

# Configurez la posture de version 1.4 ISE avec Microsoft WSUS

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Microsoft WSUS](#)

[ASA](#)

[ISE](#)

[Correction de posture pour WSUS](#)

[Condition requise de posture pour WSUS](#)

[Profil d'AnyConnect](#)

[Règles de ravitaillement de client](#)

[Profils d'autorisation](#)

[Règles d'autorisation](#)

[Vérifiez](#)

[PC avec des stratégies mises à jour GPO](#)

[Approuvez une mise à jour essentielle sur le WSUS](#)

[Vérifiez l'état PC sur le WSUS](#)

[Session VPN établie](#)

[Le module de posture reçoit des stratégies de l'ISE et exécute la correction](#)

[Plein accès au réseau](#)

[Dépannez](#)

[Remarques importantes](#)

[Détails d'option pour la correction WSUS](#)

[Service de Windows Update](#)

[Intégration SCCM](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer la fonctionnalité de posture du Logiciel Cisco Identity Services Engine (ISE) quand il est intégré avec les services de mise à jour de Microsoft Windows Server (WSUS).

**Note:** Quand vous accédez au réseau, vous êtes réorienté à l'ISE pour l'approvisionnement de version 4.1 de Client à mobilité sécurisé Cisco AnyConnect avec un module de posture, qui vérifie l'état de conformité sur le WSUS et installe les mises à jour nécessaires afin de la station soit conforme. Une fois que la station est signalée comme conforme, l'ISE tient compte du plein accès au réseau.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiements, authentification, et autorisation de Cisco ISE
- Connaissance de base au sujet de la manière dans laquelle les ISE et l'agent intermédiaire de Cisco AnyConnect fonctionnent
- Configuration de l'appliance de sécurité adaptable Cisco (ASA)
- La connaissance de base VPN et de 802.1x
- Configuration de Microsoft WSUS

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 7 de Microsoft Windows
- Version 2012 de Microsoft Windows avec la version 6.3 WSUS
- Versions 9.3.1 et ultérieures de Cisco ASA
- Versions de logiciel 1.3 de Cisco ISE et plus tard

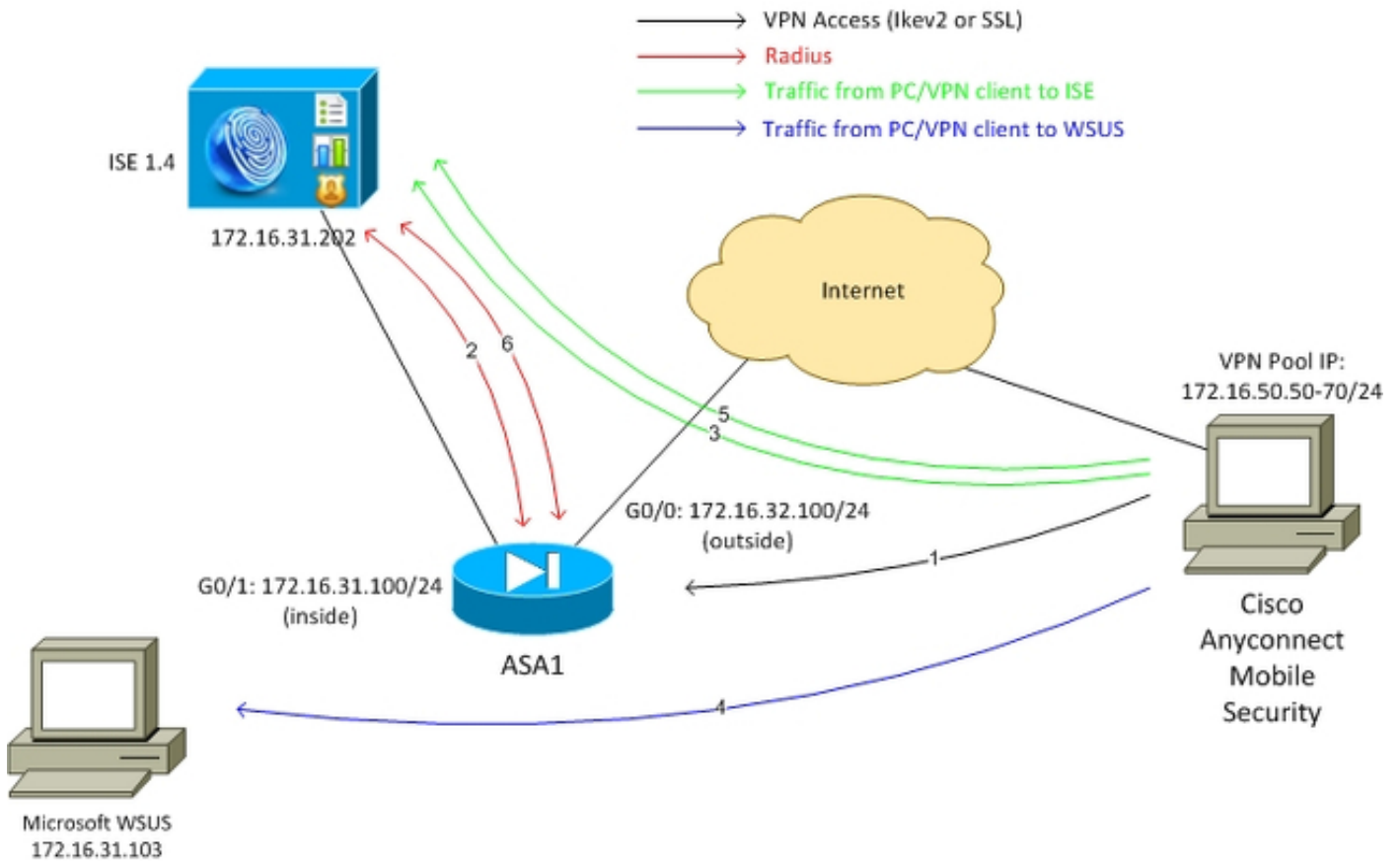
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Configurez

Cette section décrit comment configurer l'ISE et les éléments de réseau relatifs.

