

Configure ISE Version 1.4 Posture with Microsoft WSUS



Document ID: 119214

Contributed by Michal Garcarz, Cisco TAC Engineer.
Aug 03, 2015

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Network Diagram
- Microsoft WSUS
- ASA
- ISE
 - Posture Remediation for WSUS
 - Posture Requirement for WSUS
 - AnyConnect Profile
 - Client Provisioning Rules
 - Authorization Profiles
 - Authorization Rules

Verify

- PC with Updated GPO Policies
- Approve a Critical Update on the WSUS
- Check the PC Status on the WSUS
- VPN Session Established
- Posture Module Receives Policies from the ISE and Performs Remediation
- Full Network Access

Troubleshoot

Important Notes

- Option Details for WSUS Remediation
- Windows Update Service
- SCCM Integration

Related Information

Introduction

This document describes how to configure the Cisco Identity Services Engine (ISE) posture functionality when it is integrated with the Microsoft Windows Server Update Services (WSUS).

Note: When you access the network, you are redirected to the ISE for Cisco AnyConnect Secure Mobility Client Version 4.1 provisioning with a posture module, which checks the compliance status on the WSUS and installs the necessary updates in order for the station to be compliant. Once the station is reported as compliant, the ISE allows for full network access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ISE deployments, authentication, and authorization
- Basic knowledge about the way in which the ISE and the Cisco AnyConnect posture agent operate
- Configuration of the Cisco Adaptive Security Appliance (ASA)
- Basic VPN and 802.1x knowledge
- Configuration of the Microsoft WSUS

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows Version 7
- Microsoft Windows Version 2012 with WSUS Version 6.3
- Cisco ASA Versions 9.3.1 and later
- Cisco ISE software Versions 1.3 and later

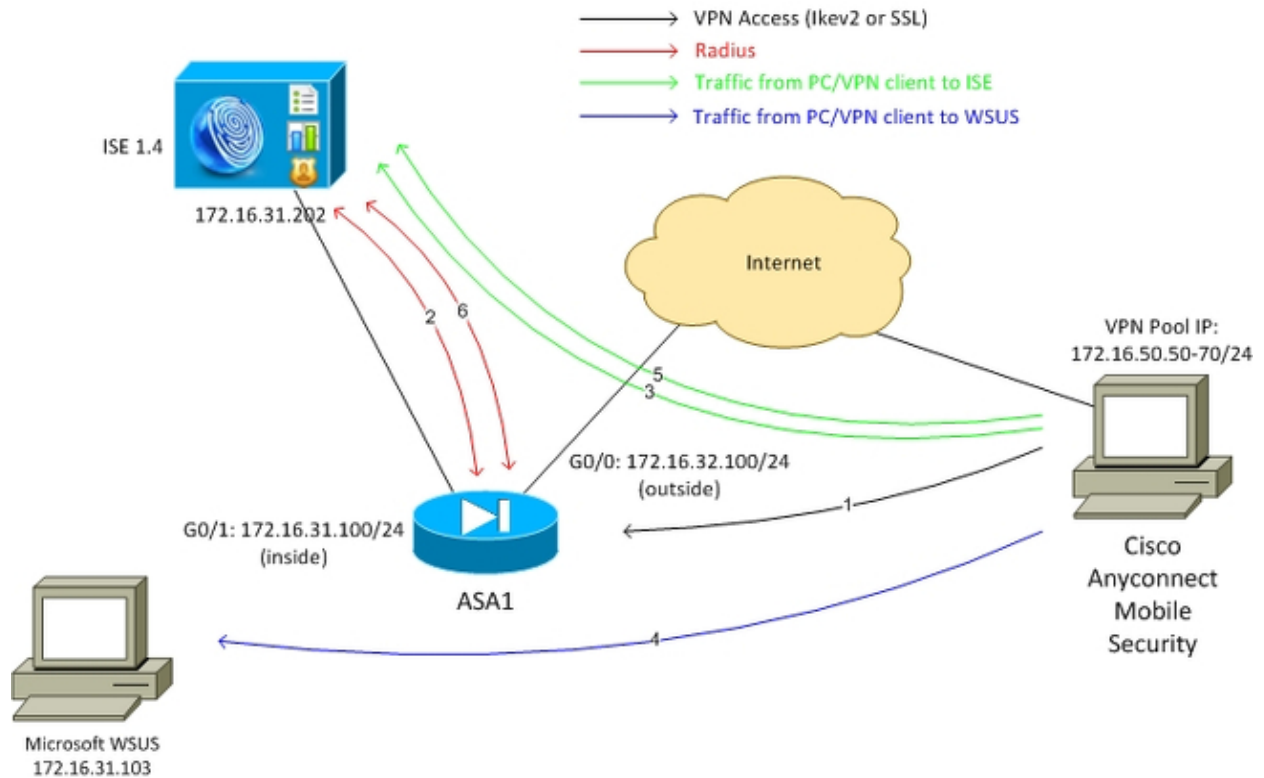
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

This section describes how to configure the ISE and related network elements.

Network Diagram

This is the topology that is used for the examples throughout this document:



Here is the traffic flow, as illustrated in the network diagram:

