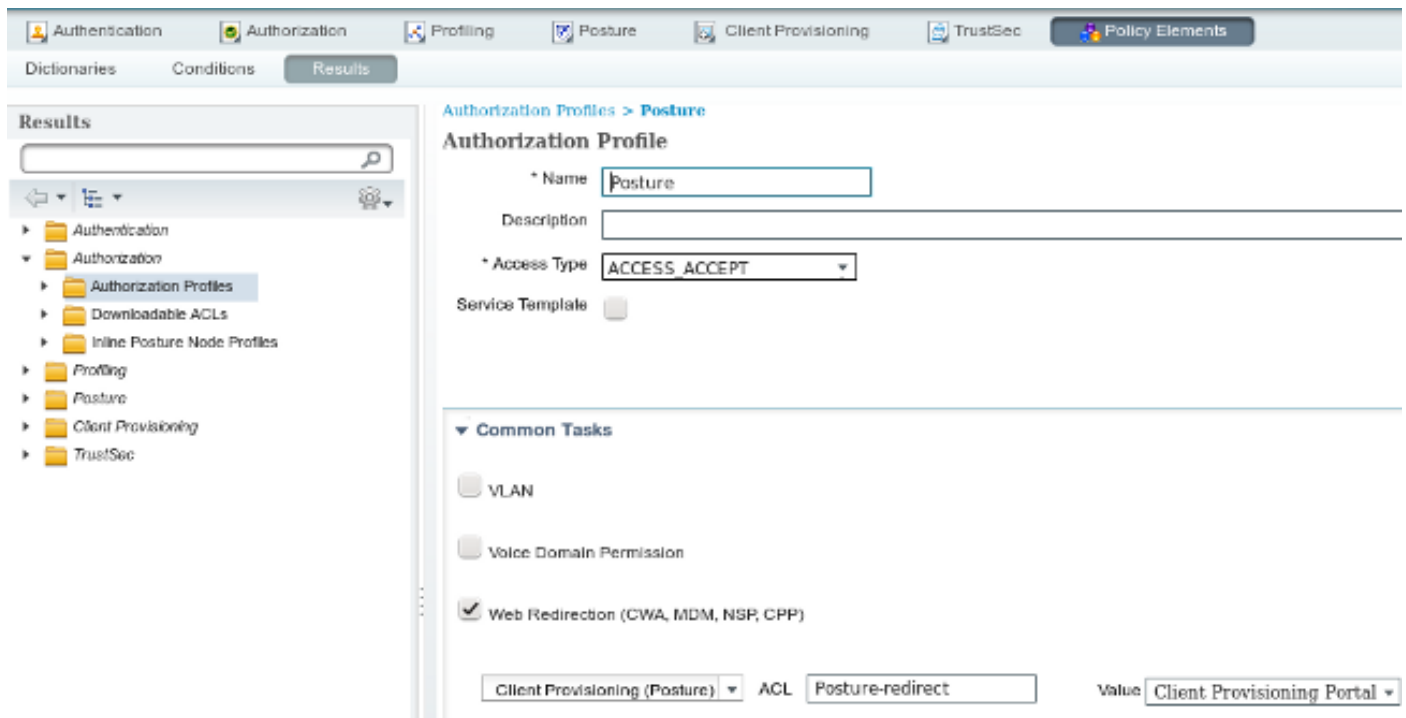
Define the Client Provisioning Policy to determine what users will receive upon login and user session initialization:  
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
 For Native Supplicant Configuration: wizard profile and/or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

Die gesamte Anwendung wird zusammen mit der Konfiguration auf dem Endpunkt installiert, der auf die Portalseite für die Client-Bereitstellung umgeleitet wird. AnyConnect 4 kann aktualisiert und ein zusätzliches Modul (Status) installiert werden.

## Autorisierungsprofile

Erstellen Sie ein Autorisierungsprofil für die Umleitung zum Client Provisioning-Profil:

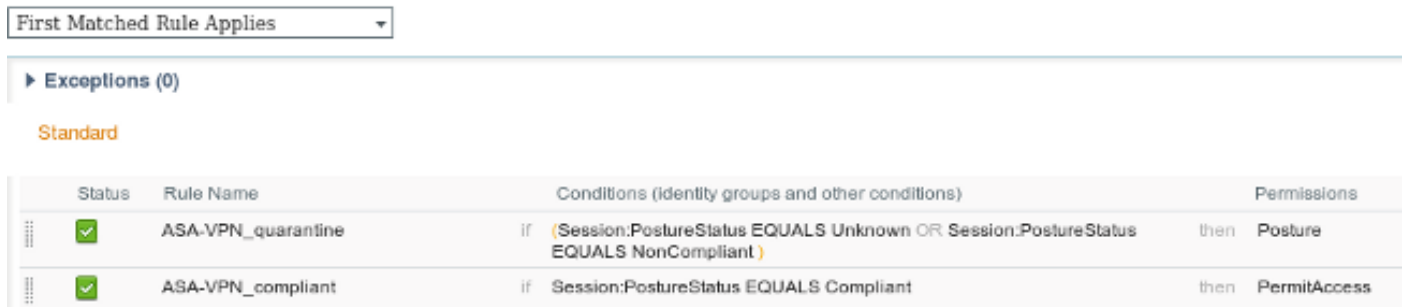


## Autorisierungsregeln

Dieses Bild zeigt die Autorisierungsregeln:

### 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](#)



Zum ersten Mal wird die *ASA-VPN\_Quarantine*-Regel verwendet. Als Ergebnis wird das *Status*-Autorisierungsprofil zurückgegeben und der Endpunkt für die AnyConnect 4-Bereitstellung (mit Statusmodul) an das Client Provisioning-Portal umgeleitet.

Sobald die Vorgaben erfüllt sind, wird die *ASA-VPN\_compliance*-Regel verwendet, und der vollständige Netzwerkzugriff ist zulässig.

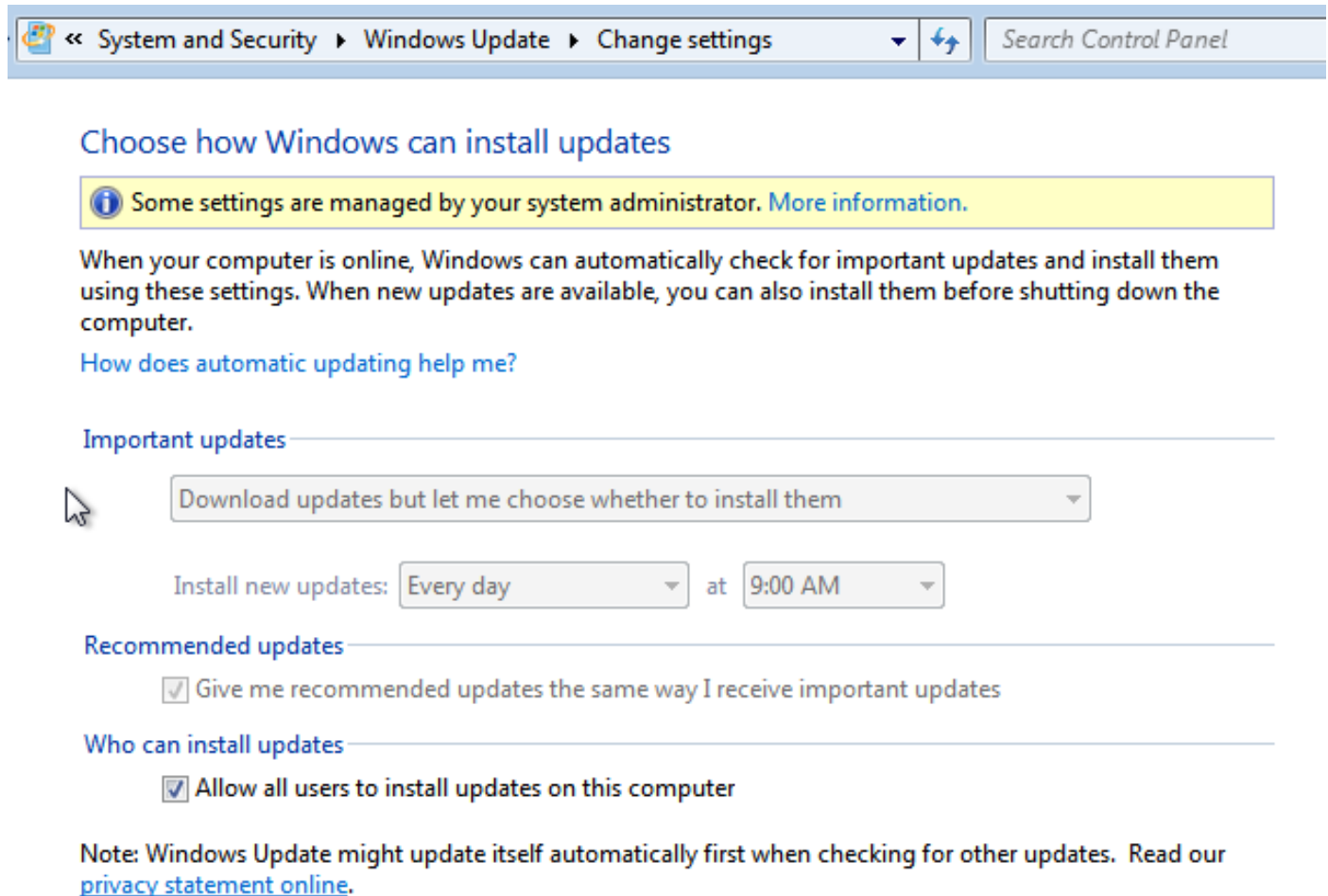
## Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

## PC mit aktualisierten GPO-Richtlinien

Die Domänenrichtlinien mit der WSUS-Konfiguration sollten nach der Anmeldung des PCs bei der Domäne weitergeleitet werden. Dies kann vor der Einrichtung der VPN-Sitzung (Out-of-Band) oder danach erfolgen, wenn die Funktion *Start Before Logon* (Start Before Logon) verwendet wird (sie kann auch für den kabelgebundenen/Wireless-Zugriff auf 802.1x verwendet werden).