## Diagramme du réseau

C'est la topologie qui est utilisée pour les exemples dans tout ce document :



Voici la circulation, comme illustré dans le schéma de réseau :

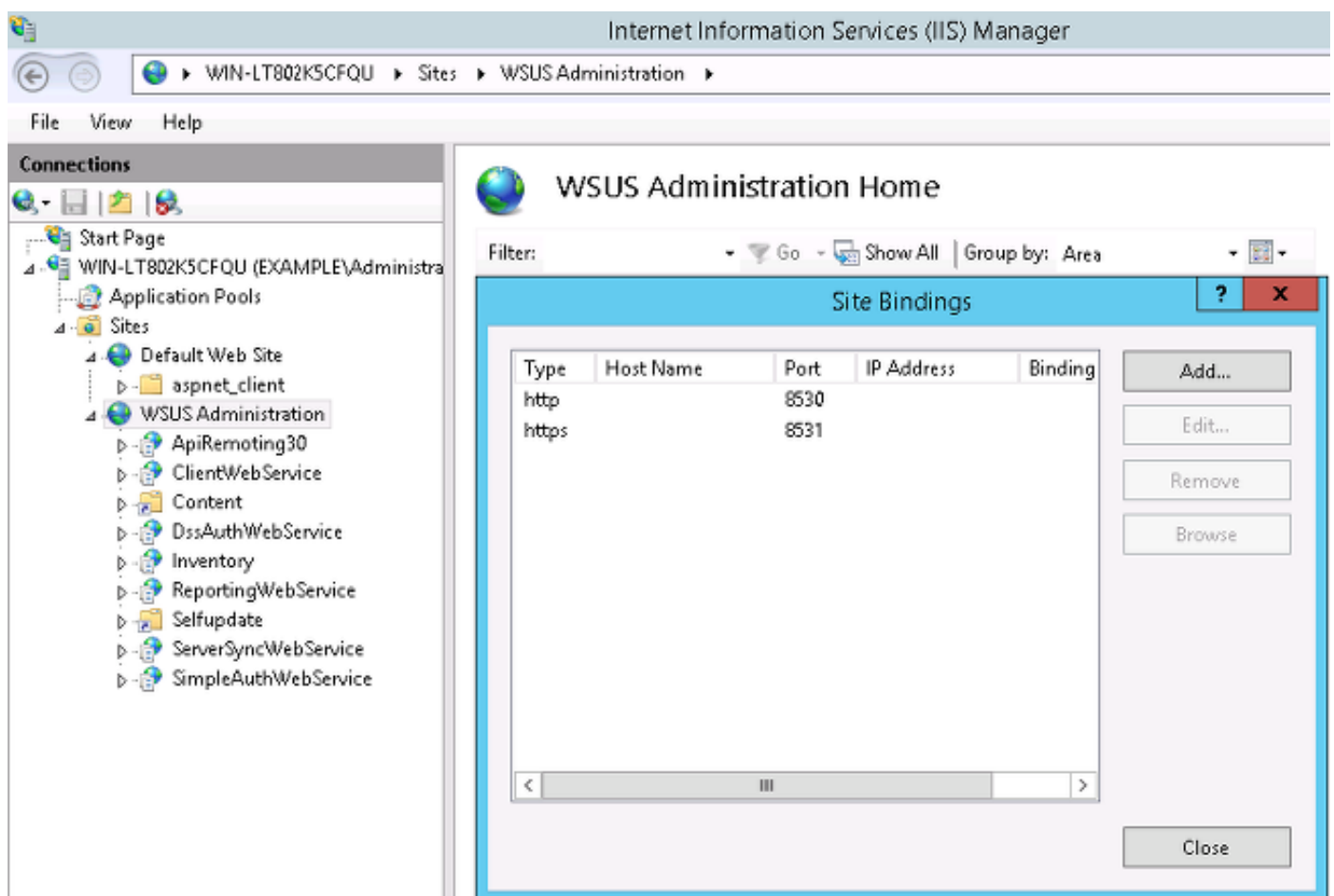
1. L'utilisateur distant se connecte par le Cisco AnyConnect pour l'accès VPN à l'ASA. Ceci peut être n'importe quel type d'accès unifié, tel qu'une session de câblage de contournement de l'authentification 802.1x/MAC (MAB) qui est terminée sur le commutateur ou une session Sans fil qui est terminée sur le contrôleur LAN Sans fil (WLC).
2. Comme partie de la procédure d'authentification, l'ISE confirme que le statut de posture de la station d'extrémité n'est pas égal à conforme (règle d'autorisation d'ASA-VPN\_quarantine) et que les attributs de redirection sont retournés dans *Radius Access-recevez le message*. En conséquence, l'ASA réoriente tout le trafic http à l'ISE.
3. L'utilisateur ouvre un navigateur Web et introduit n'importe quelle adresse. Après la redirection à l'ISE, le module de posture du Cisco AnyConnect 4 est installé sur la station. Le module de posture télécharge alors les stratégies de l'ISE (condition requise pour WSUS).
4. Le module de posture recherche Microsoft WSUS, et exécute la correction.
5. Après la correction réussie, le module de posture envoie un état à l'ISE.
6. L'ISE émet une modification de Radius de l'autorisation (CoA) qui fournit le plein accès au réseau à un utilisateur conforme VPN (règle d'autorisation d'ASA-VPN\_compliant).

**Note:** Pour que la correction fonctionne (la capacité d'installer des mises à jour de Microsoft Windows sur un PC), l'utilisateur devrait avoir des droits d'administration locales.

## Microsoft WSUS

**Note:** Une configuration détaillée du WSUS est hors de portée de ce document. Pour des détails, référez-vous aux [services de mise à jour de Windows Server de déployer dans votre documentation Microsoft d'organisation](#).

Le service WSUS est déployé par le port TCP standard 8530. Il est important de se souvenir cela pour la correction, d'autres ports sont également utilisés. C'est pourquoi il est sûr d'ajouter l'adresse IP de WSUS à la liste de contrôle d'accès de redirection (ACL) sur l'ASA (décrite plus tard dans ce document).

