

Configurazione della postura di ISE versione 1.4 con Microsoft WSUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Microsoft WSUS](#)

[ASA](#)

[ISE](#)

[Correzione postura per WSUS](#)

[Requisito postura per WSUS](#)

[Profilo AnyConnect](#)

[Regole di provisioning client](#)

[Profili di autorizzazione](#)

[Regole di autorizzazione](#)

[Verifica](#)

[PC con criteri oggetto Criteri di gruppo aggiornati](#)

[Approvare un aggiornamento critico in Windows Server Update Services](#)

[Controllare lo stato del PC in Windows Server Update Services](#)

[Sessione VPN stabilita](#)

[Il modulo Posture riceve le policy dall'ISE ed esegue il monitoraggio e l'aggiornamento](#)

[Accesso completo alla rete](#)

[Risoluzione dei problemi](#)

[Note importanti](#)

[Dettagli delle opzioni per il monitoraggio e l'aggiornamento di WSUS](#)

[Servizio Windows Update](#)

[Integrazione SCCM](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare la funzionalità di postura di Cisco Identity Services Engine (ISE) quando è integrata con Microsoft Windows Server Update Services (WSUS).

Nota: Quando si accede alla rete, si viene reindirizzati all'ISE per il provisioning Cisco AnyConnect Secure Mobility Client versione 4.1 con un modulo di postura, che controlla lo stato di conformità su WSUS e installa gli aggiornamenti necessari per rendere la stazione conforme. Una volta che la stazione è stata dichiarata conforme, ISE consente l'accesso completo alla rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Implementazioni, autenticazione e autorizzazione Cisco ISE
- Conoscenze base del modo in cui operano l'ISE e l'agente di postura Cisco AnyConnect
- Configurazione di Cisco Adaptive Security Appliance (ASA)
- VPN di base e conoscenza 802.1x
- Configurazione di Microsoft WSUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows versione 7
- Microsoft Windows versione 2012 con WSUS versione 6.3
- Cisco ASA versione 9.3.1 e successive
- Software Cisco ISE versione 1.3 e successive

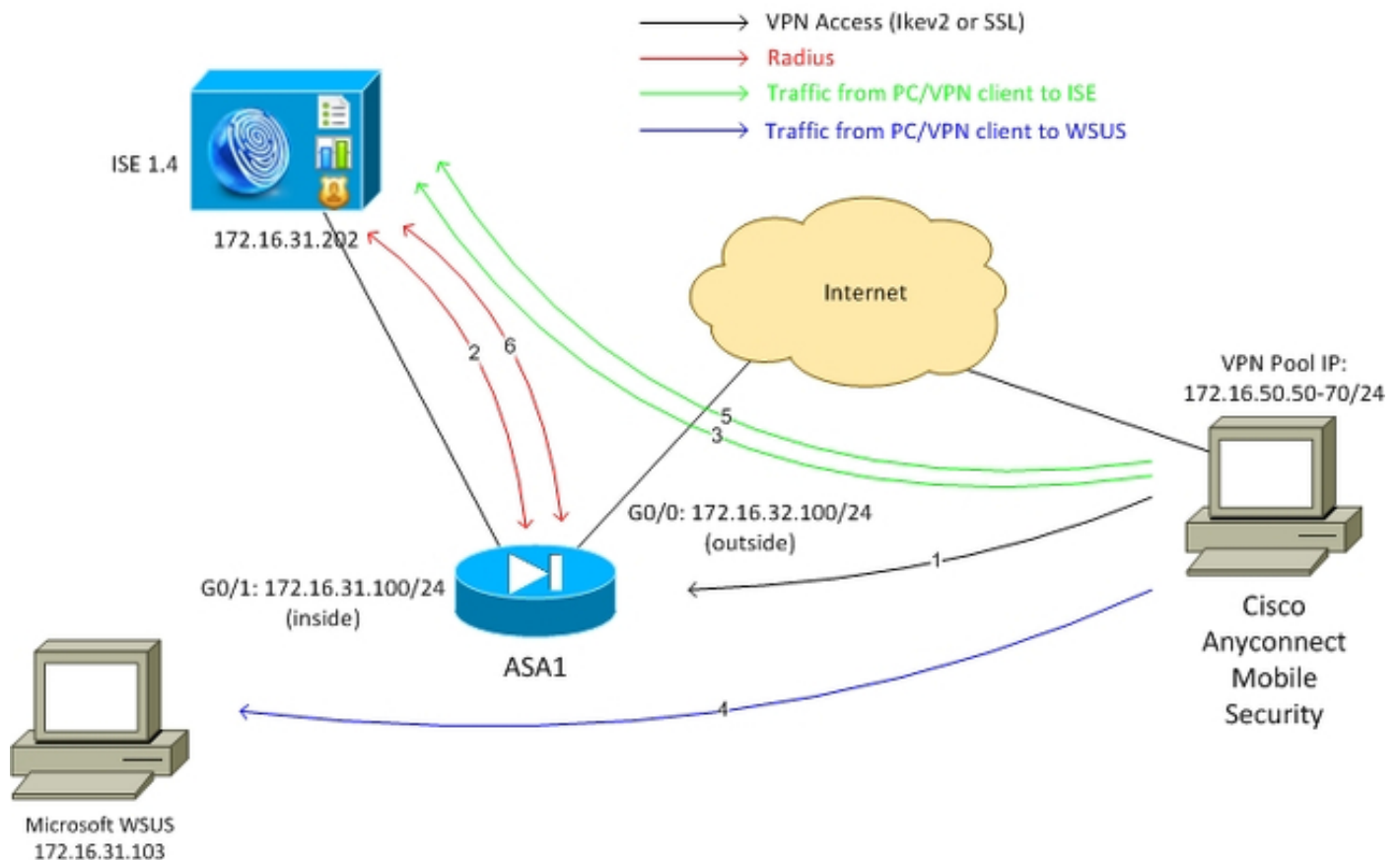
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione viene descritto come configurare l'ISE e i relativi elementi di rete.

Esempio di rete

Questa è la topologia utilizzata per gli esempi riportati nel presente documento:



Di seguito è riportato il flusso del traffico, come mostrato nello schema della rete:

1. L'utente remoto si connette tramite Cisco AnyConnect per l'accesso VPN all'appliance ASA. Può trattarsi di qualsiasi tipo di accesso unificato, ad esempio una sessione cablata 802.1x/MAC Authentication Bypass (MAB) terminata sullo switch o una sessione wireless terminata sul controller WLC.
2. Come parte del processo di autenticazione, ISE conferma che lo stato di postura della stazione terminale non è conforme (regola di autorizzazione *ASA-VPN_quarantine*) e che gli attributi di reindirizzamento vengono restituiti nel messaggio *Radius Access-Accept*. Di conseguenza, l'ASA reindirizza tutto il traffico HTTP all'ISE.
3. L'utente apre un browser Web e immette qualsiasi indirizzo. Dopo il reindirizzamento all'ISE, il modulo di postura Cisco AnyConnect 4 viene installato sulla stazione. Il modulo di postura scarica quindi le policy dall'ISE (requisito per WSUS).
4. Il modulo di postura cerca Microsoft WSUS ed esegue la correzione.
5. Dopo aver risolto con successo il problema, il modulo di postura invia un report all'ISE.
6. L'ISE emette un Radius Change of Authorization (CoA) che fornisce accesso completo alla rete a un utente VPN conforme (regola di autorizzazione *ASA-VPN_compliant*).

