Microsoft WSUS と ISE バージョン 1.4 ポスチャの設定

目次

はじめに
前提条件
要件
使用するコンポーネント
設定
ネットワーク図
Microsoft WSUS
ASA
ISE
WSUS のポスチャ修復
WSUS のポスチャ要件
AnyConnect プロファイル
クライアント プロビジョニング ルール
許可プロファイル（Authorization Profiles）
認可規則
確認
GPO ポリシーが更新された PC
WSUS での重要な更新プログラムの承認
WSUS での PC ステータスの確認
VPN セッションの確立
ポスチャ モジュールが ISE からポリシーを受信し修復を実行する
フル ネットワーク アクセス
トラブルシューティング
重要事項
WSUS 修復のオプションの詳細
Windows Update Service
SCCM 統合
関連情報

概要

このドキュメントでは、Cisco Identity Services Engine（ISE）ポスチャ機能が Microsoft Windows Server Update Services（WSUS）に統合されている場合に、このポスチャ機能を設定する方法を説明します。

注: ネットワークにアクセスすると、ポスチャ モジュールを使用した ISE for Cisco AnyConnect Secure Mobility Client Version 4.1 プロビジョニングにリダイレクトされます。これにより、WSUS の準拠ステータスが確認され、ステーションが準拠するために必要な更新プログラムがインストールされます。 ステーションが準拠しているものとして報告されたら、ISE によりフル ネットワーク アクセスが許可されます。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco ISE の導入、認証、認可
- ISE と Cisco AnyConnect ポスチャ エージェントの動作に関する基本的な知識
- Cisco 適応型セキュリティ アプライアンス（ASA）の設定
- 基本的な VPN および 802.1x の情報
- Microsoft WSUS の設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Microsoft Windows バージョン 7
- WSUS バージョン 6.3 を備えた Microsoft Windows バージョン 2012
- Cisco ASA バージョン 9.3.1 以降
- Cisco ISE ソフトウェア バージョン 1.3 以降

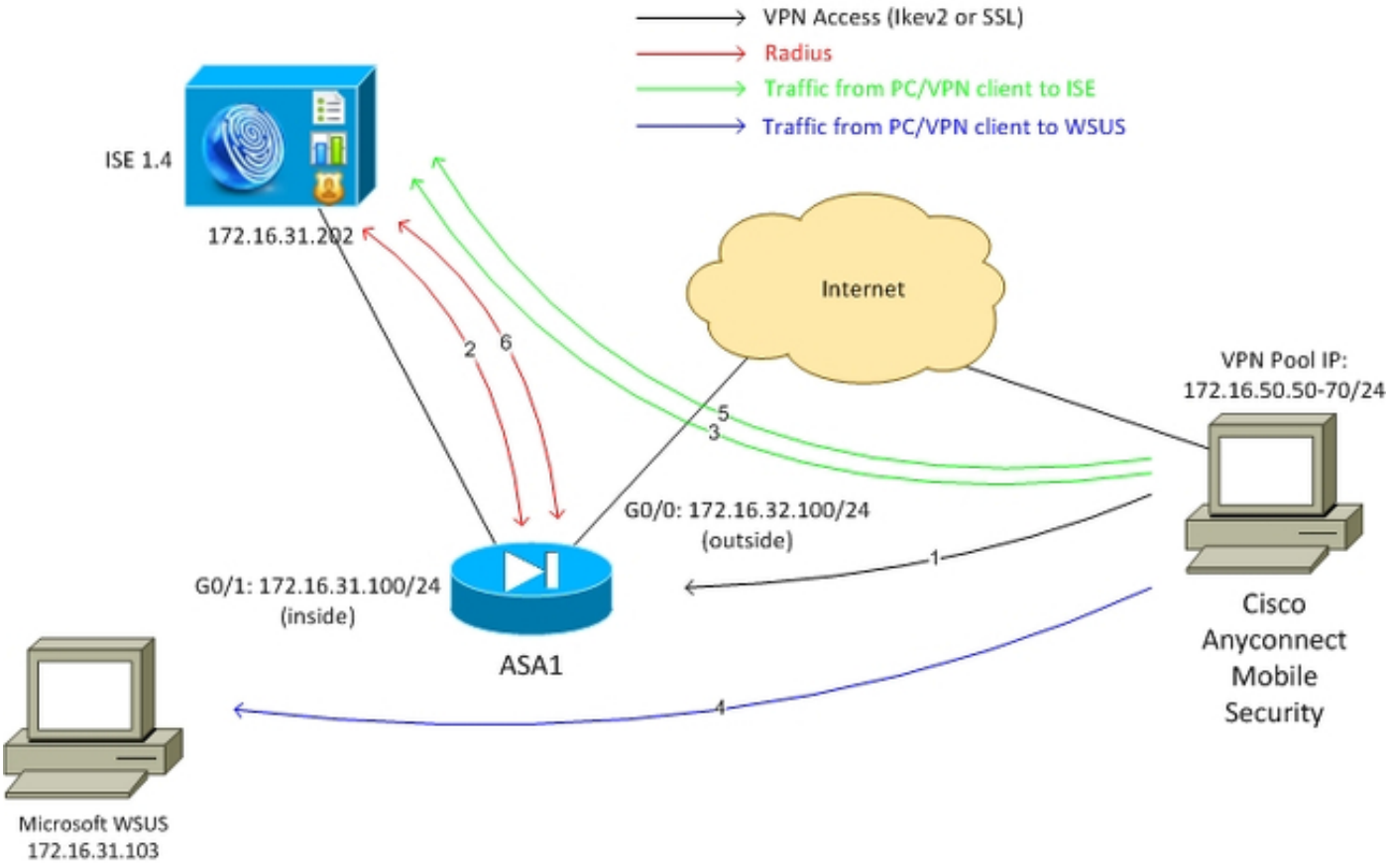
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