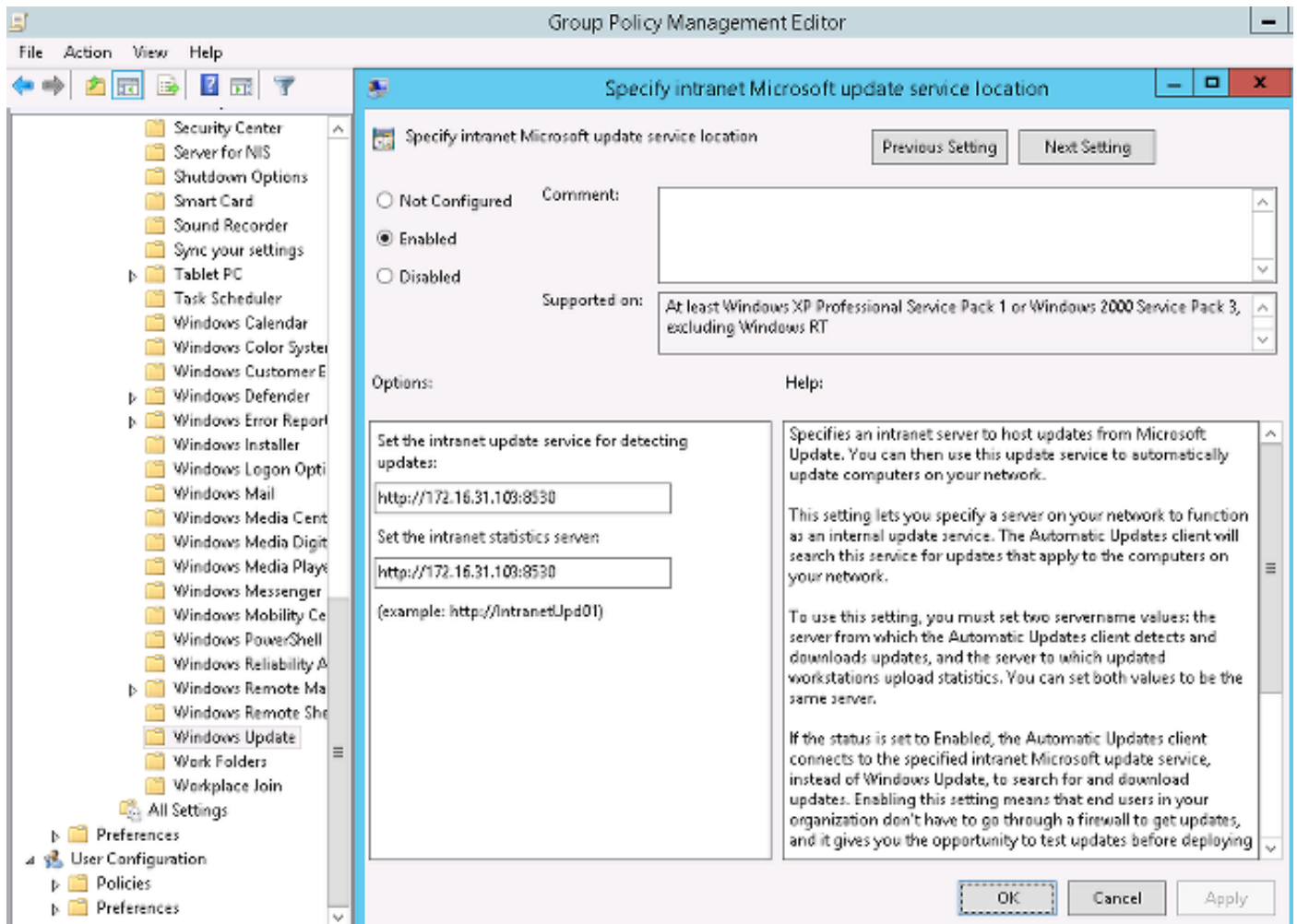


The screenshot shows the Internet Information Services (IIS) Manager interface. The main window displays the 'WSUS Administration Home' page. A 'Site Bindings' dialog box is open, showing a table with the following data:

Type	Host Name	Port	IP Address	Binding
http		8530		
https		8531		

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

La stratégie de groupe pour le domaine est configurée pour des mises à jour et des points de Microsoft Windows au serveur des gens du pays WSUS :



Ce sont les mises à jour recommandées qui sont activées pour les stratégies granulaires qui sont basées sur des différents niveaux de sévérité :

### 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

L'optimisation de côté client tient compte de la meilleure flexibilité lointaine. L'ISE peut utiliser les stratégies de posture qui sont basées sur les différents conteneurs d'ordinateur de Microsoft Active Directory (AD). Le WSUS peut approuver les mises à jour qui sont basées sur cette adhésion.

## ASA

L'accès VPN simple de Secure Sockets Layer (SSL) pour l'utilisateur distant est utilisé (les détails dont soyez hors de portée de ce document).

Voici un exemple de 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
```

Il est important de configurer une liste d'accès sur l'ASA, qui est utilisée afin de déterminer le trafic qui devrait être réorienté à l'ISE (pour les utilisateurs qui ne sont pas encore conformes) :