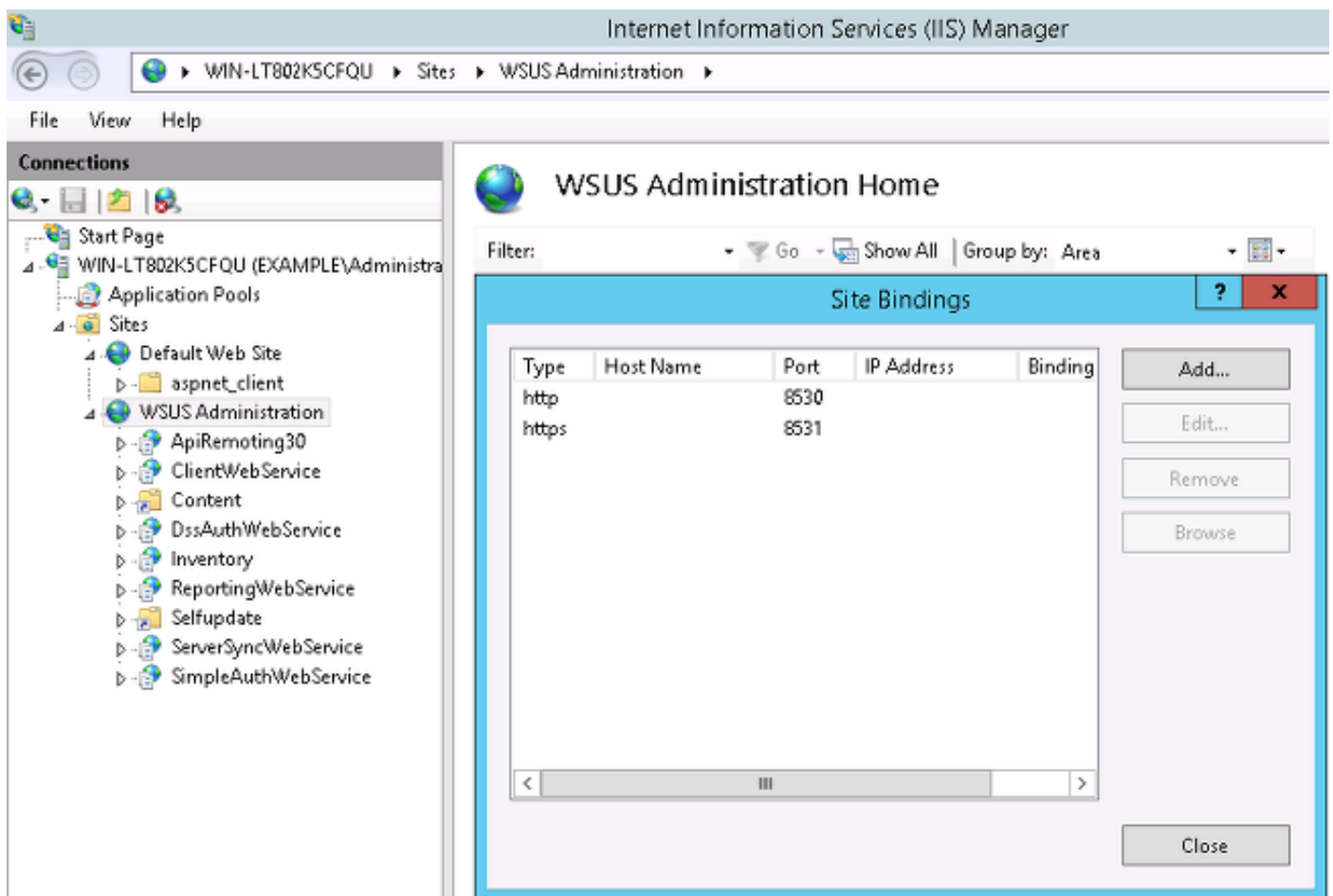
Nota: Per il corretto funzionamento del monitoraggio e dell'aggiornamento (la possibilità di installare gli aggiornamenti di Microsoft Windows in un PC), è necessario che l'utente

disponga di diritti amministrativi locali.

Microsoft WSUS

Nota: Una configurazione dettagliata di WSUS non rientra nell'ambito di questo documento. Per ulteriori informazioni, vedere la documentazione di [Distribuire Windows Server Update Services nell'organizzazione](#) Microsoft.

Il servizio WSUS viene distribuito tramite la porta TCP standard 8530. È importante ricordare che per il monitoraggio e l'aggiornamento vengono utilizzate anche altre porte. Per questo motivo, è consigliabile aggiungere l'indirizzo IP di WSUS all'elenco di controllo di accesso (ACL) di reindirizzamento sull'appliance ASA (descritto più avanti in questo documento).