ここでは、ISE と関連ネットワーク要素を設定する方法について説明します。

ネットワーク図

このドキュメントの例で使用するトポロジを次に示します。



次のネットワーク ダイアグラムにトラフィック フローを示します。

1. リモート ユーザが Cisco AnyConnect for VPN アクセスを介して ASA に接続します。 これは、任意のタイプのユニファイド アクセス（例：スイッチで終了した 802.1x/MAC 認証バイパス（MAB）有線セッションまたはワイヤレス LAN コントローラ（WLC）で終了したワイヤレス セッション）です。

2. 認証プロセスの一部として、ISE はエンドステーションのポスチャ ステータスが準拠（compliant）ではないこと（*ASA-VPN_quarantine* 認可ルール）、およびリダイレクション属性が *Radius Access-Accept* メッセージに入れて返されることを確認します。 その結果、ASA はすべての HTTP トラフィックを ISE にリダイレクトします。

3. ユーザは Web ブラウザを開いてアドレスを入力します。 ISE へのリダイレクト後に、Cisco AnyConnect 4 ポスチャ モジュールがステーションにインストールされます。 次にポスチャ モジュールが ISE からポリシーをダウンロードします（WSUS の要件）。

4. ポスチャ モジュールは Microsoft WSUS を検索し、修復を実行します。

5. 修復が正常に完了すると、ポスチャ モジュールはレポートを ISE に送信します。

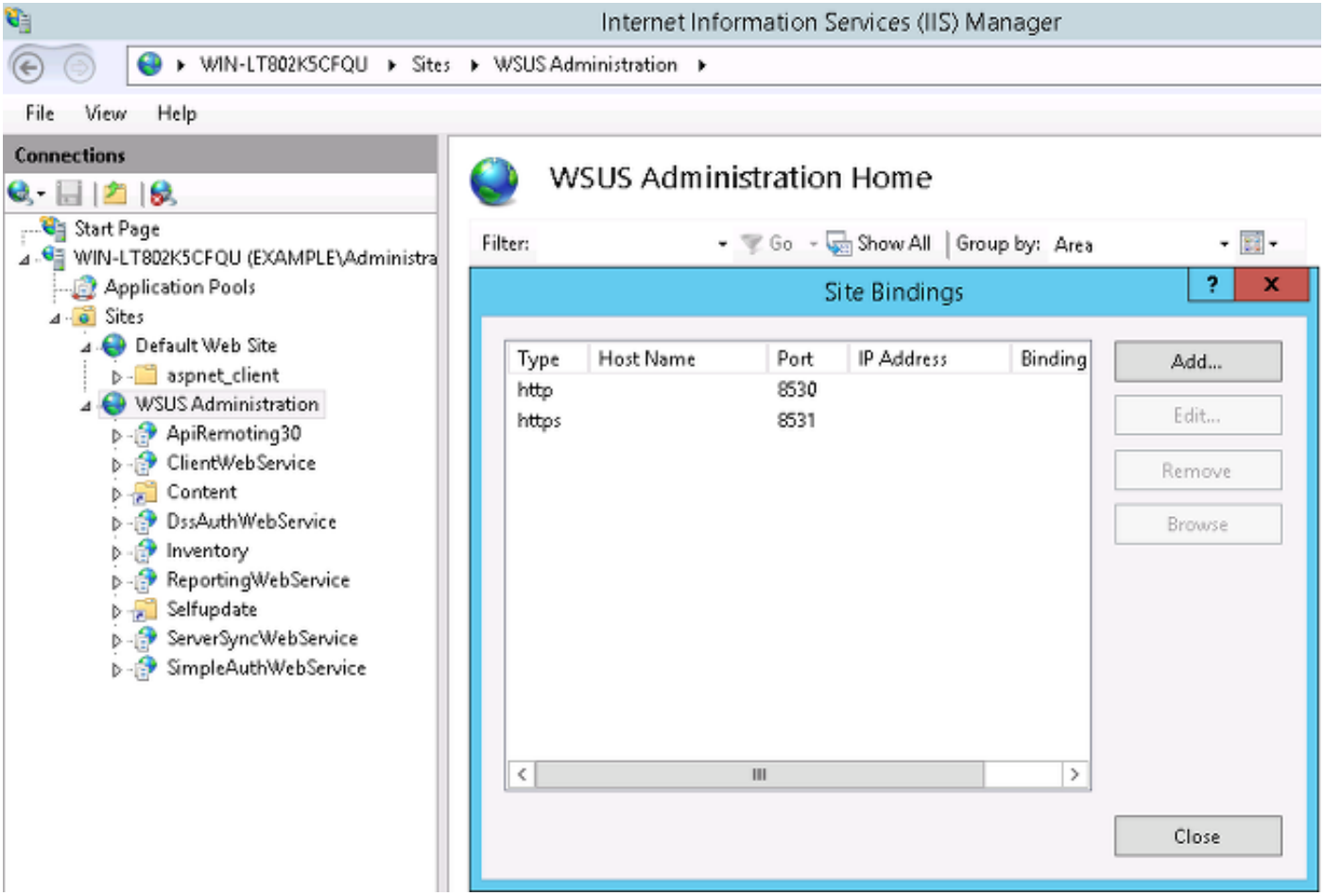
6. ISE は、準拠する VPN ユーザにフル ネットワーク アクセスを付与する Radius 認可変更（CoA）を発行します（*ASA-VPN_compliant* 認可ルール）。

   注: 修復を実行できるようにする（Microsoft Windows 更新プログラムを PC にインストールする機能）には、ユーザにローカル管理者権限が必要です。