```
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
```

On permet seulement le Système de noms de domaine (DNS), l'ISE, le WSUS, et le trafic de Protocole ICMP (Internet Control Message Protocol) pour les utilisateurs non-conformes. Tout les autre le trafic (HTTP) est réorienté à l'ISE pour le ravitaillement d'AnyConnect 4, qui est responsable de la posture et de la correction.

## ISE

**Note:** Le ravitaillement et la posture d'AnyConnect 4 est hors de portée de ce document. Référez-vous à l'[intégration d'AnyConnect 4.0 avec l'exemple de configuration de version 1.3 ISE](#) pour plus de détails, tels que la façon configurer l'ASA comme périphérique de réseau et installer l'application du Cisco AnyConnect 7.

### Correction de posture pour WSUS

Terminez-vous ces étapes afin de configurer la correction de posture pour WSUS :

1. Naviguez vers la **stratégie > les conditions > les actions de posture > de correction > la correction de services de mise à jour de Windows Server** afin de créer une nouvelle règle.
2. Vérifiez que l'établissement de *mises à jour de Microsoft Windows* est placé au **niveau d'importance**. La présente partie est responsable de la détection si le procédé de correction est initié.

L'agent de mise à jour de Microsoft Windows alors se connecte au WSUS et vérifie s'il y a des mises à jour *essentielles* pour ce PC qui attendent l'installation :

The screenshot shows the Cisco ISE configuration interface. The top navigation bar includes tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy. Below this, there are sub-tabs for Dictionaries, Conditions, and Results. The main content area is titled "Windows Server Update Services Remediations List > WSUS-Remediation". The configuration form for "Windows Server Update Services Remediation" 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

Buttons for "Save" and "Reset" are visible at the bottom of the configuration form. On the left side, a "Results" pane shows a tree view of configuration objects, with "Windows Server Update Services Remediation" selected under "Remediation Actions".

### Condition requise de posture pour WSUS

Naviguez vers la **stratégie > les conditions > la posture > les conditions requises** afin de créer une nouvelle règle. La règle utilise une condition factice appelée le *pr\_WSUSRule*, ainsi il signifie que le WSUS est entré en contact afin de vérifier la condition quand la correction est nécessaire (les mises à jour *essentielles*).

Une fois que cette condition est remplie, le WSUS installe les mises à jour qui ont été configurées pour ce PC. Ceux-ci peuvent inclure n'importe quel type de mises à jour, et également ceux avec des niveaux d'importance plus bas :

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

## Profil d'AnyConnect

Configurez le profil de module de posture, avec le profil d'AnyConnect 4 (comme décrit dans [l'intégration d'AnyConnect 4.0 avec l'exemple de configuration de version 1.3 ISE](#)) :



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 area)
- \* Compliance Module: AnyConnectComplianceModuleWindows 3.6.9

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