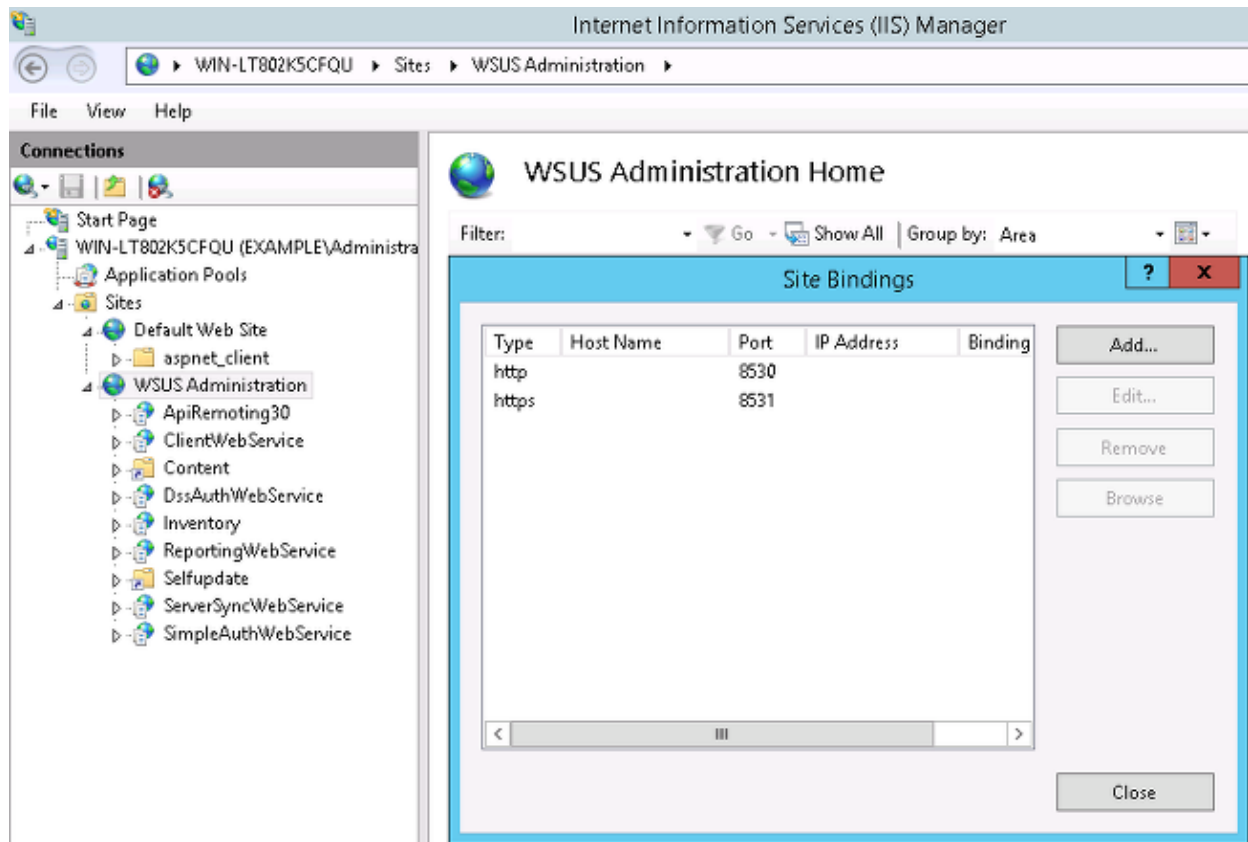
1. The remote user connects through Cisco AnyConnect for VPN access to the ASA. This can be any type of unified access, such as an 802.1x/MAC Authentication Bypass (MAB) wired session that is terminated on the switch or a wireless session that is terminated on the Wireless LAN Controller (WLC).
2. As a part of the authentication process, the ISE confirms that the posture status of the end station is not equal to compliant (*ASA-VPN_quarantine* authorization rule) and that the redirection attributes are returned in the *Radius Access-Accept* message. As a result, the ASA redirects all of the HTTP traffic to the ISE.
3. The user opens a web browser and enters any address. After the redirection to the ISE, the Cisco AnyConnect 4 posture module is installed on the station. The posture module then downloads the policies from the ISE (requirement for WSUS).
4. The posture module searches for Microsoft WSUS, and performs remediation.
5. After successful remediation, the posture module sends a report to the ISE.
6. The ISE issues a Radius Change of Authorization (CoA) that provides full network access to a compliant VPN user (*ASA-VPN_compliant* authorization rule).

Note: In order for the remediation to work (the ability to install Microsoft Windows updates on a PC), the user should have local administrative rights.

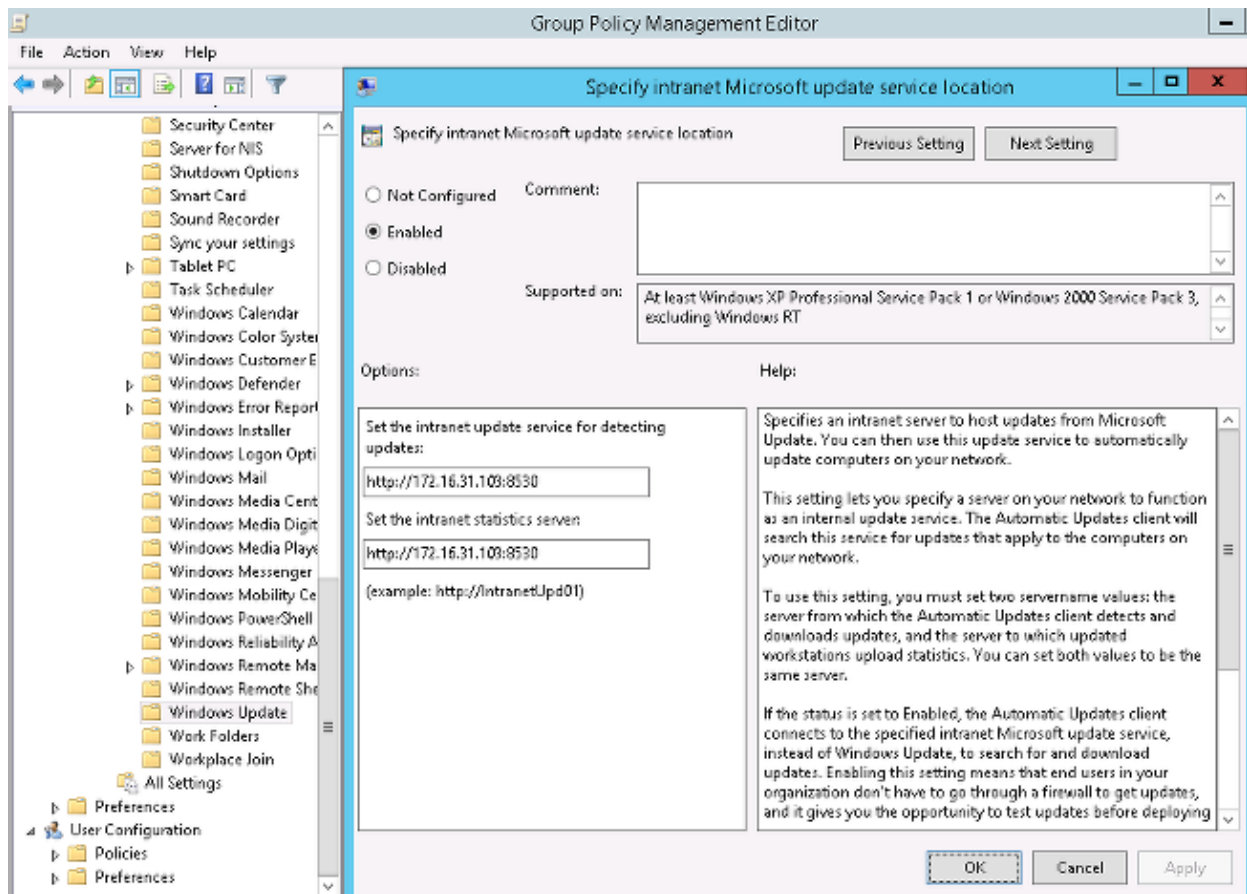
Microsoft WSUS

Note: A detailed configuration of the WSUS is out of the scope of this document. For details, refer to the *Deploy Windows Server Update Services in Your Organization* Microsoft documentation.

The WSUS service is deployed through the standard TCP port 8530. It is important to remember that for remediation, other ports are also used. This is why it is safe to add the IP address of WSUS to the redirection Access Control List (ACL) on the ASA (described later in this document).