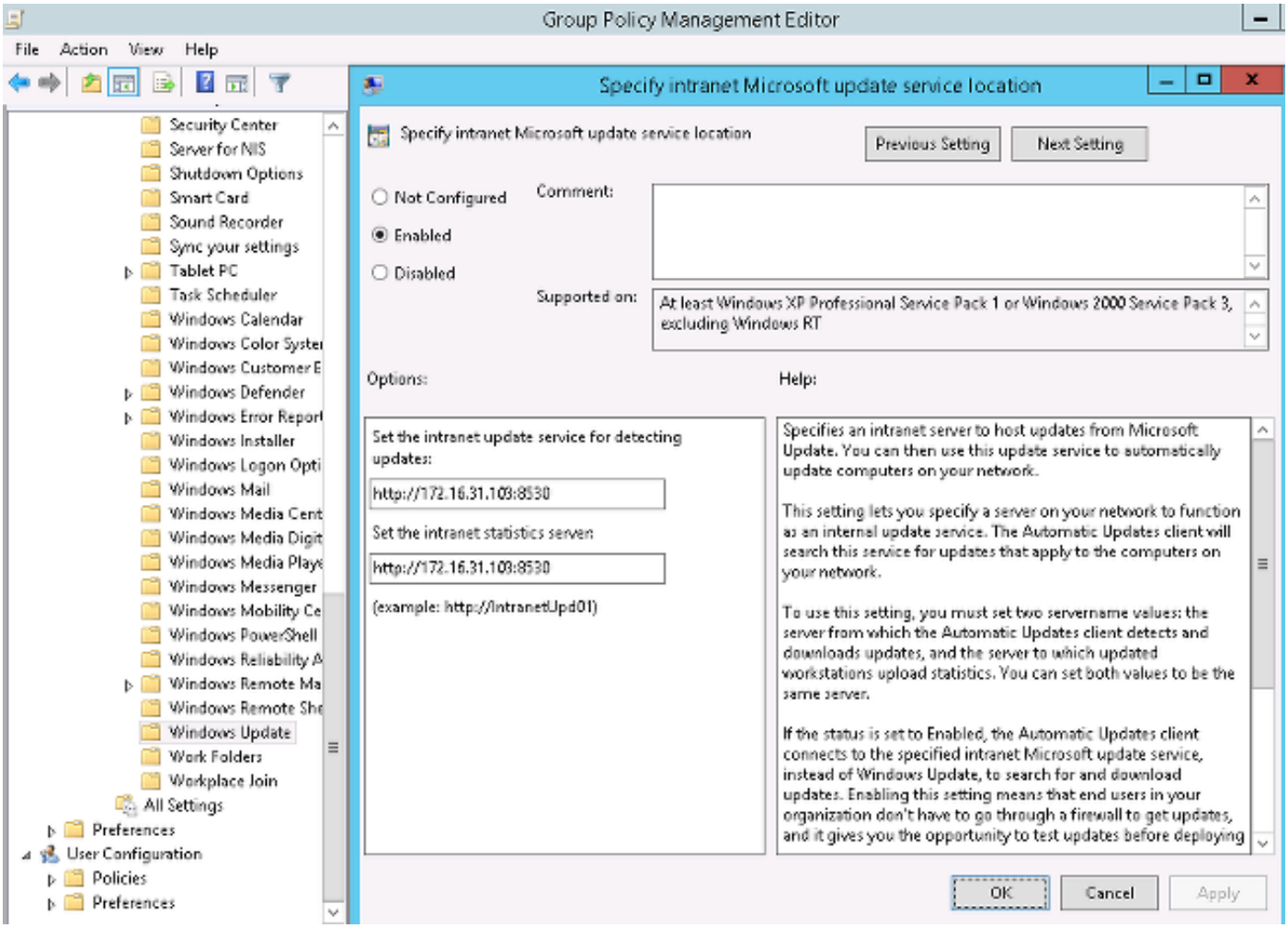
Microsoft WSUS

> **注:** WSUS の詳しい設定は、このドキュメントでは説明しません。 詳細については、Microsoft の「Windows Server Update Services を組織に展開する」を参照してください。