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

The 'Profile Selection' section contains:

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

## Règles de ravitaillement de client

Une fois que le profil d'AnyConnect est prêt, il peut être mis en référence de la stratégie de *ravitaillement de client* :

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

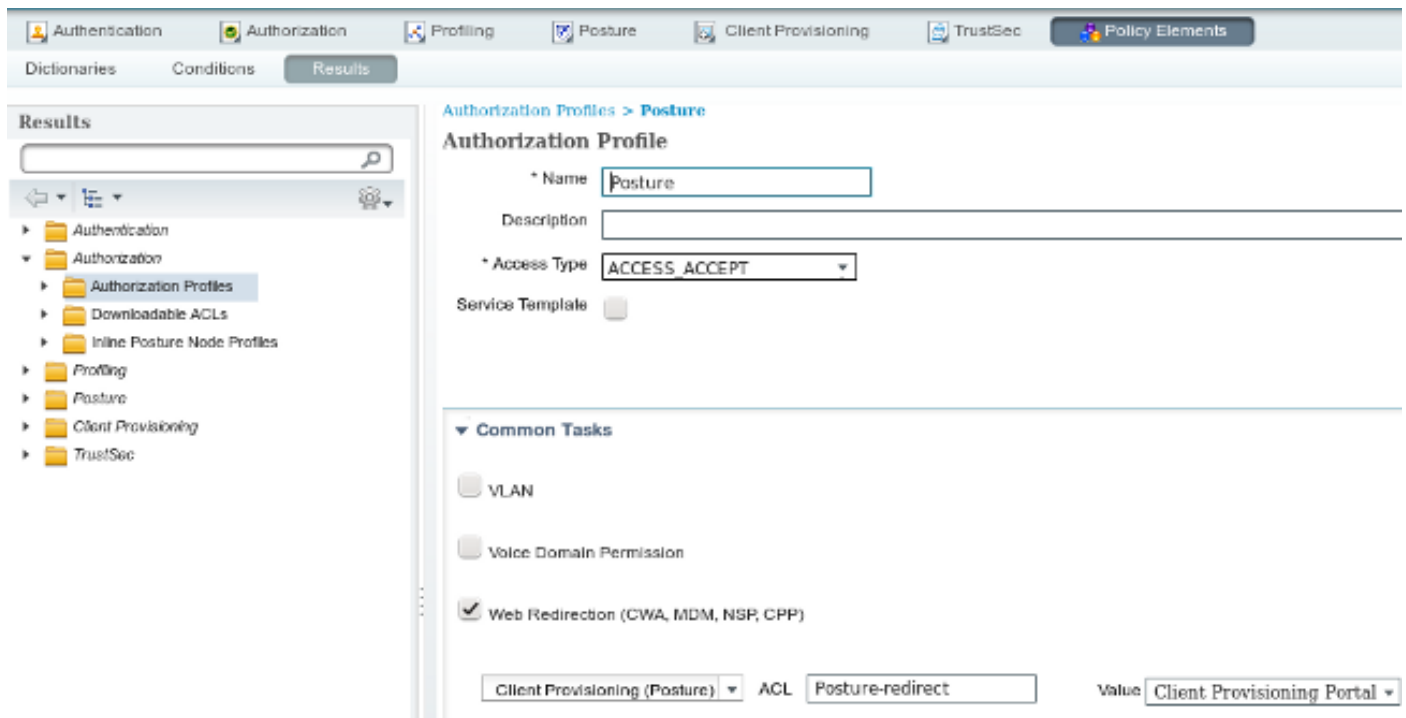
The main content area displays a table of rules:

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

L'application entière, avec la configuration, est installée sur le point final, qui est réorienté à la page du portail de ravitaillement de client. AnyConnect 4 pourrait être mis à jour et un module supplémentaire (posture) être installé.

## Profils d'autorisation

Créez un profil d'autorisation pour la redirection au profil de ravitaillement de client :



## Règles d'autorisation

Cette image affiche les règles d'autorisation :

### 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

Pour la première fois, la règle d'*ASA-VPN\_quarantine* est utilisée. En conséquence, le profil d'autorisation de *posture* est retourné, et le point final est réorienté au portail de ravitaillement de client pour le ravitaillement d'AnyConnect 4 (avec le module de posture).

Une fois que conforme, la règle d'*ASA-VPN\_compliant* est utilisée et le plein accès au réseau est permis.

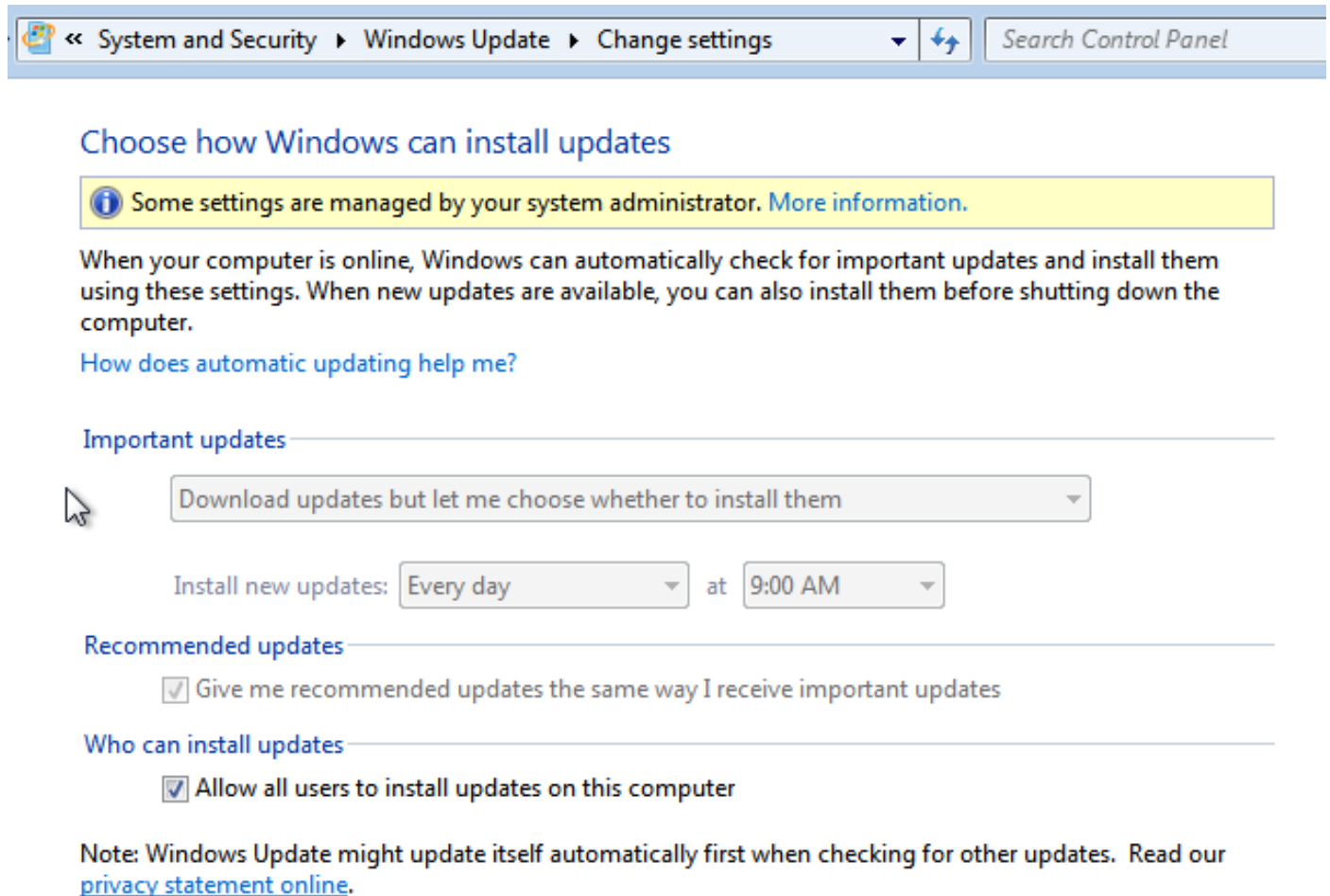
## Vérifiez

Cette section fournit les informations que vous pouvez employer afin de vérifier que vous configuration travaille correctement.

## PC avec des stratégies mises à jour GPO

Les stratégies de domaine avec la configuration WSUS devraient être poussées après que le PC se connecte dans le domaine. Ceci peut se produire avant que la session VPN soit établie (hors de la bande) ou ensuite si la fonctionnalité de *Start Before Logon* est utilisée (elle peut être également utilisée pour accès de câble/Sans fil de 802.1x).

Une fois que le client de Microsoft Windows a la configuration correcte, ceci peut être reflété des configurations de Windows Update :



The screenshot shows the Windows Update settings page in the Control Panel. The breadcrumb trail 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, a yellow information box states: '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, the setting is 'Download updates but let me choose whether to install them'. The 'Install new updates' section is set to 'Every day' at '9:00 AM'. Under the 'Recommended updates' section, the checkbox 'Give me recommended updates the same way I receive important updates' is checked. Under the 'Who can install updates' section, the checkbox 'Allow all users to install updates on this computer' is checked. A note at the bottom states: 'Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.'

Si nécessaire, un objet de stratégie de groupe (GPO) régénèrent et serveur d'agent de mise à jour de Microsoft Windows que la détection peut être utilisée :

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

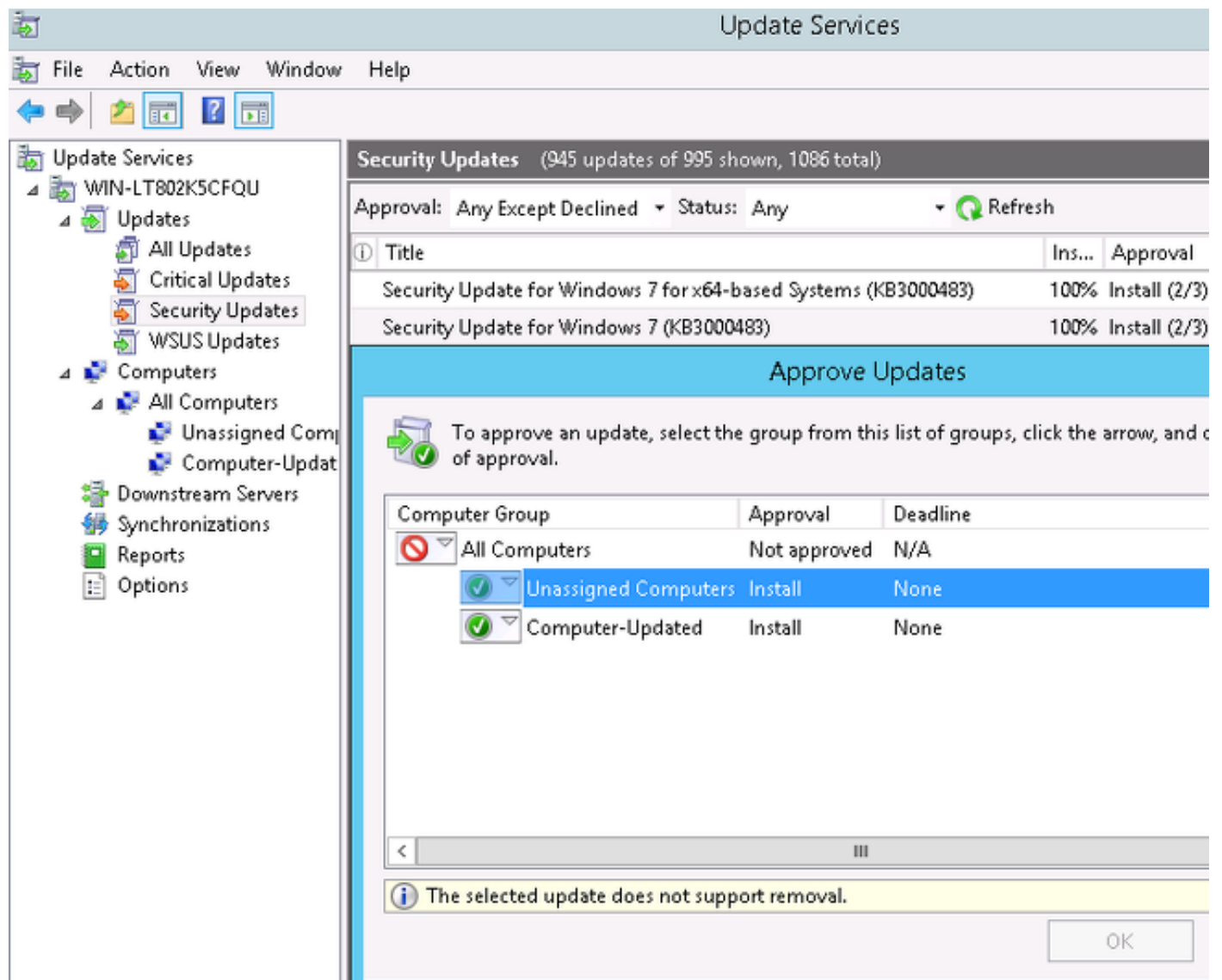
```
User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