The group policy for the domain is configured for Microsoft Windows updates and points to the local WSUS server:



These are the recommended updates that are enabled for granular policies that are based on different levels of severity:

| Windows Update | |
|---|----------------|
| 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 |

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.

The client-side targeting allows for far greater flexibility. The ISE can use posture policies that are based on the different Microsoft Active Directory (AD) computer containers. The WSUS can approve updates that are

based on this membership.

ASA

Simple Secure Sockets Layer (SSL) VPN access for the remote user is employed (the details of which are out of the scope of this document).

Here is an example configuration:

```
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
```

It is important to configure an access-list on the ASA, which is used in order to determine the traffic that should be redirected to the ISE (for users that are not yet compliant):

```
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
```

Only Domain Name System (DNS), ISE, WSUS, and Internet Control Message Protocol (ICMP) traffic is allowed for non-compliant users. All of the other traffic (HTTP) is redirected to the ISE for AnyConnect 4 provisioning, which is responsible for the posture and remediation.

ISE

Note: AnyConnect 4 provisioning and posture is out of the scope of this document. Refer to the AnyConnect 4.0 Integration with ISE Version 1.3 Configuration Example for more details, such as how to configure the ASA as a network device and install the Cisco AnyConnect 7 application.

Posture Remediation for WSUS

Complete these steps in order to configure the posture remediation for WSUS:

1. Navigate to **Policy > Conditions > Posture > Remediation Actions > Windows Server Update Services Remediation** in order to create a new rule.
2. Verify that the *Microsoft Windows Updates* setting is set to **Severity Level**. This part is responsible for detection if the remediation process is initiated.

The Microsoft Windows Update Agent then connects to the WSUS and checks whether there are any *Critical* updates for that PC that await installation:

The screenshot shows the Cisco ISE Policy configuration interface. The top navigation bar includes tabs for 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 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

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

Posture Requirement for WSUS

Navigate to **Policy > Conditions > Posture > Requirements** in order to create a new rule. The rule uses a dummy condition called *pr_WSUSRule*, which means that the WSUS is contacted in order to check for the condition when remediation is necessary (*Critical* updates).

Once this condition is met, the WSUS installs the updates that have been configured for that PC. These can include any type of updates, and also those with lower severity levels:

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 Profile

Configure the posture module profile, along with the AnyConnect 4 profile (as described in the AnyConnect 4.0 Integration with ISE Version 1.3 Configuration Example):

The screenshot shows the Cisco ISE Policy Elements configuration interface for the 'AnyConnect Configuration' posture module. The interface includes a navigation pane on the left with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, Resources, and TrustSec. The main configuration area is titled 'AnyConnect Configuration > AnyConnect Configuration' and contains the following settings:

- Select AnyConnect Package:** AnyConnectDesktopWindows 4.1.2011.0
- Configuration Name:** AnyConnect Configuration
- Description:** (Empty text box)
- Description Value:** (Empty text box)
- Compliance Module:** AnyConnectComplianceModuleWindows 3.6.9

Under the **AnyConnect Module Selection** section, the following options are checked:

- ISE Posture
- VPN

The following options are unchecked:

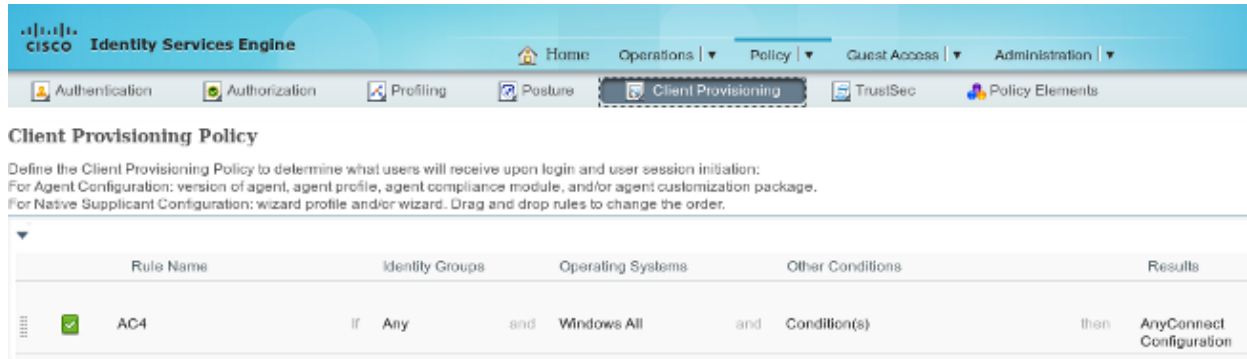
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Start Before Logon
- Diagnostic and Reporting Tool

Under the **Profile Selection** section:

- ISE Posture:** AC4 profile
- VPN:** (Empty dropdown menu)

Client Provisioning Rules

Once the AnyConnect profile is ready, it can be referenced from the *Client Provisioning* policy:



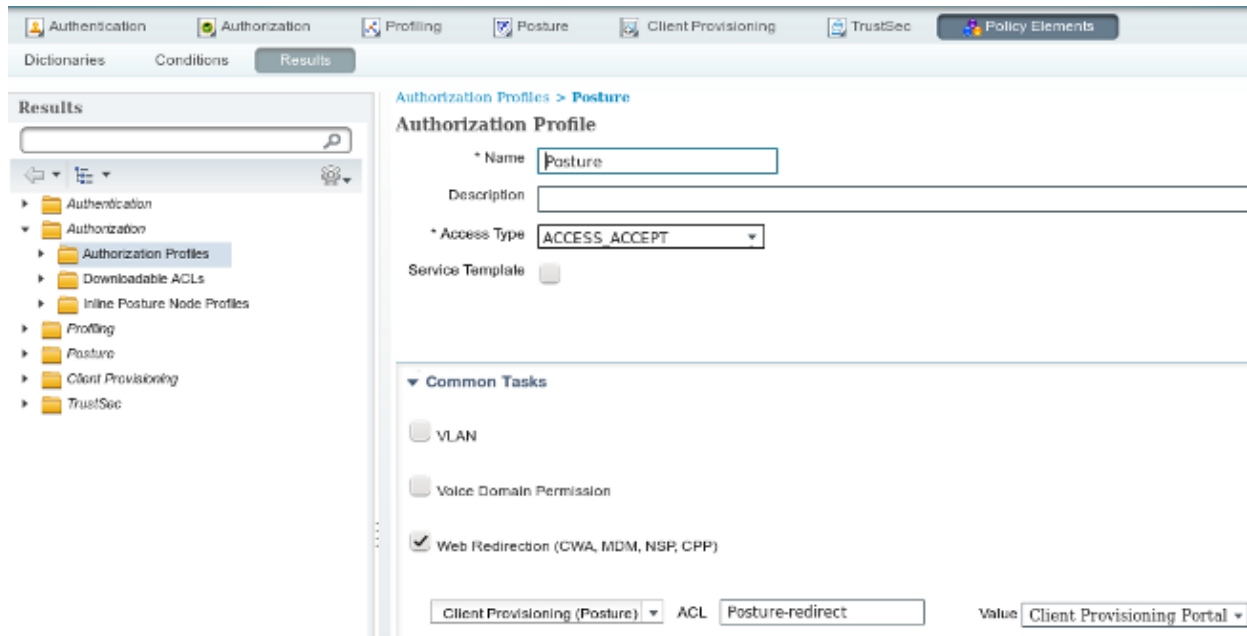
The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Client Provisioning Policy. The navigation bar includes Home, Operations, Policy, Guest Access, and Administration. The main menu has Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The Client Provisioning Policy configuration page is displayed, showing a table with one rule named 'AC4'. The rule is configured with the following conditions: 'If Any and Windows All and Condition(s) then AnyConnect Configuration'. The 'AC4' rule is marked with a green checkmark.