Sobald der Microsoft Windows-Client die richtige Konfiguration aufweist, kann dies in den Windows Update-Einstellungen angezeigt werden:



The screenshot shows the Windows Update settings window 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 explains that Windows can automatically check for updates and install them, or they can be installed manually before shutting down. A link 'How does automatic updating help me?' is provided. Under the 'Important updates' section, a dropdown menu is set to 'Download updates but let me choose whether to install them'. Below this, '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.'

Bei Bedarf können eine GPO-Aktualisierung (Group Policy Object) und die Microsoft Windows Update Agent-Servererkennung verwendet werden:

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

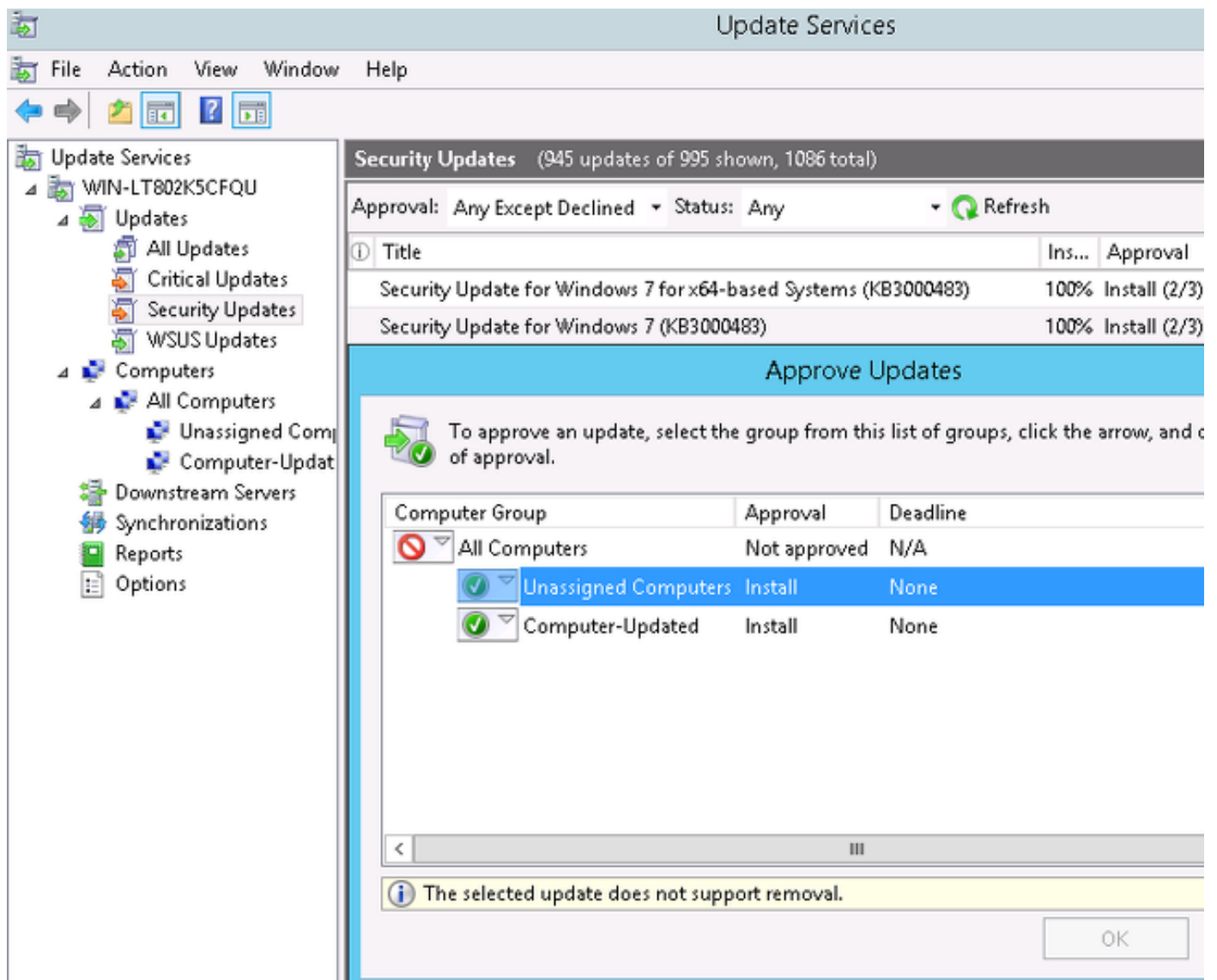
```
User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

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

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

## Genehmigen eines kritischen Updates für den WSUS

Der Genehmigungsprozess kann von der Ausrichtung auf Kundenstandorte profitieren:



Senden Sie den Bericht *bei* Bedarf erneut.

## Überprüfen Sie den PC-Status auf dem WSUS.

Dieses Bild zeigt, wie Sie den PC-Status auf dem WSUS überprüfen:

The screenshot shows the WSUS console interface. The left pane displays a tree view with 'Update Services' expanded to 'All Computers'. The main pane shows 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 for 'admin-pc.example.com' is shown as a green circle. The status legend indicates:

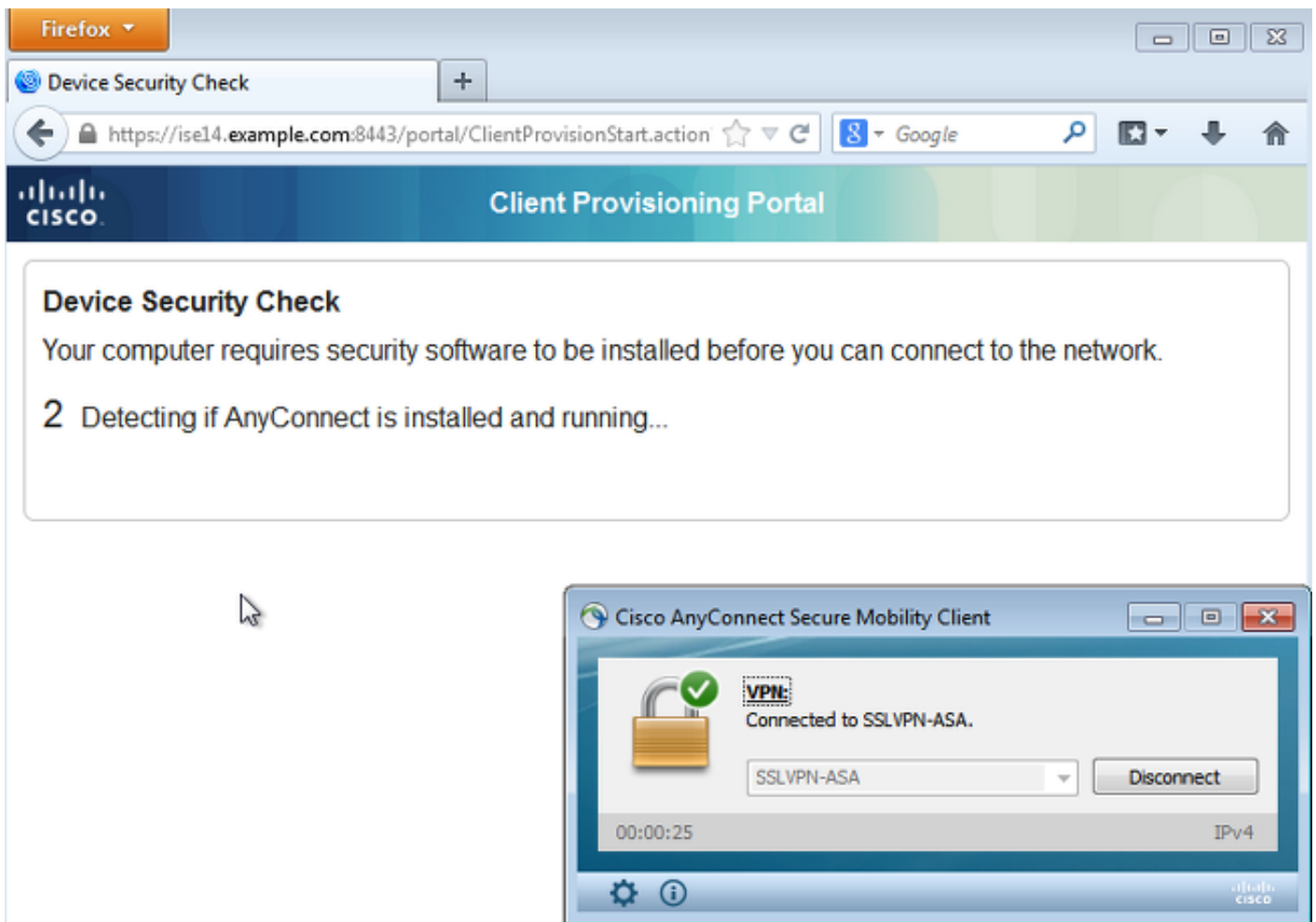
- Updates with errors: 0
- Updates needed: 1
- Updates installed/not applicable: 1035
- Updates with no status: 0

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

Für die nächste Aktualisierung mit dem WSUS sollte ein Update installiert werden.

## VPN-Sitzung eingerichtet

Nach Einrichtung der VPN-Sitzung wird die ISE-Autorisierungsregel für *ASA-VPN\_Quarantine* verwendet, die das *Status*-Autorisierungsprofil zurückgibt. Als Ergebnis wird der HTTP-Datenverkehr vom Endpunkt zur Bereitstellung des AnyConnect 4-Updates und -Statusmoduls umgeleitet:



An diesem Punkt zeigt der Sitzungsstatus auf der ASA eingeschränkten Zugriff mit der Umleitung des HTTP-Datenverkehrs zur ISE an:

```
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
```

## Statusmodul empfängt Richtlinien von der ISE und führt Problembehebung durch

Das Statusmodul empfängt die Richtlinien von der ISE. Die `ise-psc.log`-Debugger zeigen die Anforderung an, die an das Statusmodul gesendet wird:

```
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>
```

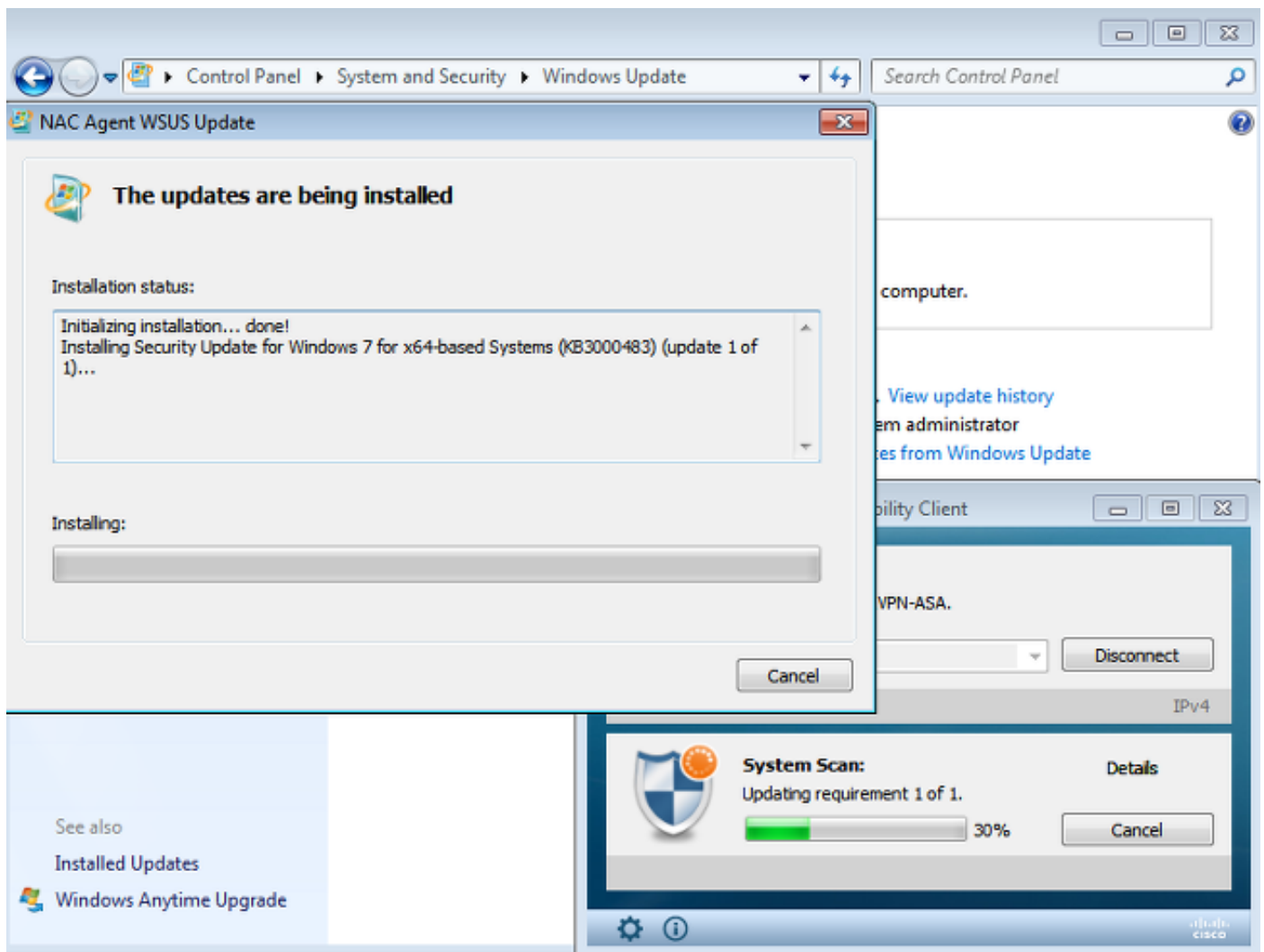
```
<package>  
  <id>10</id>
```