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

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

## Approuvez une mise à jour essentielle sur le WSUS

Le processus d'approbation peut tirer bénéfice de l'optimisation de site client :



The screenshot shows the WSUS console interface. On the left, a tree view shows the hierarchy: Update Services > WIN-LT802K5CFQU > Updates > Security Updates. The main pane displays a list of security updates. Below this, the 'Approve Updates' dialog box is open. It contains a table with the following data:

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

At the bottom of the dialog, there is a message: "The selected update does not support removal." and an "OK" button.

Renvoyez l'état avec le *wuauctl* si nécessaire.

## Vérifiez l'état PC sur le WSUS

Cette image affiche comment vérifier l'état PC sur le WSUS :

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

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

Below the table, the status for 'admin-pc.example.com' is shown as a green circle. The status bar at the bottom indicates:

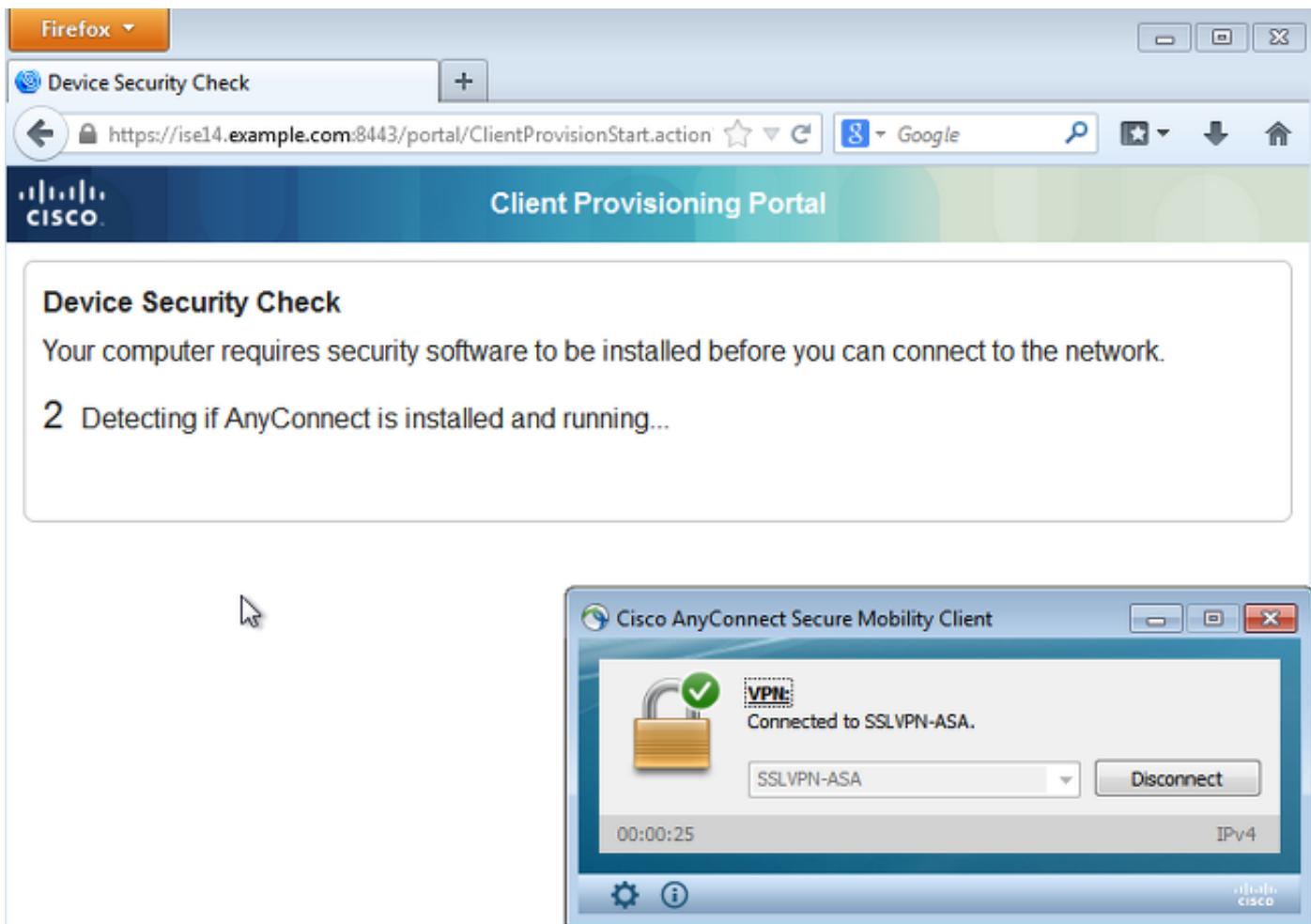
- Updates with errors: 0
- Updates needed: 1
- Updates installed/not applicable: 1035
- Updates with no status: 0

Group membership: All Computer, s, Unassigne d, Computer

Une mise à jour devrait être installée pour le prochain régénèrent avec le WSUS.

## Session VPN établie

Après que la session VPN soit établie, la règle d'autorisation d'*ASA-VPN\_quarantine* ISE est utilisée, qui renvoie le profil d'autorisation de *posture*. En conséquence, le trafic http du point final est réorienté pour les 4 ravitaillements de module de mise à jour et de posture d'AnyConnect :



En ce moment, l'état de session sur l'ASA indique l'accès limité avec la redirection du trafic http à l'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
```

## Le module de posture reçoit des stratégies de l'ISE et exécute la correction

Le module de posture reçoit les stratégies de l'ISE. `ise-psc.log` met au point l'exposition la condition qui soit envoyé au module de posture :

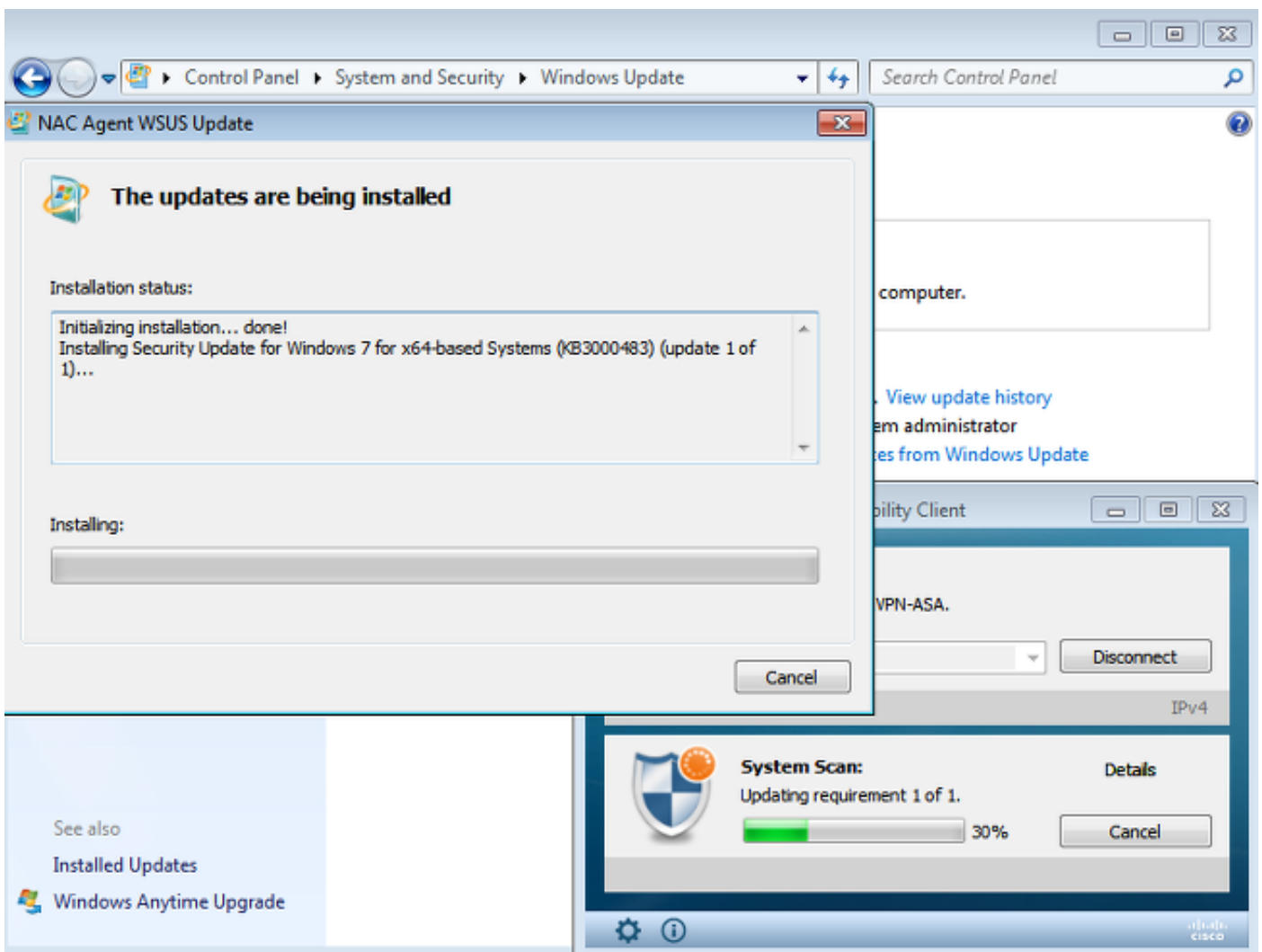
```
2015-06-05 07:33:40,493 DEBUG [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
<version>2</version>
<encryption>0</encryption>
```