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

The entire application, along with the configuration, is installed on the endpoint, which is redirected to the Client Provisioning portal page. AnyConnect 4 might be upgraded and an additional module (posture) installed.

Authorization Profiles

Create an authorization profile for redirection to the Client Provisioning profile:



The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Profile. The navigation bar includes Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The main menu has Dictionaries, Conditions, and Results. The Authorization Profile configuration page is displayed, showing the following settings: Name: Posture, Description: (empty), Access Type: ACCESS_ACCEPT, Service Template: (unchecked). Under Common Tasks, Web Redirection (CWA, MDM, NSP, CPP) is checked. The ACL is configured as Posture-redirect with a value of Client Provisioning Portal.

Authorization Profiles > Posture

Authorization Profile

* Name: Posture

Description: (empty)

* Access Type: ACCESS_ACCEPT

Service Template:

Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: Posture-redirect Value: Client Provisioning Portal

Authorization Rules

This image shows the authorization rules:

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 |

For the first time, the *ASA-VPN_quarantine* rule is used. As a result, the *Posture* authorization profile is returned, and the endpoint is redirected to the Client Provisioning portal for AnyConnect 4 (with posture module) provisioning.

Once compliant, the *ASA-VPN_compliant* rule is used and full network access is allowed.

Verify

This section provides information that you can use in order to verify that your configuration works properly.

PC with Updated GPO Policies

The domain policies with the WSUS configuration should be pushed after the PC logs into the domain. This can occur before the VPN session is established (out of band) or after if the *Start Before Logon* functionality is used (it can be also used for 802.1x wired/wireless access).

Once the Microsoft Windows client has the correct configuration, this can be reflected from the Windows Update settings:

Choose how Windows can install updates

i Some settings are managed by your system administrator. [More information.](#)

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.

[How does automatic updating help me?](#)

Important updates

Download updates but let me choose whether to install them

Install new updates: Every day at 9:00 AM

Recommended updates

Give me recommended updates the same way I receive important updates

Who can install updates

Allow all users to install updates on this computer

Note: Windows Update might update itself automatically first when checking for other updates. Read our [privacy statement online.](#)

If needed, a Group Policy Object (GPO) refresh and Microsoft Windows Update Agent server discovery can be used:

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

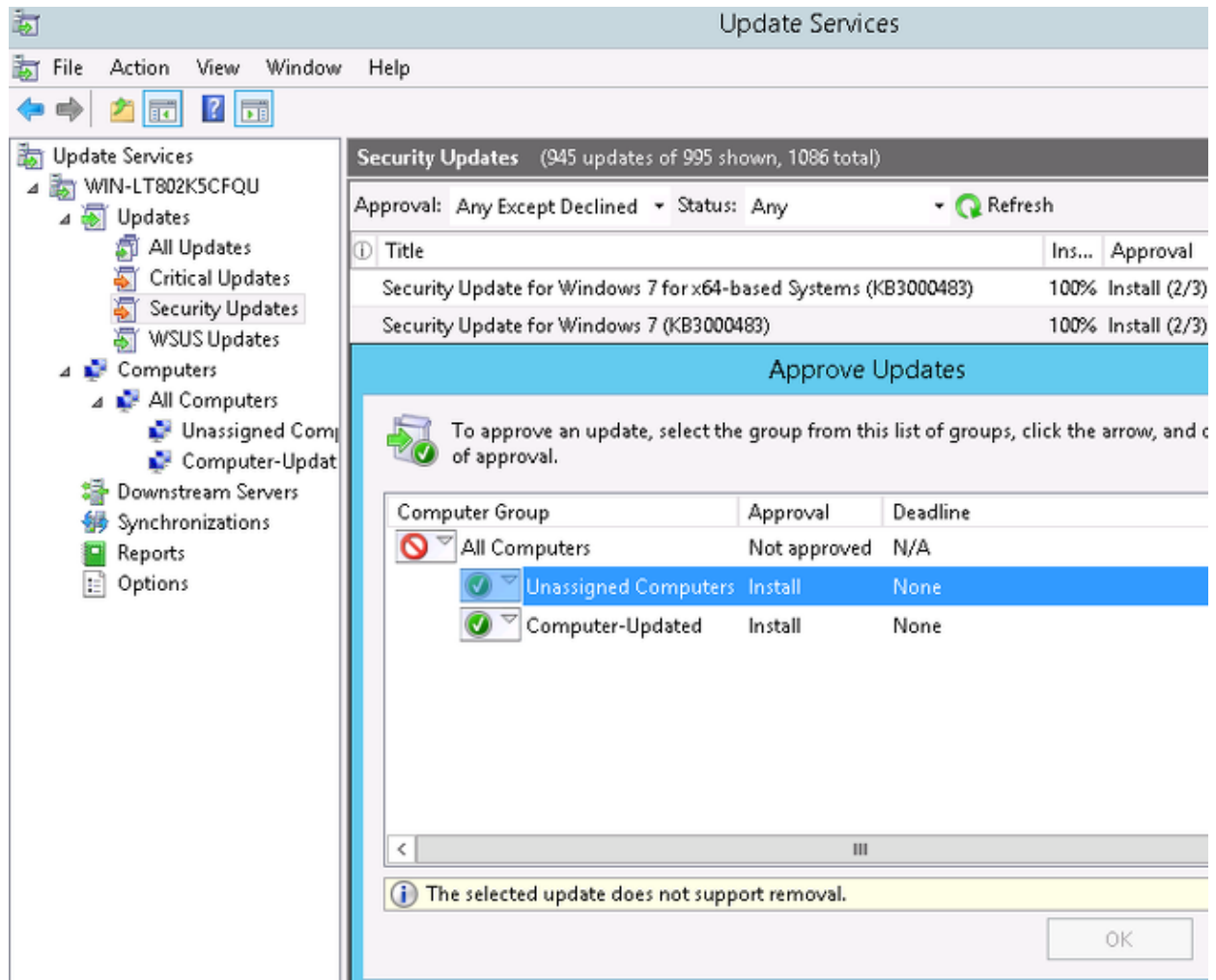
```
User Policy update has completed successfully.  
Computer Policy update has completed successfully.
```