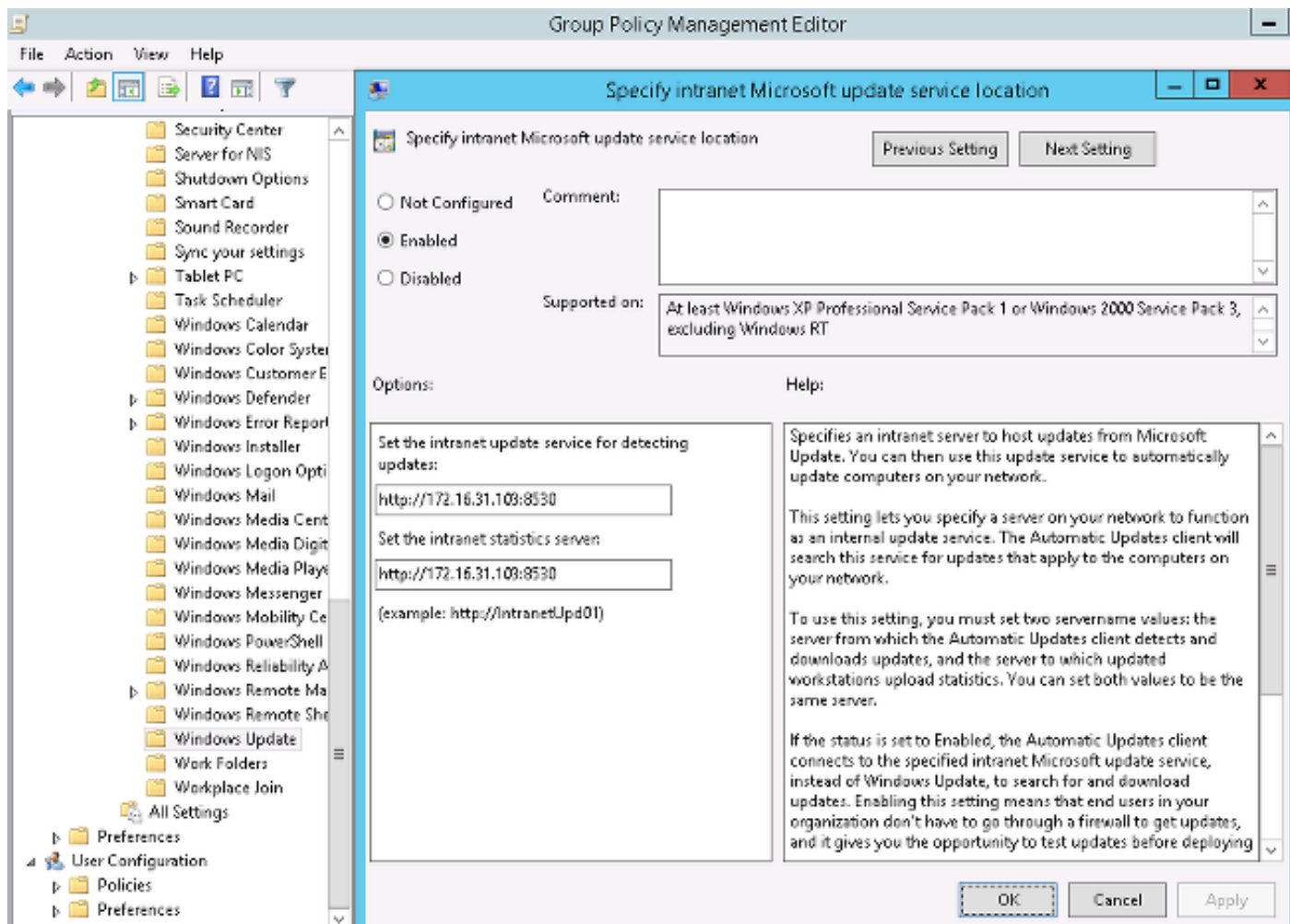


The screenshot shows the Internet Information Services (IIS) Manager interface. The left-hand pane displays the 'Connections' tree, with 'WSUS Administration' selected under the 'Sites' folder. The main pane shows the 'WSUS Administration Home' page. A 'Site Bindings' dialog box is open, displaying a table of bindings for the selected site.

| Type | Host Name | Port | IP Address | Binding |
|-------|-----------|------|------------|---------|
| http | | 8530 | | |
| https | | 8531 | | |

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

I Criteri di gruppo per il dominio sono configurati per gli aggiornamenti di Microsoft Windows e puntano al server WSUS locale:



Di seguito sono riportati gli aggiornamenti consigliati abilitati per i criteri granulari basati su livelli di gravità diversi:

📁 **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 |

Il targeting lato client offre una flessibilità molto maggiore. L'ISE può utilizzare criteri di postura basati sui diversi contenitori di computer di Microsoft Active Directory (AD). WSUS può approvare gli aggiornamenti basati su questa appartenenza.

ASA

Viene utilizzato l'accesso VPN SSL (Secure Sockets Layer) semplice per l'utente remoto (i cui dettagli non rientrano nell'ambito di questo documento).

Di seguito è riportato un esempio di configurazione:

```
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
```

È importante configurare un elenco degli accessi sull'appliance ASA, che viene utilizzata per determinare il traffico da reindirizzare all'ISE (per gli utenti non ancora conformi):

```
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
```

Per gli utenti non conformi è consentito solo il traffico DNS (Domain Name System), ISE, WSUS e

ICMP (Internet Control Message Protocol). Tutto il resto del traffico (HTTP) viene reindirizzato all'ISE per il provisioning AnyConnect 4, che è responsabile della postura e delle operazioni di monitoraggio e aggiornamento.

ISE

Nota: Il provisioning e la postura di AnyConnect 4 non sono compresi nell'ambito di questo documento. Per ulteriori informazioni, ad esempio su come configurare l'ASA come dispositivo di rete e installare l'applicazione Cisco AnyConnect 7, consultare l'[esempio di configurazione dell'integrazione di AnyConnect 4.0 con ISE versione 1.3](#).

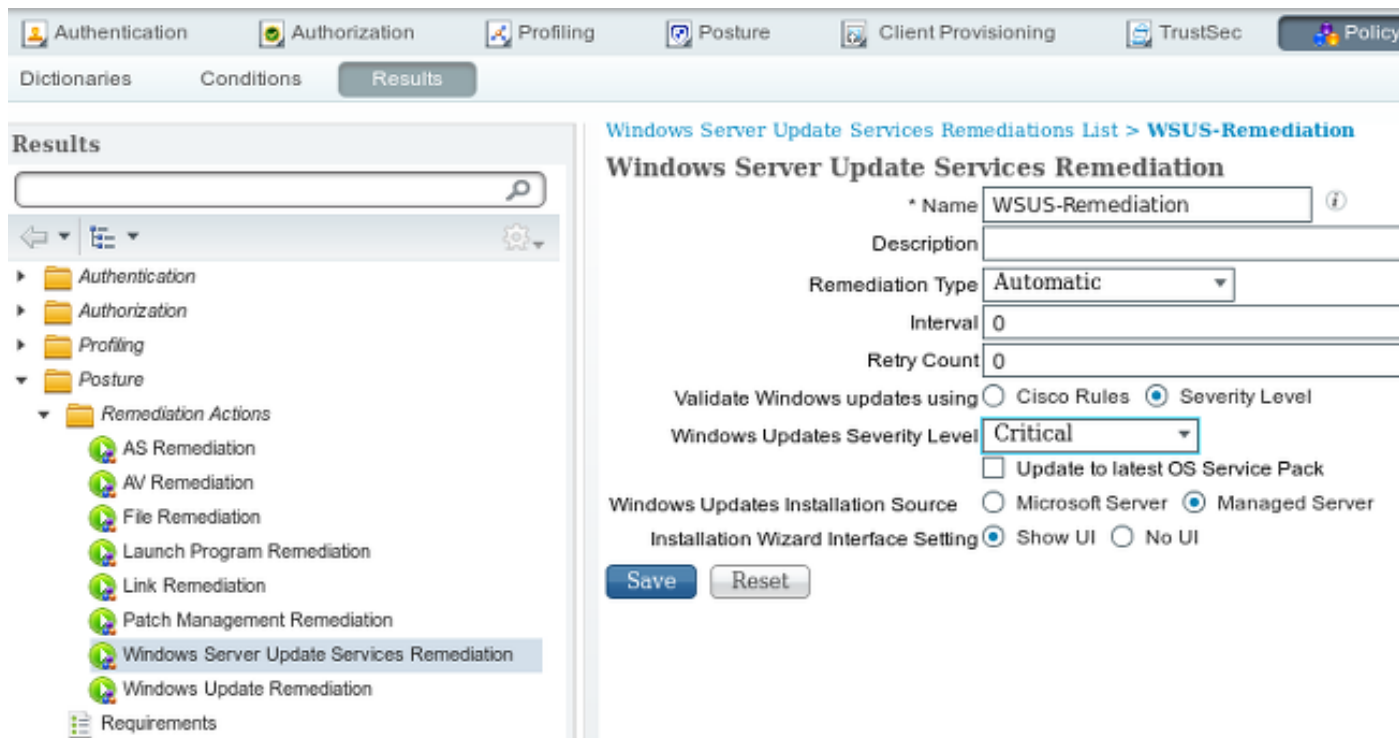
Correzione postura per WSUS

Completare questi passaggi per configurare la correzione della postura per WSUS:

1. Per creare una nuova regola, passare a **Criteri > Condizioni > Postura > Azioni di correzione > Monitoraggio e aggiornamento di Windows Server Update Services**.