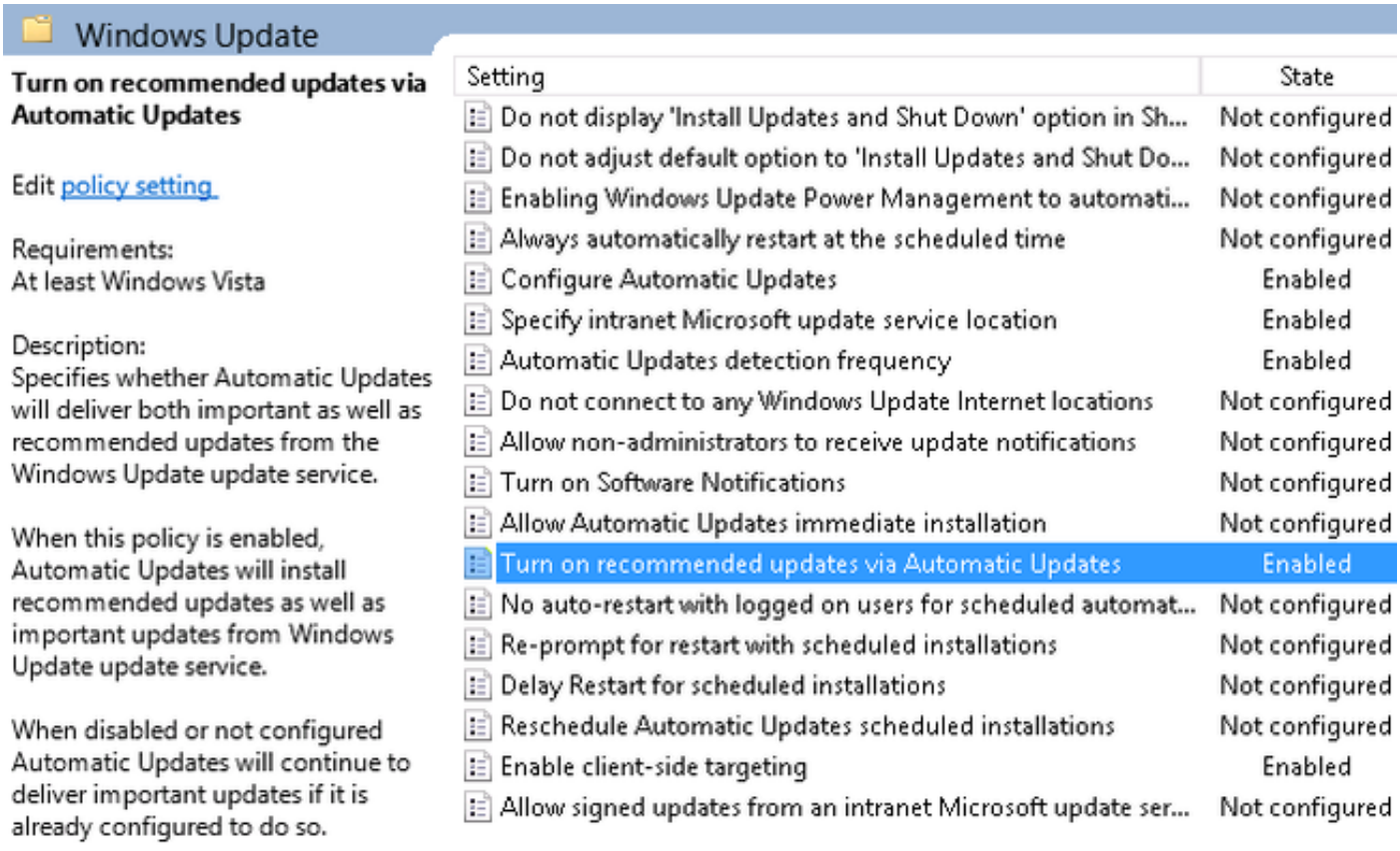
WSUS サービスは、標準 TCP ポート 8530 経由で導入されます。 重要な点として、修復には他のポートも使用されます。 そのため、WSUS の IP アドレスを ASA のリダイレクト アクセス コントロール リスト（ACL）に安全に追加できます（これについては後述します）。



ドメインのグループ ポリシーで Microsoft Windows 更新プログラムが設定されており、ローカル WSUS サーバが指定されています。



これらは、さまざまな重大度に基づく詳細なポリシーのために有効に設定されている推奨更新プログラムです。



クライアント側でのターゲット設定により、柔軟性が大きく向上します。 ISE は、さまざまな Microsoft Active Directory（AD）コンピュータ コンテナに基づくポスチャ ポリシーを使用できます。 WSUS はこのメンバーシップに基づく更新プログラムを承認できます。

ASA

リモート ユーザ用にシンプルなセキュア ソケット レイヤ（SSL）VPN アクセスが採用されています（詳細についてはこのドキュメントでは説明しません）。

次に設定例を示します。

```
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
```

ASA でアクセスリストを設定することが重要です。このアクセスリストは、（非準拠ユーザの場合に）ISE へリダイレクトする必要があるトラフィックを判別するために使用されます。

```
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
```

非準拠ユーザの場合、許可されているトラフィックはドメイン ネーム システム（DNS）、ISE、

WSUS、および Internet Control Message Protocol（ICMP）トラフィックだけです。 その他のトラフィック（HTTP）はすべて、AnyConnect 4 プロビジョニングのために ISE にリダイレクトされ、ISE がポスチャと修復を実行します。

ISE

> **注:** AnyConnect 4 プロビジョニングとポスチャについては、このドキュメントでは説明しません。 ASA をネットワーク デバイスとして設定し、Cisco AnyConnect 7 アプリケーションをインストールする方法などの詳細については、「AnyConnect 4.0 と ISE バージョン 1.3 の統合：設定例」を参照してください。