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

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

Approve a Critical Update on the WSUS

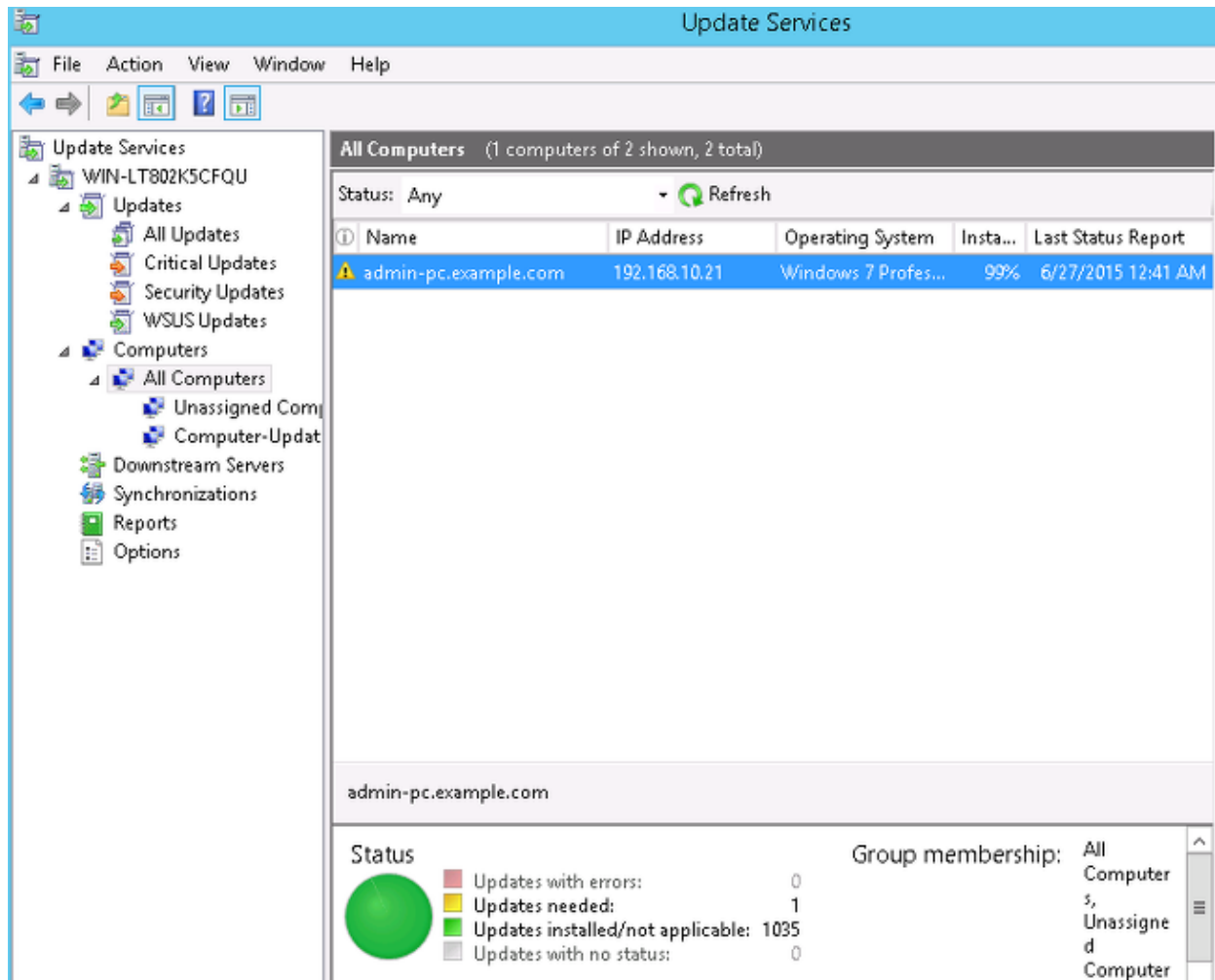
The approval process can benefit from client-site targeting:



Resend the report with *wuauctl* if needed.

Check the PC Status on the WSUS

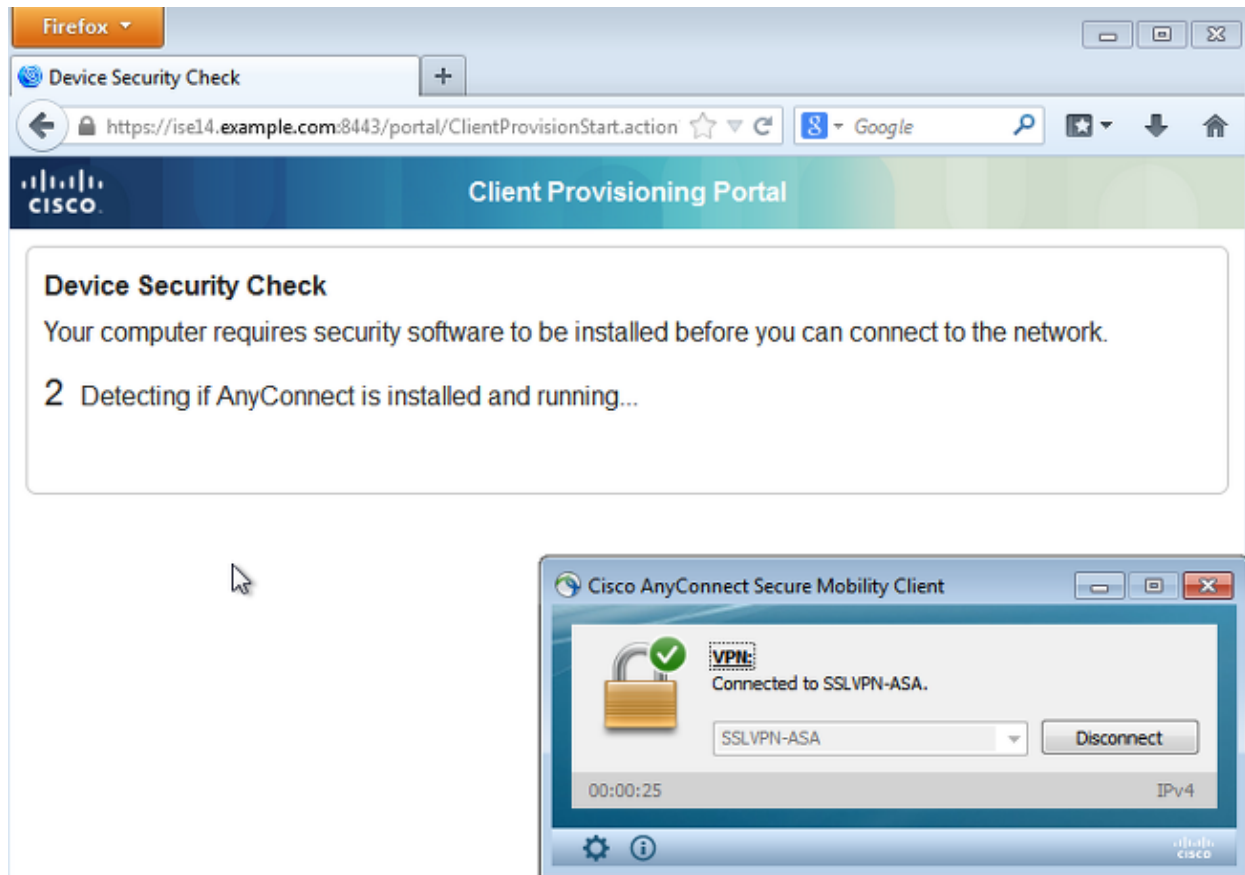
This image shows how to check the PC status on the WSUS:



One update should be installed for the next refresh with the WSUS.

VPN Session Established

After the VPN session is established, the *ASA-VPN_quarantine* ISE authorization rule is used, which returns the *Posture* authorization profile. As a result, the HTTP traffic from the endpoint is redirected for the AnyConnect 4 update and posture module provisioning:



At this point, the session status on the ASA indicates limited access with the redirection of the HTTP traffic to the 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
```

Posture Module Receives Policies from the ISE and Performs Remediation

The posture module receives the policies from the ISE. The `ise-psc.log` debugs show the requirement that is sent to the posture module:

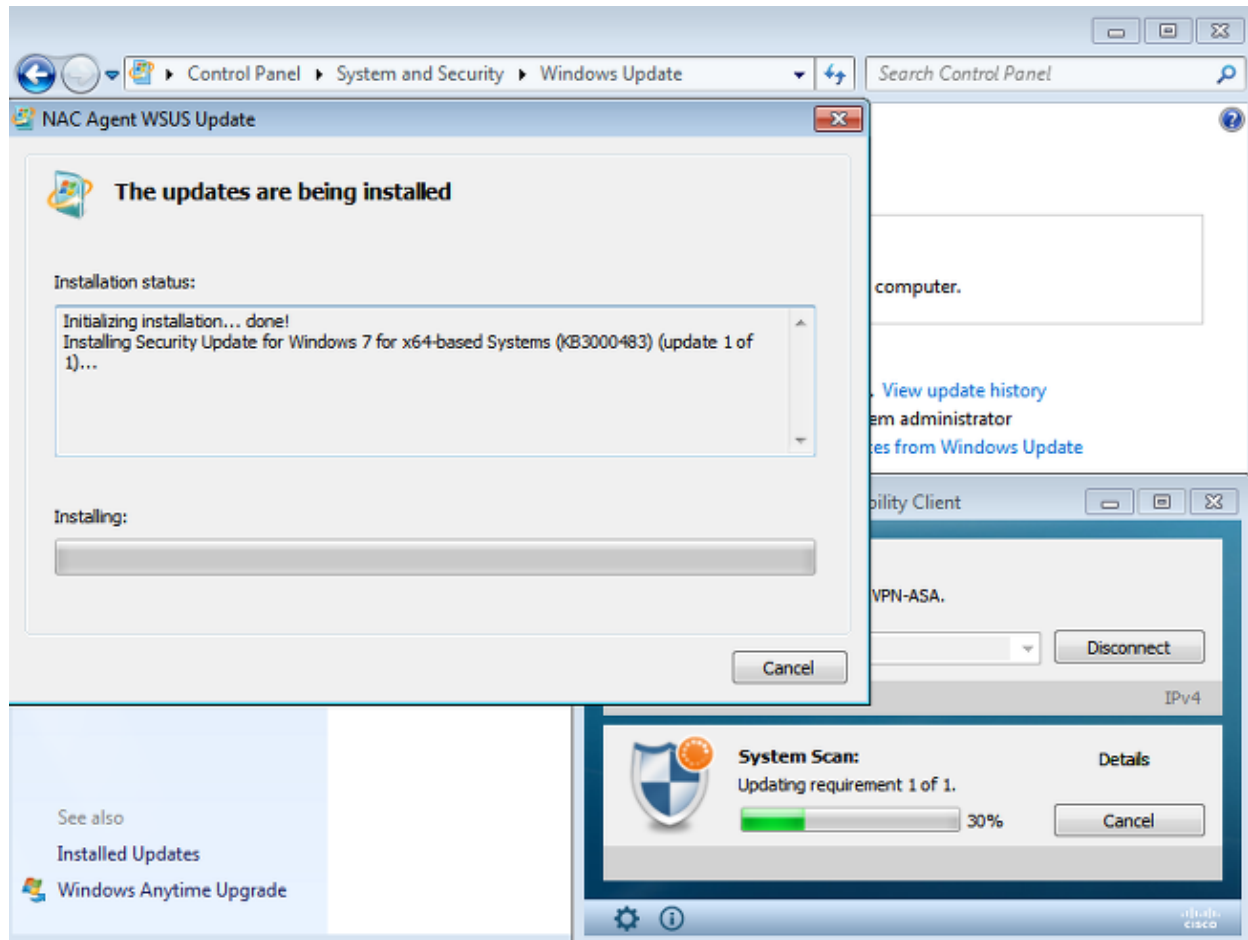
```
2015-06-05 07:33:40,493 DEBUG [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
  <version>2</version>
  <encryption>0</encryption>
  <package>
    <id>10</id>
    <name>WSUS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

```

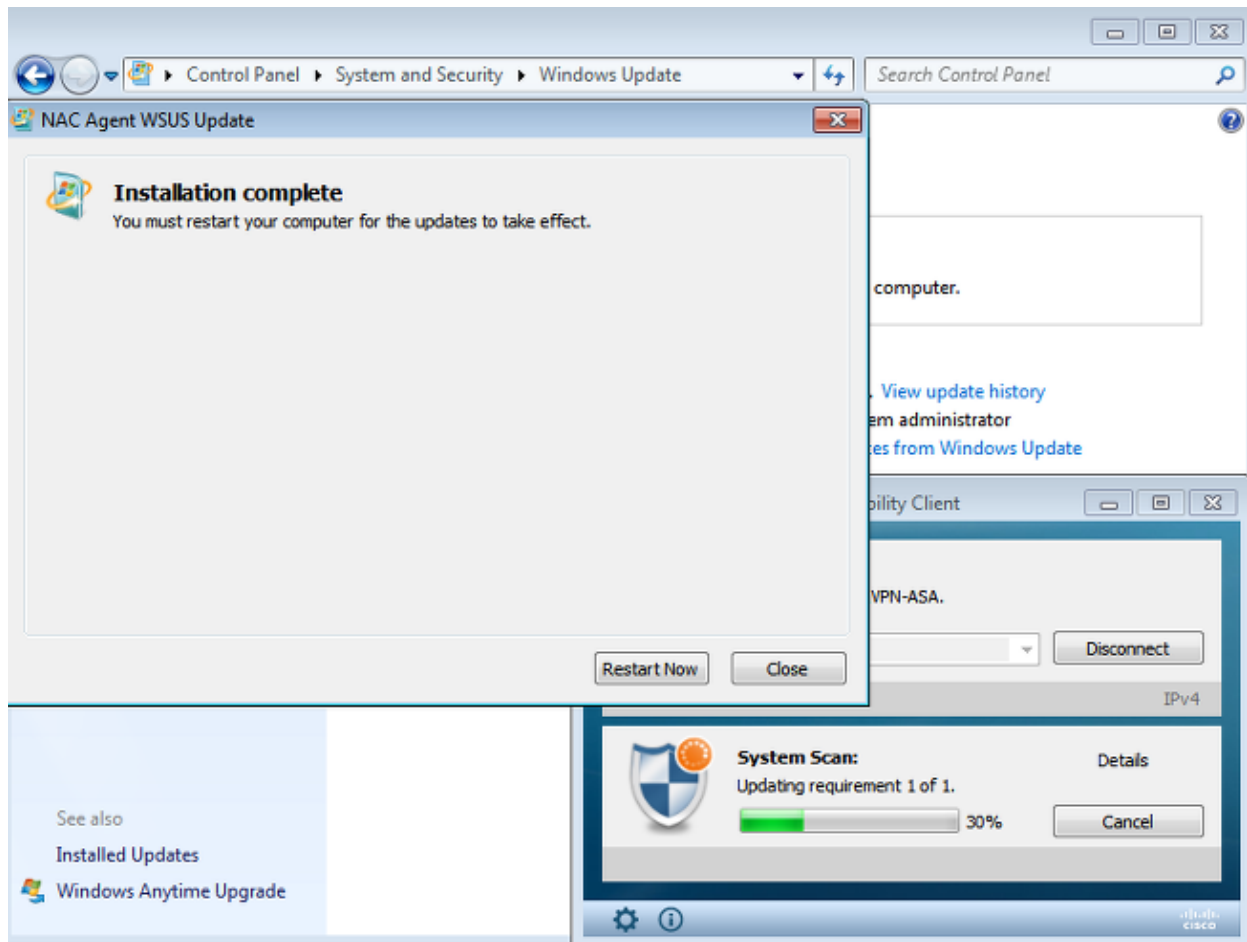
<description>This endpoint has failed check for any AS installation</description>
<type>10</type>
<optional>0</optional>
<path>42#1</path>
<remediation_type>1</remediation_type>
<remediation_retry>0</remediation_retry>
<remediation_delay>0</remediation_delay>
<action>10</action>
<check>
  <id>pr_WSUSCheck</id>
</check>
<criteria/>
</package>
</cleanmachines>