```
<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>
```

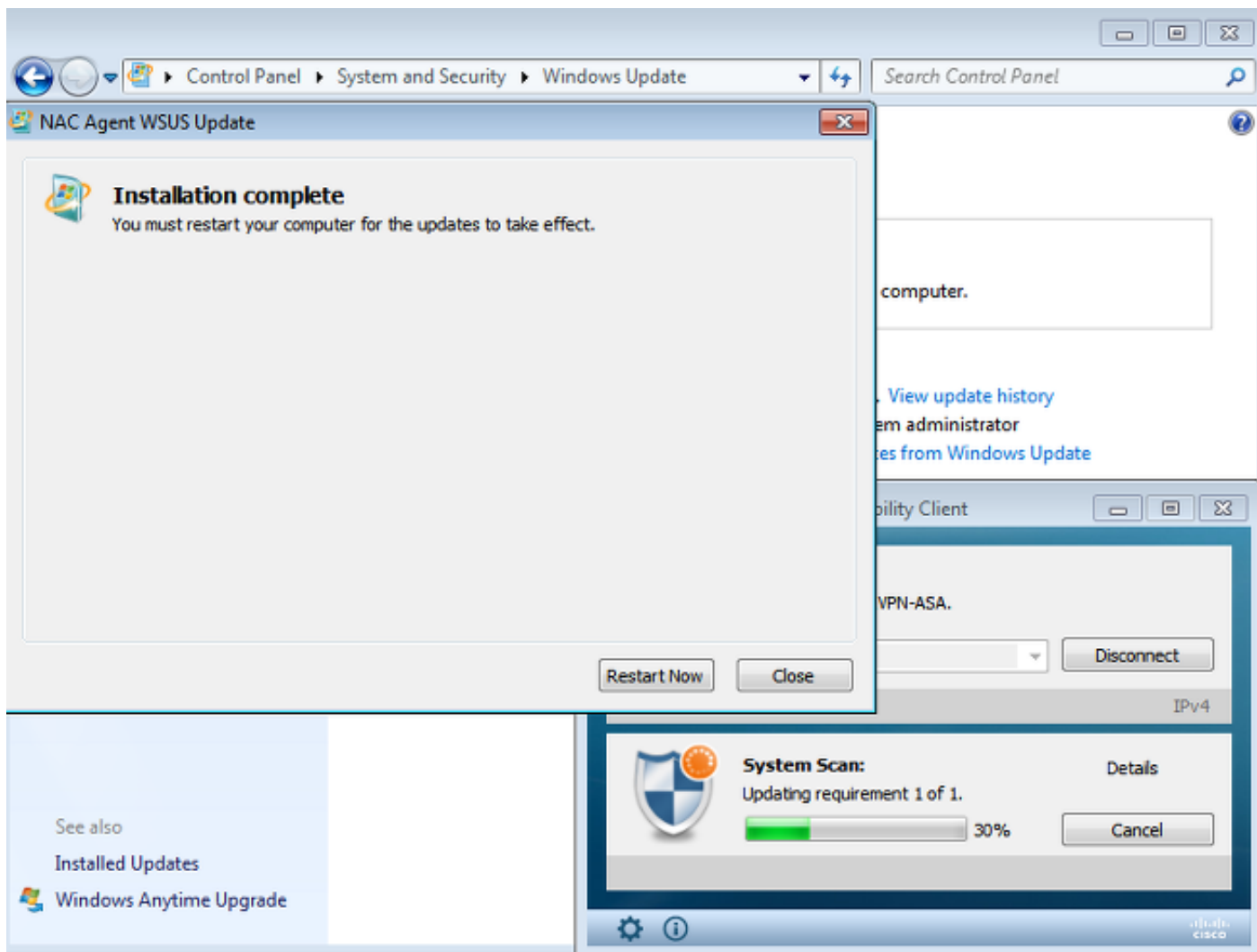
```
</check>  
<criteria/>  
</package>  
</cleanmachines>
```

Das Statusmodul veranlasst den Microsoft Windows Update Agent automatisch, eine Verbindung zum WSUS herzustellen und Updates entsprechend der WSUS-Richtlinien herunterzuladen (alle automatisch ohne Benutzereingriff):



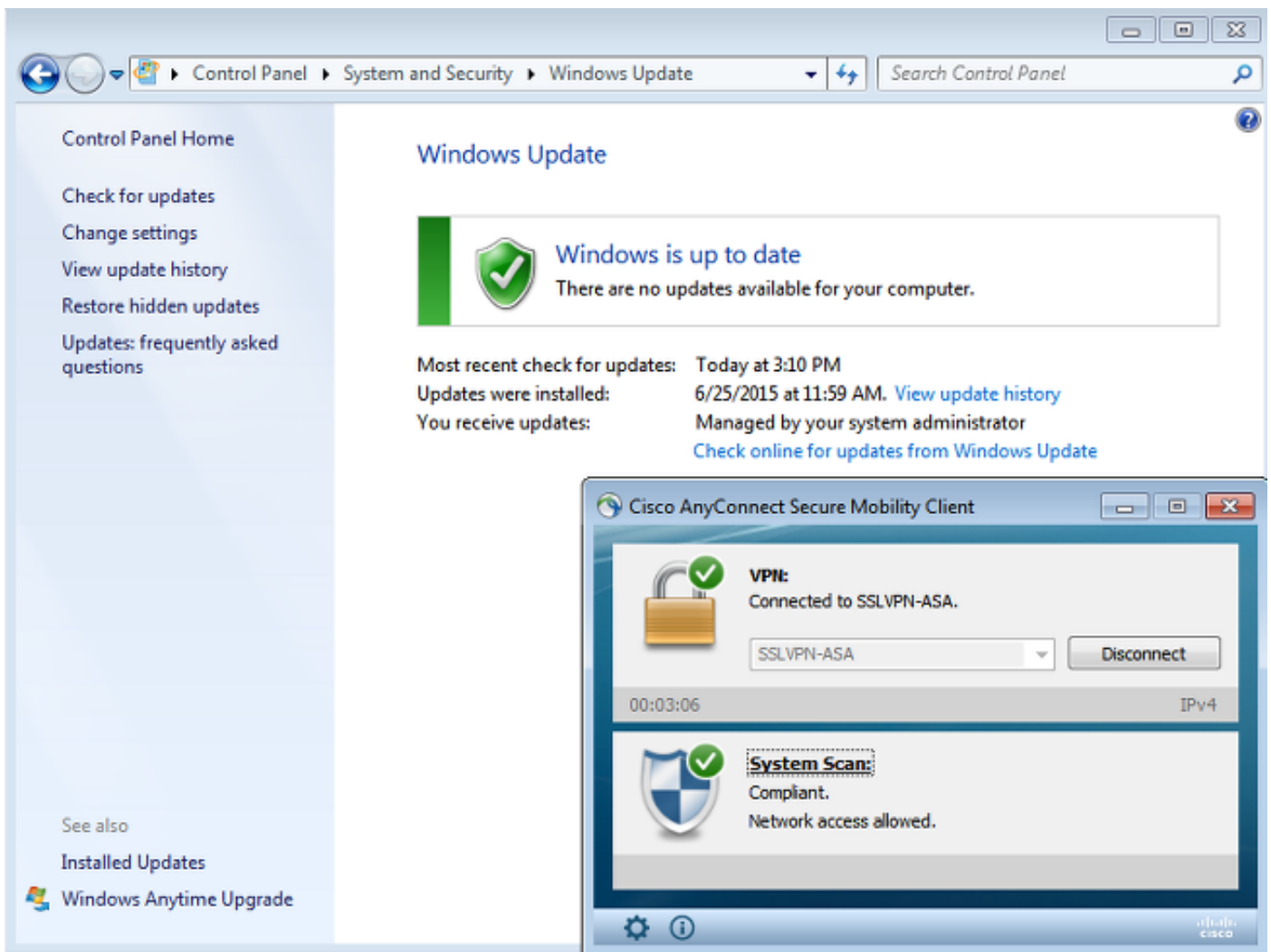
**Hinweis:** Einige der Updates erfordern möglicherweise einen Neustart des Systems.



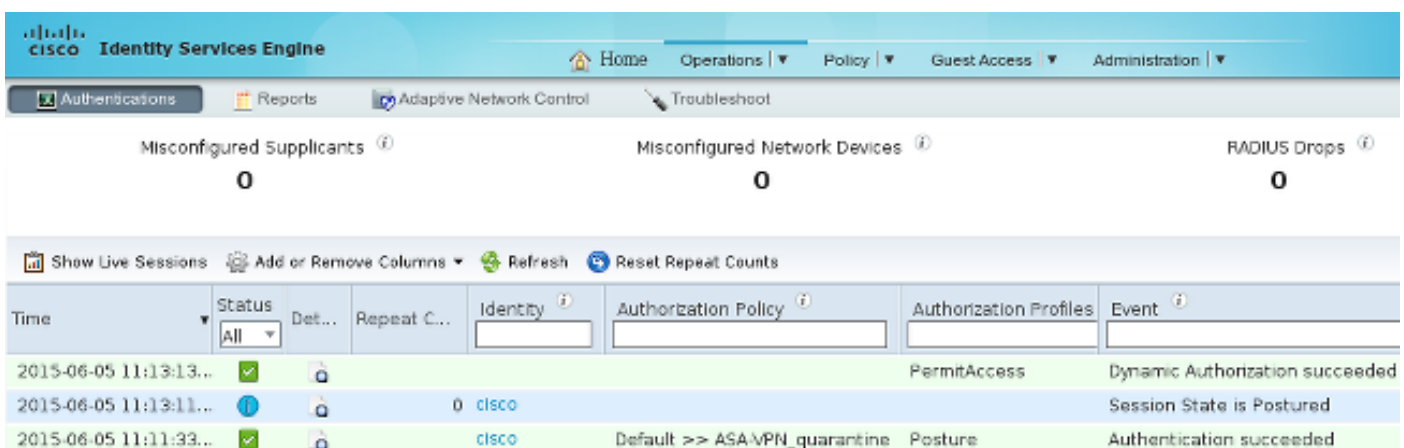


## Vollständiger Netzwerkzugriff

Dies wird angezeigt, nachdem die Station vom AnyConnect-Statusmodul als konform gemeldet wurde:



Der Bericht wird an die ISE gesendet, die die Richtlinie neu bewertet und die *ASA-VPN\_compliance*-Autorisierungsregel aufruft. Dadurch wird der vollständige Netzwerkzugriff (über Radius CoA) gewährleistet. Navigieren Sie zu **Operations > Authentications (Vorgänge > Authentifizierungen)**, um Folgendes zu bestätigen:



Die debugs (**ise-psc.log**) bestätigen auch den Compliance-Status, den CoA-Trigger und die endgültigen Einstellungen für den Status:

```
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]
```

Der ISE Detailed Status Assessment Report bestätigt außerdem, dass die Station die folgenden Richtlinien erfüllt:

## 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

**Hinweis:** Die genaue MAC-Adresse (Media Access Control) der physischen Netzwerkschnittstelle auf dem Microsoft Windows PC ist aufgrund der ACIDEX-Erweiterungen bekannt.

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine Informationen zur Fehlerbehebung verfügbar.

## Wichtige Hinweise

Dieser Abschnitt enthält wichtige Informationen zur Konfiguration, die in diesem Dokument

beschrieben wird.

## Optionsdetails für die WSUS-Bereinigung

Es ist wichtig, die Anforderungsbedingung von der Problembehebung zu unterscheiden. AnyConnect veranlasst den Microsoft Windows Update Agent, die Compliance zu überprüfen, abhängig von der Einstellung *Windows-Updates mithilfe der Problembehebungseinstellungen validieren*.

### 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

In diesem Beispiel wird *der Schweregrad* verwendet. Bei der *kritischen* Einstellung überprüft Microsoft Windows Agent, ob ausstehende (nicht installierte) kritische Updates vorliegen. Wenn dies der Fall ist, beginnt die Problembehebung.

Im Zuge der Problembehebung können dann alle kritischen und weniger wichtigen Updates auf Basis der WSUS-Konfiguration (Updates, die für das jeweilige System genehmigt wurden) installiert werden.

Wenn die *Windows-Updates mithilfe von Cisco Regeln validieren*, entscheiden die in der Anforderung dargelegten Bedingungen, ob die Workstation die Anforderungen erfüllt, darüber.

## Windows Update-Dienst

Für Bereitstellungen ohne WSUS-Server gibt es einen anderen Sanierungstyp, der als *Windows Update Remediation (Windows Update-Problembhebung)* verwendet werden kann:

[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

Dieser Sanierungstyp ermöglicht die Steuerung der Microsoft Windows Update-Einstellungen und die Durchführung sofortiger Aktualisierungen. Eine typische Bedingung für diesen Sanierungstyp ist *pc\_AutoUpdateCheck*. Dadurch können Sie überprüfen, ob die Microsoft Windows Update-Einstellung auf dem Endpunkt aktiviert ist. Falls nicht, können Sie es aktivieren und die Aktualisierung durchführen.

## SCCM-Integration

Eine neue Funktion für die ISE Version 1.4, die als *Patch-Management* bezeichnet wird, ermöglicht die Integration mit zahlreichen Drittanbietern. Je nach Anbieter stehen verschiedene Optionen für die Bedingungen und Abhilfemaßnahmen zur Verfügung.

Microsoft unterstützt sowohl den System Management Server (SMS) als auch den System Center Configuration Manager (SCCM).

## Zugehörige Informationen

- [Statusservices im Cisco ISE-Konfigurationshandbuch](#)
- [Administratoranleitung für Cisco Identity Services Engine, Version 1.4](#)
- [Administratoranleitung für Cisco Identity Services Engine, Version 1.3](#)
- [Bereitstellen von Windows Server Update Services in Ihrer Organisation](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)