2. Verificare che l'impostazione di *Microsoft Windows Updates* sia impostata sul **livello di gravità**. Questa parte è responsabile dell'individuazione dell'avvio del processo di correzione.

L'agente di Microsoft Windows Update si connette quindi a Windows Server Update Services e verifica se sono presenti aggiornamenti *critici* per il PC in attesa dell'installazione:



The screenshot displays the Cisco ISE web interface. At the top, there are navigation tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy. Below these, there are sub-tabs for Dictionaries, Conditions, and Results. The main content area is titled "Results" and shows a tree view on the left with folders for Authentication, Authorization, Profiling, Posture, Remediation Actions, and Requirements. Under Remediation Actions, "Windows Server Update Services Remediation" is selected. The main panel shows the configuration for "Windows Server Update Services Remediation" 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 panel.

Requisito postura per WSUS

Per creare una nuova regola, passare a **Criteri > Condizioni > Postura > Requisiti**. La regola utilizza una condizione fittizia denominata *pr_WSUSRule*, ovvero viene contattato WSUS per

verificare la condizione quando è necessario eseguire il monitoraggio e l'aggiornamento (aggiornamenti *critici*).

Quando questa condizione viene soddisfatta, WSUS installa gli aggiornamenti configurati per il PC. Tra questi sono inclusi tutti i tipi di aggiornamenti e quelli con livelli di gravità inferiori:

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 |

Profilo AnyConnect

Configurare il profilo del modulo di postura insieme al profilo AnyConnect 4 (come descritto nell'[esempio di configurazione di AnyConnect 4.0 Integration con ISE versione 1.3](#)):

Regole di provisioning client

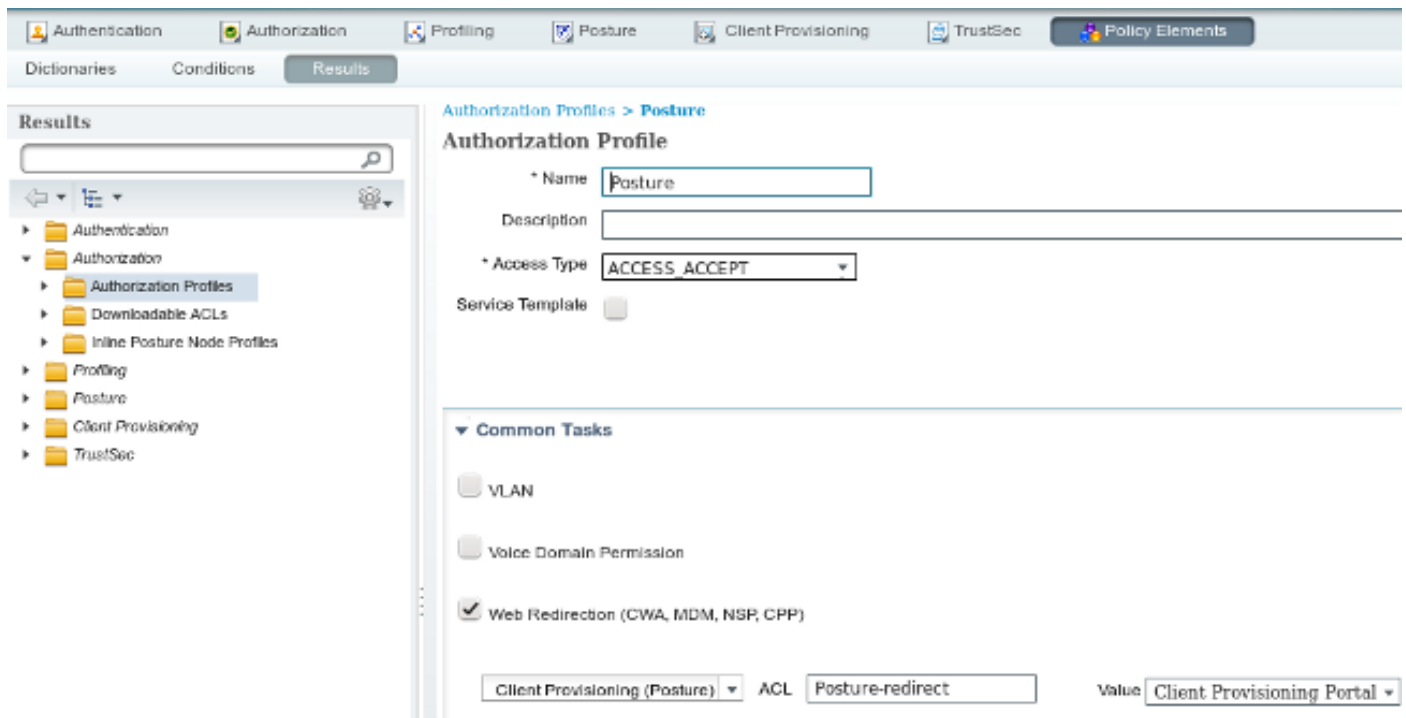
Quando il profilo AnyConnect è pronto, è possibile farvi riferimento dai criteri di *provisioning client*.

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

L'intera applicazione, insieme alla configurazione, viene installata sull'endpoint, che viene reindirizzato alla pagina del portale di provisioning client. È possibile aggiornare AnyConnect 4 e installare un modulo aggiuntivo (postura).

Profili di autorizzazione

Creare un profilo di autorizzazione per il reindirizzamento al profilo di provisioning client:



Regole di autorizzazione

L'immagine mostra le regole di autorizzazione:

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 |

Per la prima volta, viene utilizzata la regola *ASA-VPN_quarantine*. Di conseguenza, viene restituito il profilo di autorizzazione *Posture* e l'endpoint viene reindirizzato al portale di provisioning client per AnyConnect 4 (con modulo posture).

Una volta ottenuta la conformità, viene utilizzata la regola *ASA-VPN_compliant* e viene consentito l'accesso completo alla rete.