```

The posture module automatically triggers the Microsoft Windows Update Agent to connect to the WSUS and download updates as configured in the WSUS policies (all automatically without any user intervention):

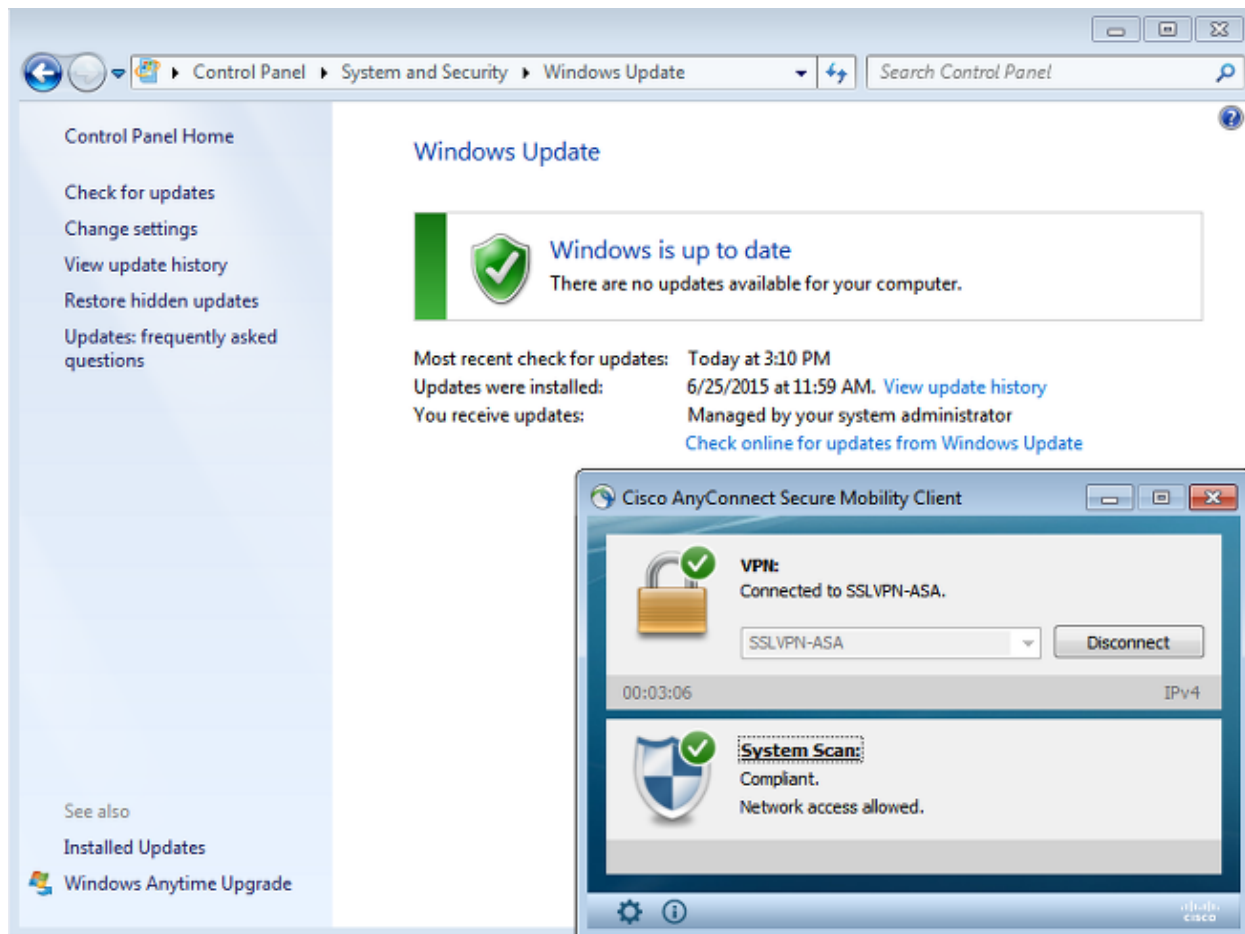


Note: Some of the updates might require a system restart.