```

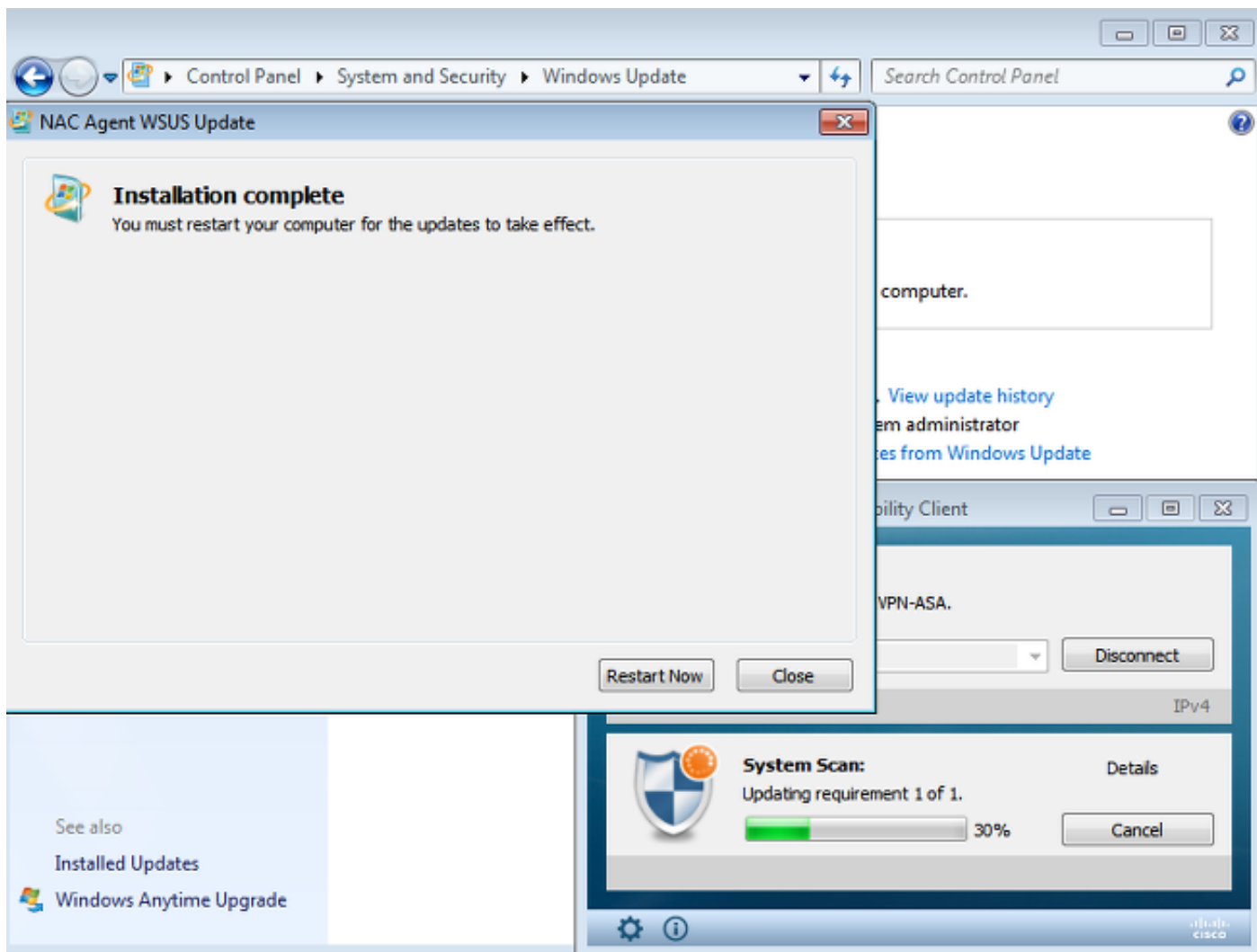
<package>
  <id>10</id>
  <name>WSUS</name>
  <version/>
  <description>This endpoint has failed check for any AS installation</description>
  <type>10</type>
  <optional>0</optional>
  <path>42#1</path>
  <remediation_type>1</remediation_type>
  <remediation_retry>0</remediation_retry>
  <remediation_delay>0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

```

Le module de posture déclenche automatiquement l'agent de mise à jour de Microsoft Windows pour se connecter au WSUS et pour télécharger des mises à jour comme configurées dans les stratégies WSUS (toutes automatiquement sans toute intervention de l'utilisateur) :



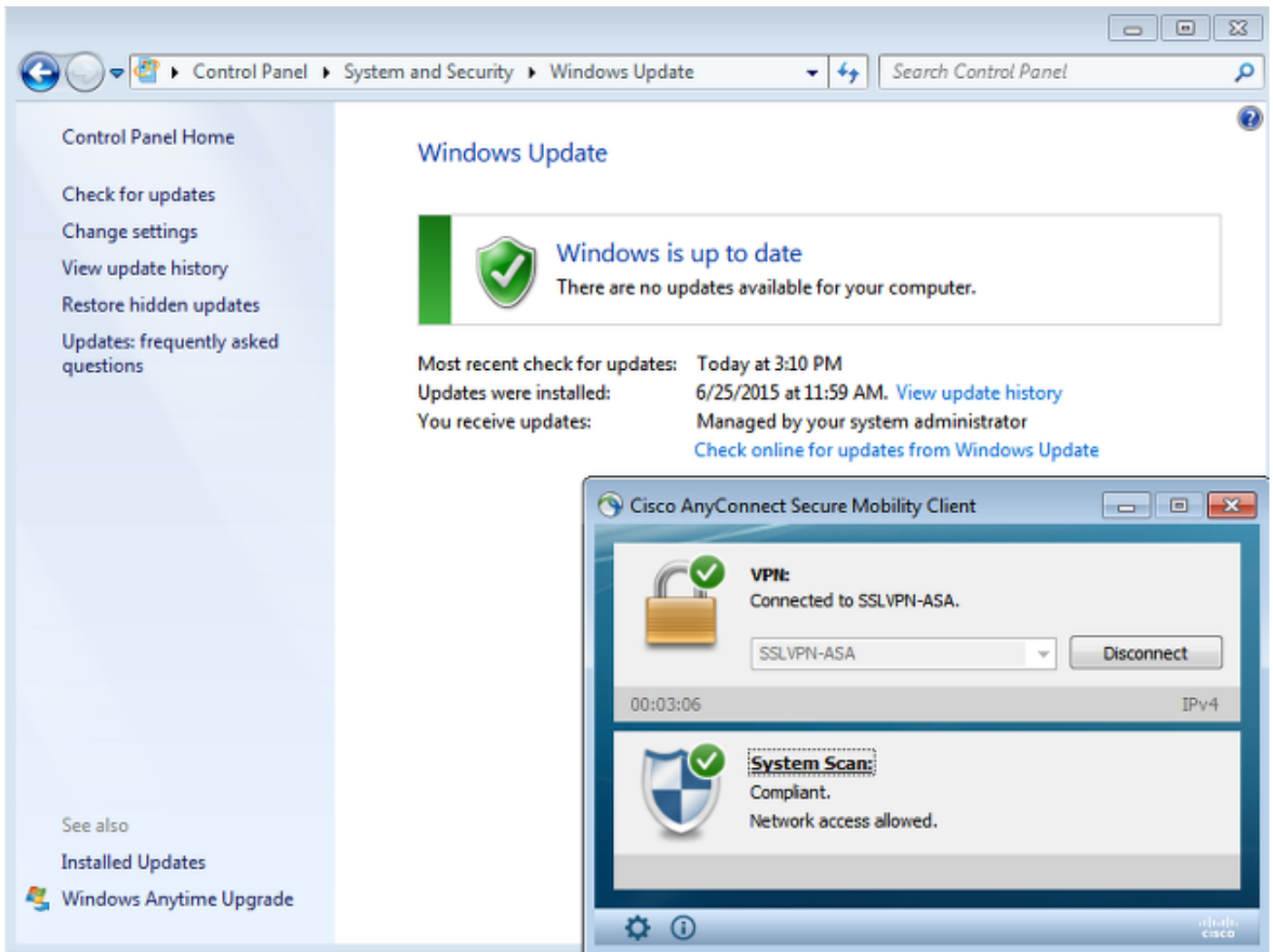
**Note:** Certaines des mises à jour pourraient exiger un redémarrage du système.



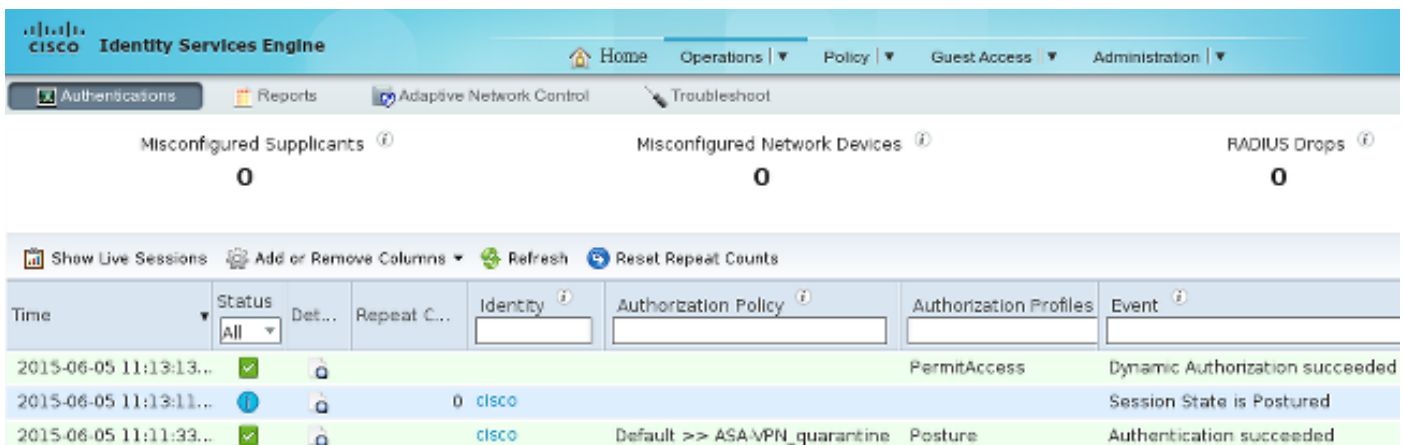
## Plein accès au réseau

Vous verrez ceci après que la station soit signalée comme conforme par le module de posture d'AnyConnect :





L'état est envoyé à l'ISE, qui réévalue la stratégie et frappe la règle d'autorisation d'ASA-VPN\_compliant. Ceci fournit le plein accès au réseau (par l'intermédiaire du CoA de Radius). Naviguez vers des **exécutions > des authentications** afin de confirmer ceci :



Met au point (**ise-psc.log**) confirment également l'état de conformité, le déclencheur CoA, et les configurations finales pour la 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]
```