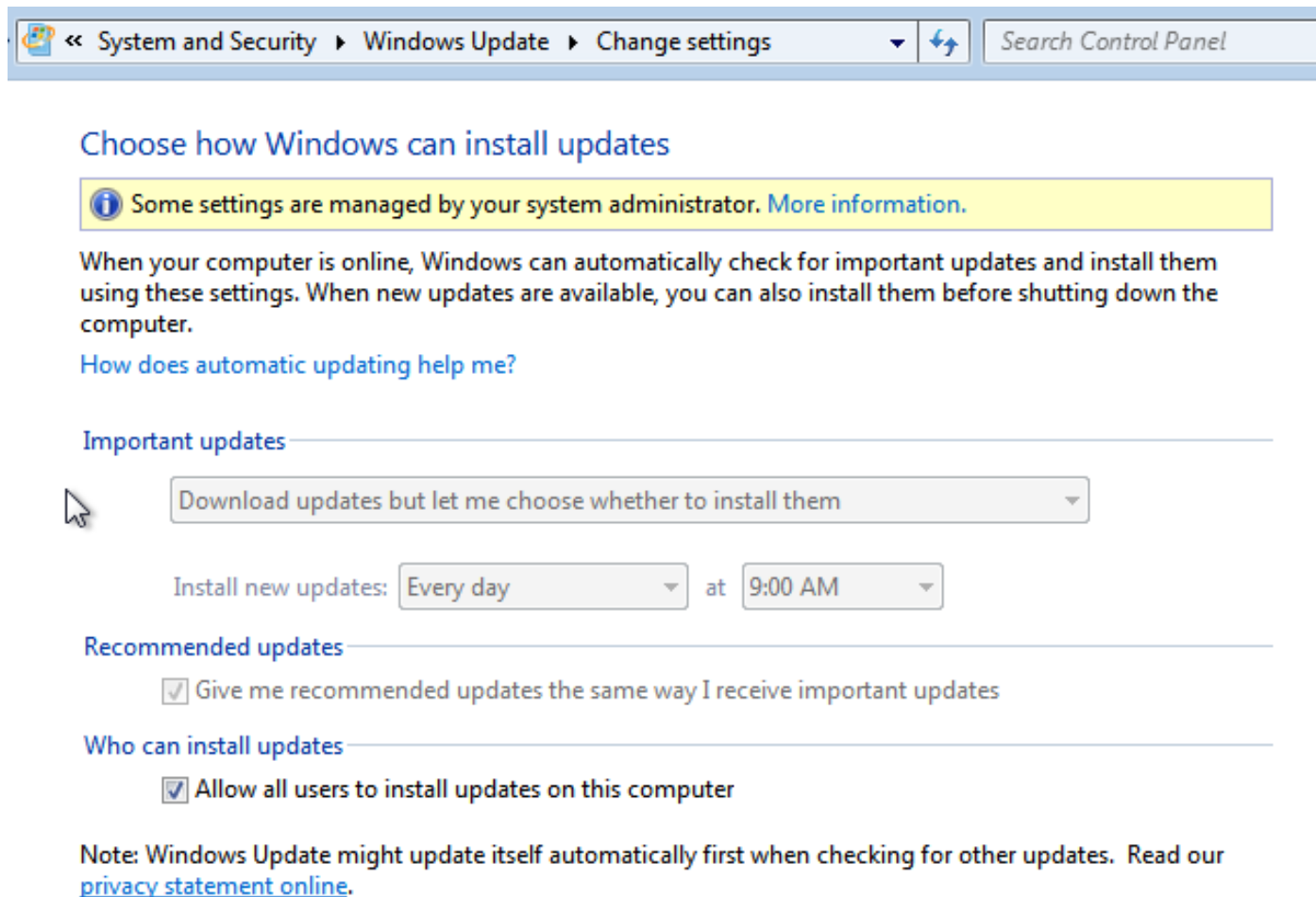
Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

PC con criteri oggetto Criteri di gruppo aggiornati

I criteri di dominio con la configurazione WSUS devono essere sottoposti a push dopo che il PC ha eseguito l'accesso al dominio. Questa situazione può verificarsi prima che la sessione VPN venga stabilita (fuori banda) o dopo l'utilizzo della funzionalità *Avvia prima dell'accesso* (utilizzabile anche per l'accesso wireless/cablato 802.1x).

Una volta che il client Microsoft Windows ha la configurazione corretta, questa può essere riflessa dalle impostazioni di Windows Update:



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

Se necessario, è possibile aggiornare un oggetto Criteri di gruppo e utilizzare l'individuazione del server dell'agente Microsoft Windows Update:

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

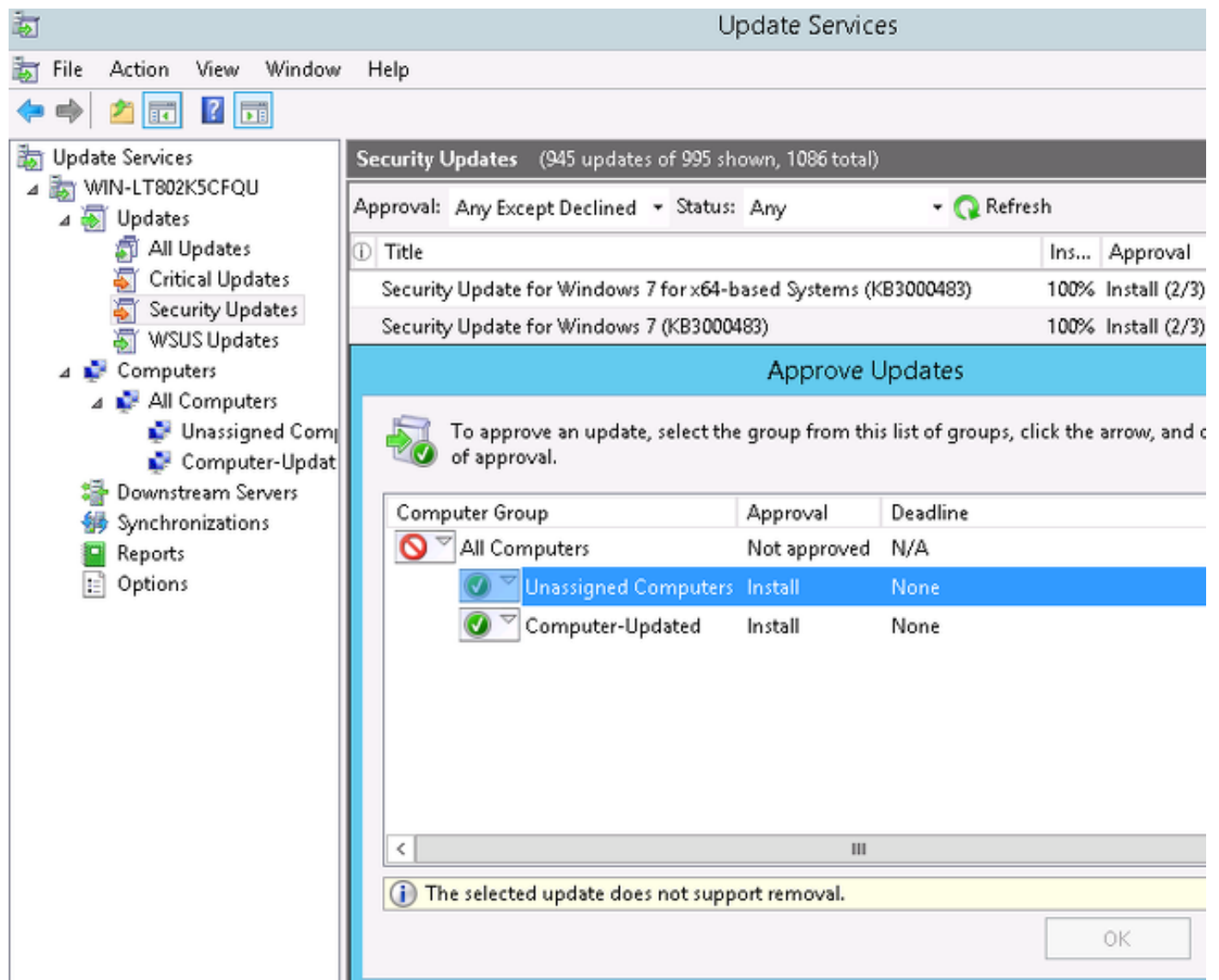
```
User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

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

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

Approvare un aggiornamento critico in Windows Server Update Services

Il processo di approvazione può trarre vantaggio dall'assegnazione dei siti client:



Se necessario, inviare nuovamente il report con *wuclt*.

Controllare lo stato del PC in Windows Server Update Services

In questa immagine viene illustrato come controllare lo stato del PC in Windows Server Update Services:

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:

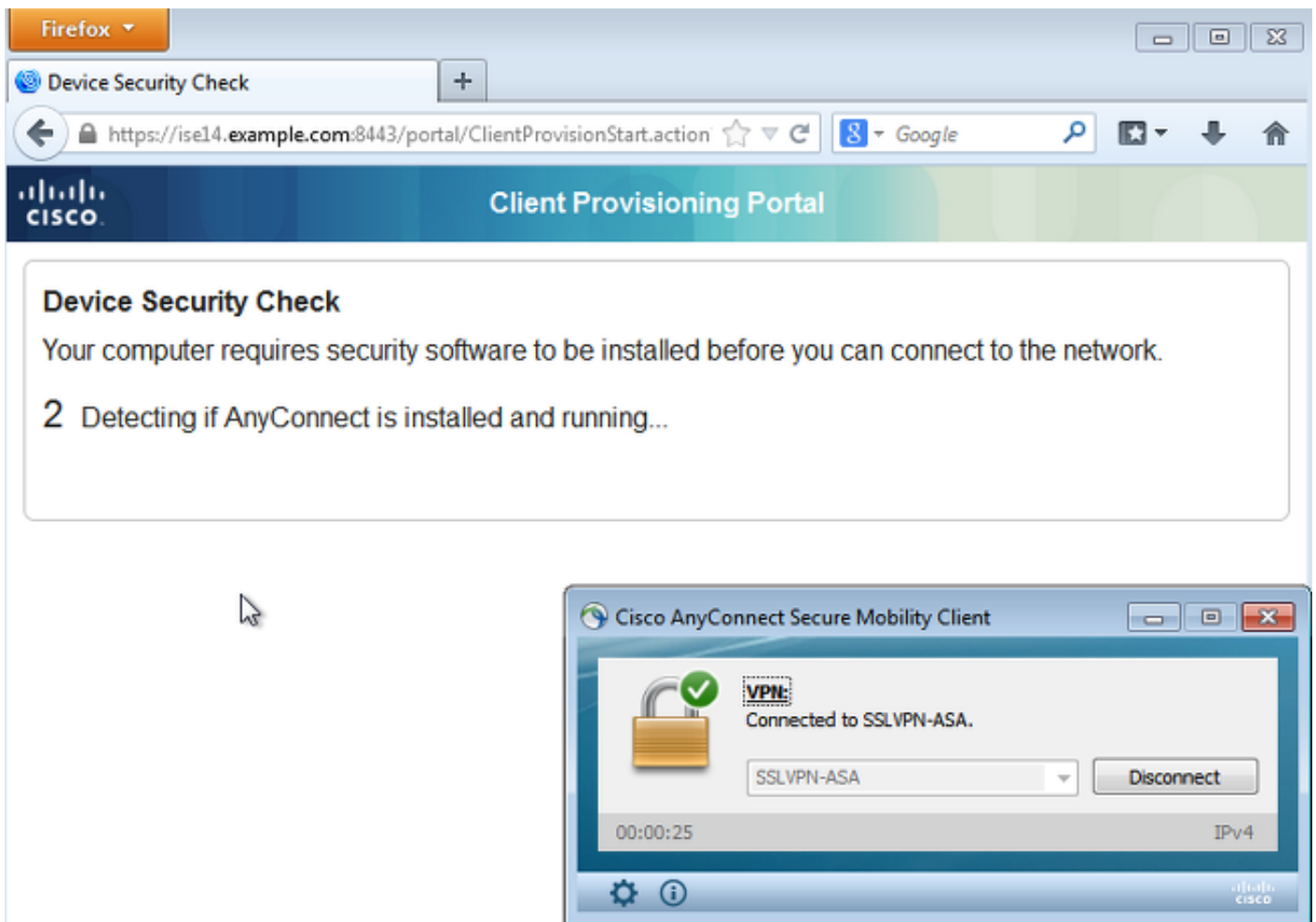
- Updates with errors: 0
- Updates needed: 1
- Updates installed/not applicable: 1035
- Updates with no status: 0

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

È necessario installare un aggiornamento per l'aggiornamento successivo con WSUS.

Sessione VPN stabilita

Dopo aver stabilito la sessione VPN, viene utilizzata la regola di autorizzazione ASA-*VPN_quarantine* ISE, che restituisce il profilo di autorizzazione *Posture*. Di conseguenza, il traffico HTTP dall'endpoint viene reindirizzato per il provisioning del modulo di aggiornamento e postura di AnyConnect 4:



A questo punto, lo stato della sessione sull'appliance ASA indica che l'accesso è limitato con il reindirizzamento del traffico HTTP all'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
```

Il modulo Posture riceve le policy dall'ISE ed esegue il monitoraggio e l'aggiornamento

Il modulo di postura riceve le policy dall'ISE. I debug `ise-psc.log` mostrano il requisito inviato al modulo della postura:

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

```
<encryption>0</encryption>
```

```
<package>
```

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

```
<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>
```