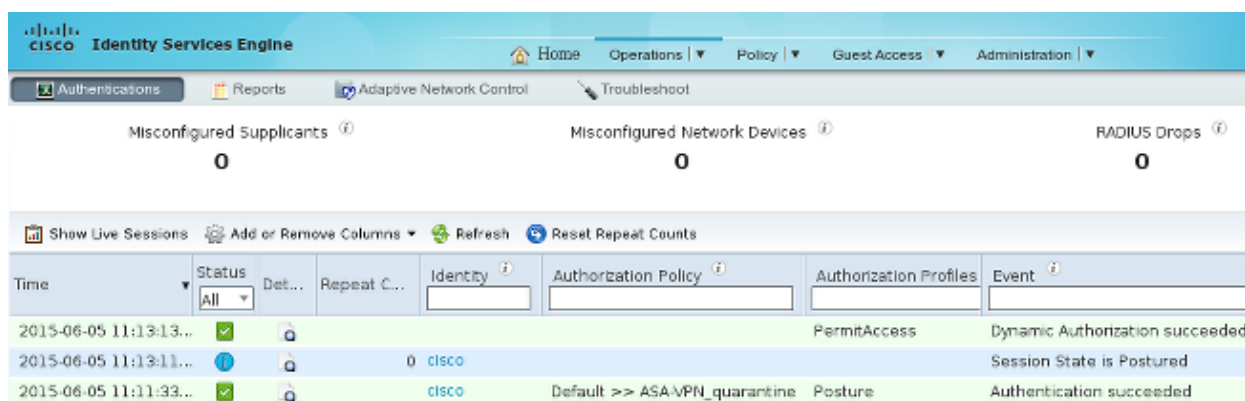


Full Network Access

You will see this after the station is reported as compliant by the AnyConnect posture module:



The report is sent to the ISE, which reevaluates the policy and hits the *ASA-VPN_compliant* authorization rule. This provides full network access (via the Radius CoA). Navigate to **Operations > Authentications** in order to confirm this:



The debugs (*ise-psc.log*) also confirm the compliance status, the CoA trigger, and the final settings for the posture:

```
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]

```

Also, the ISE Detailed Posture Assessment report confirms that the station is compliant:

Posture More Detail Assessment

| Time Range: From 05/30/2015 12:00:00 AM to 06/05/2015 11:59:59 PM | | | | | |
|---|---|-------------|-------|--------|----------------------------|
| Generated At: 2015-06-05 20:09:00.047 | | | | | |
| Client Details | | | | | |
| Username: | cisco | | | | |
| Mac Address: | 08:00:27:DA:EF:AD | | | | |
| IP address: | 172.16.50.50 | | | | |
| Session ID: | ac101f6400036000556b3f52 | | | | |
| Client Operating System: | Windows 7 Professional 64-bit | | | | |
| Client NAC Agent: | AnyConnect Posture Agent for Windows 4.1.02011 | | | | |
| PRA Enforcement: | 0 | | | | |
| CoA: | Received a posture report from an endpoint | | | | |
| PRA Grace Time: | 0 | | | | |
| PRA Interval: | 0 | | | | |
| PRA Action: | N/A | | | | |
| User Agreement Status: | NotEnabled | | | | |
| System Name: | ADMIN-PC | | | | |
| System Domain: | example.com | | | | |
| System User: | Administrator | | | | |
| User Domain: | EXAMPLE | | | | |
| AV Installed: | ClamWin Free Antivirus;0.98.5;55.20615;06/26/2015; | | | | |
| AS Installed: | Windows Defender;6.1.7600.16385;1.201.171.0;06/26/2015; | | | | |
| Posture Report | | | | | |
| Posture Status: | Compliant | | | | |
| Logged At: | 2015-06-05 07:28:49.194 | | | | |
| Posture Policy Details | | | | | |
| Policy | Name | Enforcement | Statu | Passed | Failed Conditions |
| WSUS | WSUS | Mandatory | | | Missing windows updates: 0 |

Note: The exact Media Access Control (MAC) address of the physical network interface on the Microsoft Windows PC is known because of the ACIDEX extensions.

Troubleshoot

There is currently no troubleshooting information available for this configuration.

Important Notes

This section provides some important information about the configuration that is described in this document.

Option Details for WSUS Remediation

It is important to differentiate the requirement condition from remediation. AnyConnect triggers the Microsoft Windows Update Agent to check the compliance, dependent upon the *Validate Windows updates using* remediation setting.

Windows Server Update Services Remediation

The screenshot shows a configuration form for 'Windows Server Update Services Remediation'. The fields and their values are as follows:

- * Name: WSUS-Remediation (with an information icon)
- Description: (empty text box)
- Remediation Type: Automatic (dropdown menu)
- Interval: 0 (text box, with note '(in secs) (Valid Range 0 to 9999)')
- Retry Count: 0 (text box, with note '(Valid Range 0 to 99)')
- Validate Windows updates using: Cisco Rules, Severity Level
- Windows Updates Severity Level: Medium (dropdown menu)
- Update to latest OS Service Pack
- Windows Updates Installation Source: Microsoft Server, Managed Server
- Installation Wizard Interface Setting: Show UI, No UI

For this example, the *Severity Level* is used. With the *Critical* setting, the Microsoft Windows Agent checks whether there are any pending (not installed) critical updates. If there are, then remediation begins.

The remediation process might then install all of the critical and less important updates based on the WSUS configuration (updates approved for the specific machine).

With the *Validate Windows updates using* set as **Cisco Rules**, the conditions that are detailed in the requirement decide whether the station is compliant.

Windows Update Service

For deployments without a WSUS server, there is another remediation type that can be used called *Windows Update Remediation*:

Windows Update Remediation

| | | |
|---|---|-----------------------------------|
| * Name | <input type="text" value="WindowsUpdate"/> | ? |
| 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"/> | |

This remediation type allows control over the Microsoft Windows Update settings and enables you to perform immediate updates. A typical condition that is used with this remediation type is *pc_AutoUpdateCheck*. This allows you to check whether the Microsoft Windows Update setting is enabled on the endpoint. If not, you can enable it and perform the update.

SCCM Integration

A new feature for the ISE Version 1.4 called *patch management* allows for integration with many third-party vendors. Dependent upon the vendor, multiple options are available for both the conditions and remediations.

For Microsoft, both the System Management Server (SMS) and the System Center Configuration Manager (SCCM) are supported.

Related Information

- [Posture Services on the Cisco ISE Configuration Guide](#)
- [Cisco Identity Services Engine Administrator Guide, Release 1.4](#)
- [Cisco Identity Services Engine Administrator Guide, Release 1.3](#)
- [Deploy Windows Server Update Services in Your Organization](#)
- [Technical Support & Documentation - Cisco Systems](#)