En outre, le rapport d'évaluation de posture détaillé par ISE confirme que la station est 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

**Note:** L'adresse précise de Contrôle d'accès au support (MAC) de l'interface réseau physique sur le PC de Microsoft Windows est connue en raison des extensions d'ACIDEX.

## Dépannez

Il n'y a actuellement aucune information de dépannage disponible pour cette configuration.

## Remarques importantes

Cette section fournit quelques informations importantes au sujet de la configuration qui est décrite dans ce document.

## Détails d'option pour la correction WSUS

Il est important de différencier la condition de condition requise de la correction. AnyConnect déclenche l'agent de mise à jour de Microsoft Windows pour vérifier la conformité, dépendante sur les *mises à jour de Windows de validation utilisant la configuration de correction*.

### 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

Pour cet exemple, le *niveau d'importance* est utilisé. Avec la configuration *essentielle*, l'agent de Microsoft Windows vérifie s'il y a ( ) les mises à jour essentielles non installées en suspens. S'il y a, alors la correction commence.

Le procédé de correction pourrait alors installer tout les essentiel et moins de mises à jour importantes du routage basés sur la configuration WSUS (mises à jour approuvées pour l'ordinateur spécifique).

Avec *Windows de validation* les *mises à jour utilisant le positionnement* comme **Cisco ordonne**, les conditions qui sont détaillées dans la condition requise décident si la station est conforme.

## Service de Windows Update

Pour des déploiements sans serveur WSUS, il y a un autre type de correction qui peut être utilisé a appelé la *correction de 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

Ce type de correction permet le contrôle des configurations de mise à jour de Microsoft Windows et te permet d'exécuter les mises à jour immédiates. Un état typique qui est utilisé avec ce type de

correction est *pc\_AutoUpdateCheck*. Ceci te permet pour vérifier si la configuration de mise à jour de Microsoft Windows est activée sur le point final. Sinon, vous pouvez l'activer et exécuter la mise à jour.

## Intégration SCCM

Une nouvelle caractéristique pour la version 1.4 ISE appelée la *Gestion de correctif* tient compte de l'intégration avec beaucoup de tiers constructeurs. La personne à charge sur le constructeur, des nombreuses options sont disponible pour les conditions et des corrections.

Pour Microsoft, le serveur de gestion du système (SMS) et la Configuration Manager de System Center (SCCM) sont pris en charge.

## Informations connexes

- [Services de posture sur le guide de configuration de Cisco ISE](#)
- [Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 1.4](#)
- [Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 1.3](#)
- [Déployez les services de mise à jour de Windows Server dans votre organisation](#)
- [Support et documentation techniques - Cisco Systems](#)