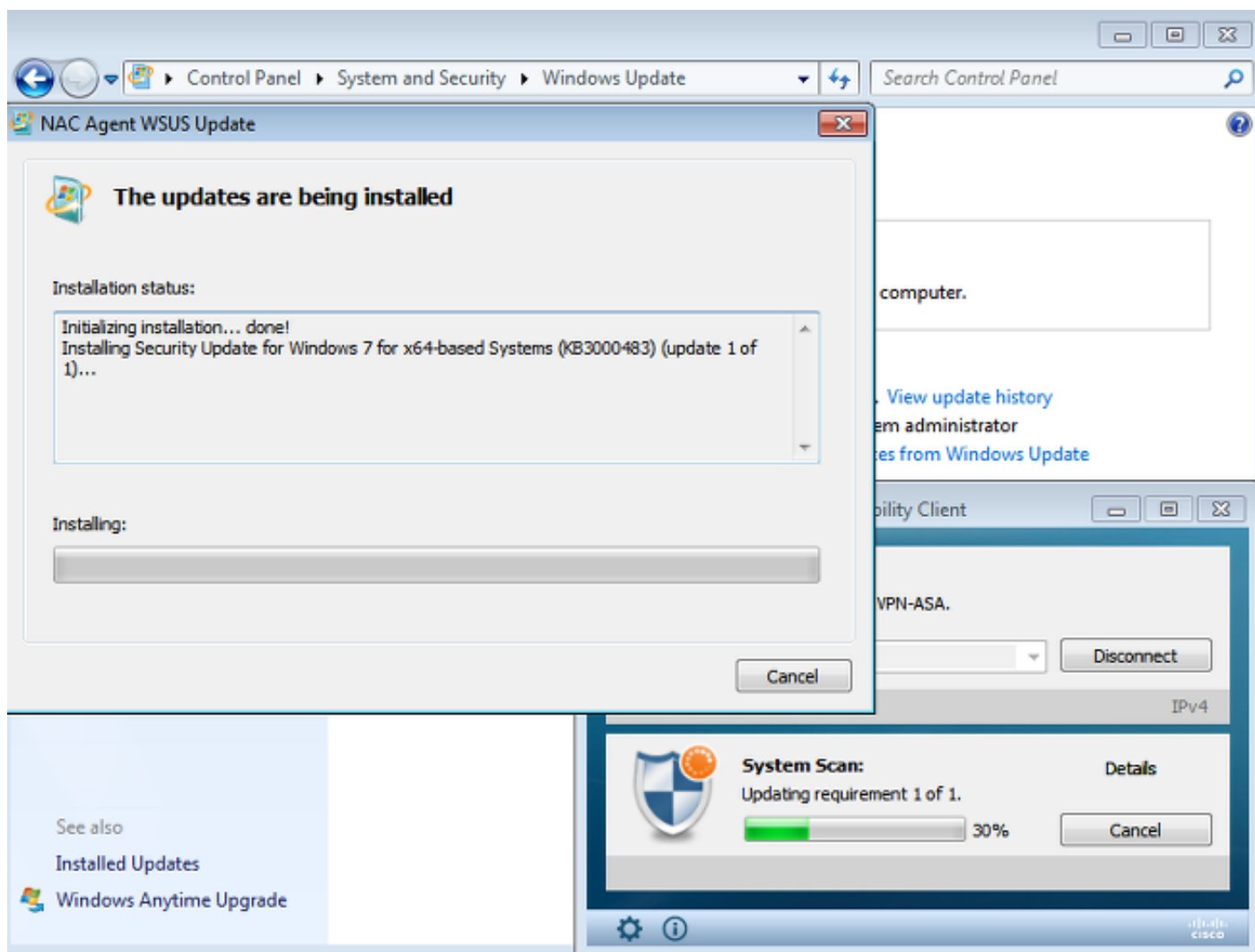
```
</check>
```

```
<criteria/>
```

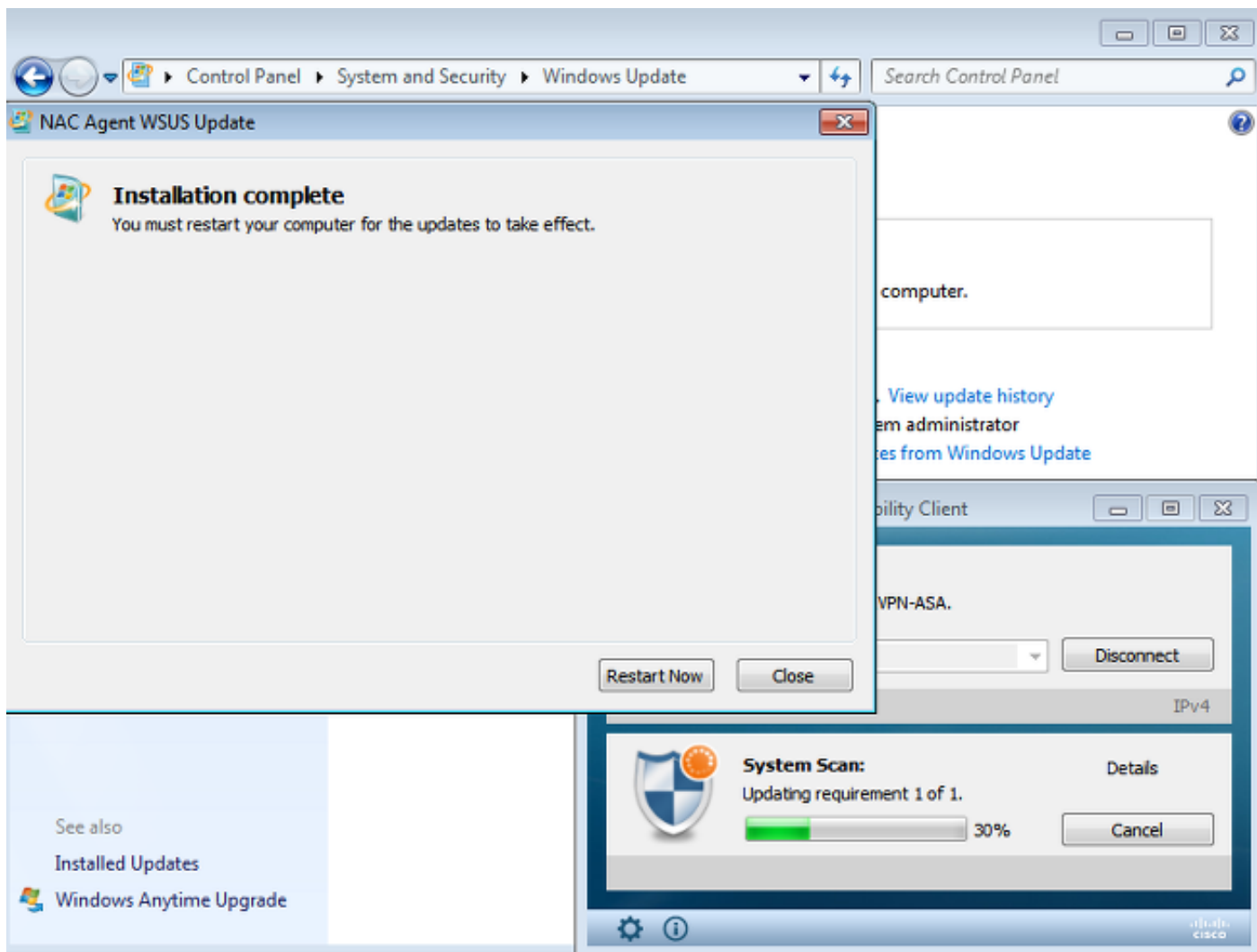
```
</package>
```

```
</cleanmachines>
```

Il modulo di postura attiva automaticamente l'agente di Microsoft Windows Update per la connessione a Windows Server Update Services e il download degli aggiornamenti come configurato nei criteri di Windows Server Update Services (il tutto automaticamente senza alcun intervento da parte dell'utente):

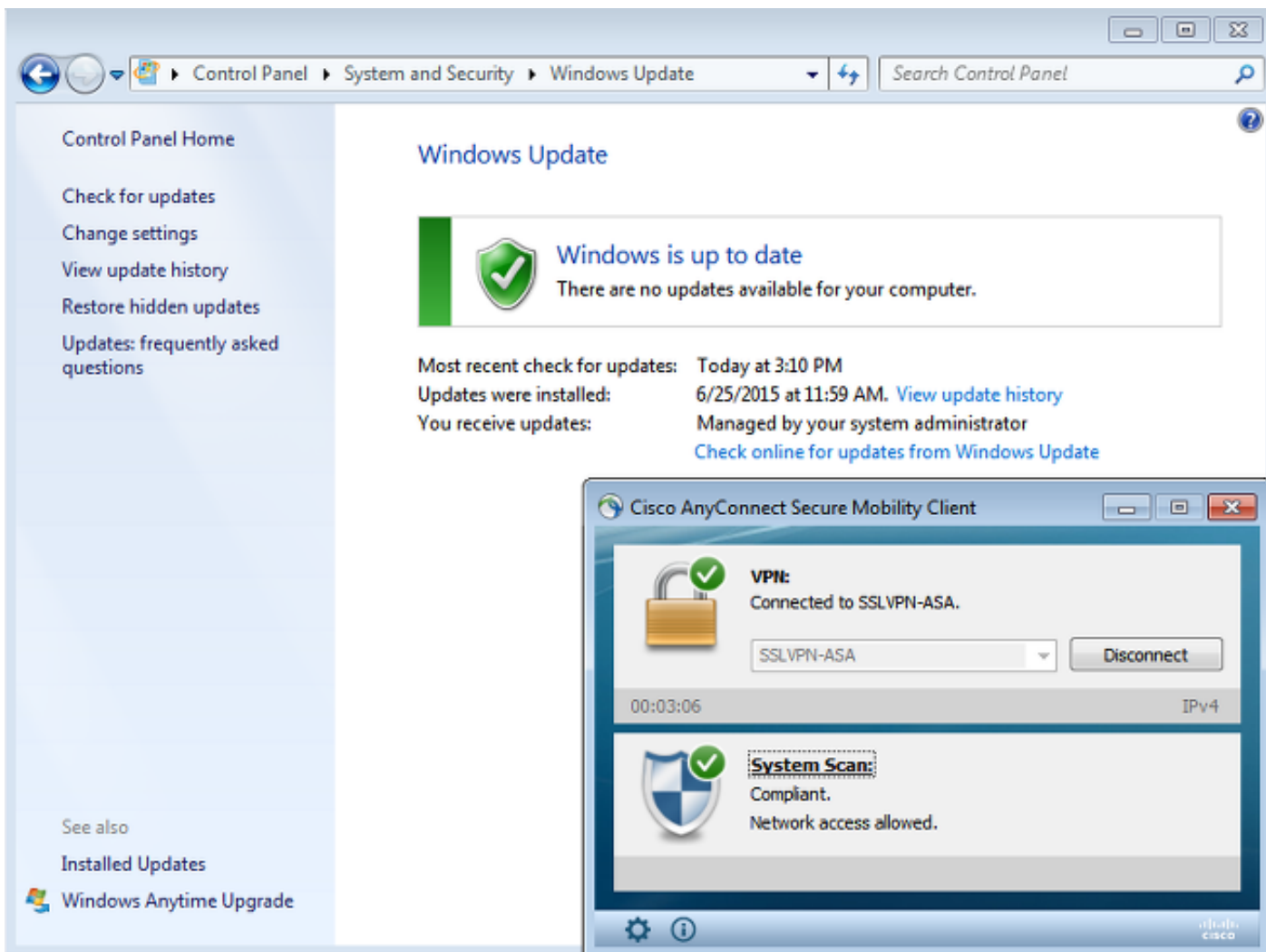


Nota: Per alcuni aggiornamenti potrebbe essere necessario riavviare il sistema.



Accesso completo alla rete

Ciò si verifica quando la stazione viene segnalata come conforme dal modulo di postura di AnyConnect:



Il report viene inviato all'ISE, che valuta nuovamente la policy e incontra la regola di autorizzazione *ASA-VPN_compliant*. Ciò consente l'accesso completo alla rete (tramite Radius CoA). Per verificare questa condizione, passare a **Operazioni > Autenticazioni**:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs for Home, Operations, Policy, Guest Access, and Administration. Below these are several status indicators: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), and 'RADIUS Drops' (0). The main area displays a table of authentication sessions.

| Time | Status | Det... | Repeat C... | Identity | Authorization Policy | Authorization Profiles | Event |
|------------------------|--------|--------|-------------|----------|-------------------------------|------------------------|---------------------------------|
| 2015-06-05 11:13:13... | ✓ | 🔒 | | | | PermitAccess | Dynamic Authorization succeeded |
| 2015-06-05 11:13:11... | ⓘ | 🔒 | 0 | cisco | | | Session State is Postured |
| 2015-06-05 11:11:33... | ✓ | 🔒 | | cisco | Default >> ASA-VPN_quarantine | Posture | Authentication succeeded |

I debug (*ise-psc.log*) confermano anche lo stato di conformità, il trigger CoA e le impostazioni finali per la postura:

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

ac101f6400039000556b4200

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

```
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:ac101f6400039000556b4200::- DM_PKG report non-AUP:html = <!--X-Perfigo-DM-Error=0--><!--error=0--><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--><!--X-Perfigo-Auto-Close-Login-Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--><!--user role=--><!--X-Perfigo-OrigRole=--><!--X-Perfigo-UserKey=dummykey--><!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-Perfigo-Session=--><!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter--><!--X-Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4--><!--X-Perfigo-DHCP-Renew-Delay=1--><!--X-Perfigo-Client-MAC=08:00:27:DA:EF:AD-->
```

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

Inoltre, il report ISE Detailed Posture Assessment conferma che la stazione è conforme:

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 |

Nota: L'indirizzo MAC (Media Access Control) esatto dell'interfaccia di rete fisica sul PC Microsoft Windows è noto a causa delle estensioni ACIDEX.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni sulla risoluzione dei problemi per questa configurazione.

Note importanti

In questa sezione vengono fornite alcune informazioni importanti sulla configurazione descritta in

questo documento.

Dettagli delle opzioni per il monitoraggio e l'aggiornamento di WSUS

È importante distinguere la condizione del requisito dalla correzione. AnyConnect attiva l'agente di Microsoft Windows Update per verificare la conformità, a seconda dell'impostazione di *convalida degli aggiornamenti di Windows tramite* monitoraggio e aggiornamento.

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

Per questo esempio viene utilizzato il *livello di gravità*. Con l'impostazione *Critico*, l'agente di Microsoft Windows controlla se sono presenti aggiornamenti critici in sospeso (non installati). In caso affermativo, verrà avviata la risoluzione.

Il processo di monitoraggio e aggiornamento potrebbe quindi installare tutti gli aggiornamenti critici e meno importanti in base alla configurazione di WSUS (aggiornamenti approvati per il computer specifico).

Se l'opzione *Convalida aggiornamenti di Windows tramite* è impostata su **Cisco Rules**, la conformità della stazione è determinata dalle condizioni descritte nei requisiti.

Servizio Windows Update

Per le distribuzioni senza un server WSUS, è possibile utilizzare un altro tipo di monitoraggio e aggiornamento denominato *Monitoraggio e aggiornamento di Windows Update*:

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

Windows Update Remediation

* Name ⓘ

Description

Remediation Type

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

Retry Count (Valid Range 0 to 99)

Windows Update Setting

Override User's Windows Update setting with administrator's

Questo tipo di monitoraggio e aggiornamento consente di controllare le impostazioni di Microsoft Windows Update e di eseguire aggiornamenti immediati. Una condizione tipica utilizzata con questo tipo di monitoraggio e aggiornamento è *pc_AutoUpdateCheck*. In questo modo è possibile verificare se l'impostazione di Microsoft Windows Update è abilitata sull'endpoint. In caso contrario, è possibile attivarlo ed eseguire l'aggiornamento.

Integrazione SCCM

Una nuova funzione di ISE versione 1.4, chiamata *gestione delle patch*, consente l'integrazione con molti fornitori terzi. A seconda del fornitore, sono disponibili diverse opzioni sia per le condizioni che per le soluzioni.

Per Microsoft sono supportati sia il server di gestione del sistema (SMS) che System Center Configuration Manager (SCCM).

Informazioni correlate

- [Servizi di postura nella guida alla configurazione di Cisco ISE](#)
- [Guida dell'amministratore di Cisco Identity Services Engine, versione 1.4](#)
- [Guida dell'amministratore di Cisco Identity Services Engine, versione 1.3](#)
- [Distribuire Windows Server Update Services nell'organizzazione](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)