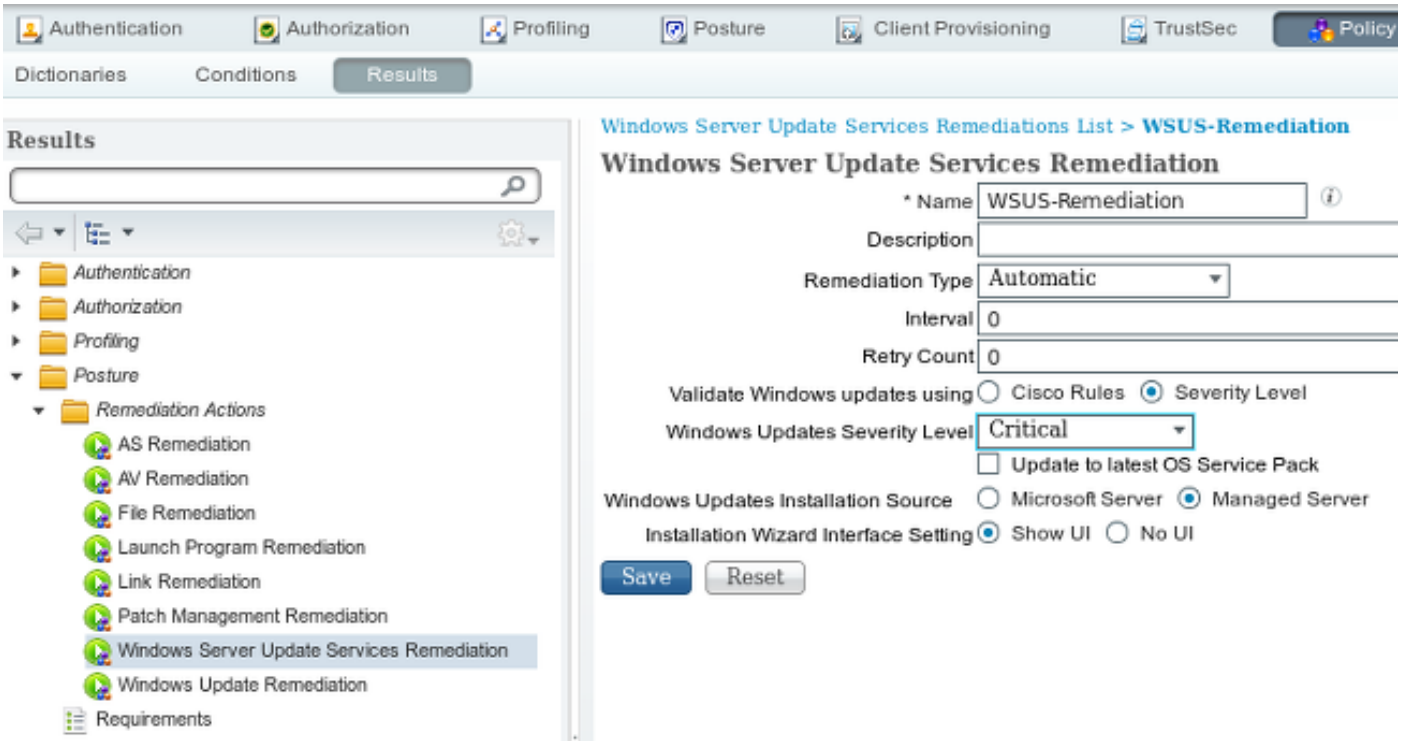
WSUS のポスチャ修復

WSUS のポスチャ修復を設定するには、次の手順を実行します。

1. 新規ルールを作成するため、[Policy] > [Conditions] > [Posture] > [Remediation Actions] > [Windows Server Update Services Remediation] に移動します。

2. [Microsoft Windows Updates] 設定が [Severity Level] に設定されていることを確認します。 この設定により、修復プロセスが開始されているかどうかを検出できるようになります。

Microsoft Windows Update Agent が WSUS に接続し、当該 PC にインストール可能な [Critical] 更新プログラムがあるかどうかを確認します。



WSUS のポスチャ要件

新規ルールを作成するため、[Policy] > [Conditions] > [Posture] > [Requirements] に移動します。 ルールでは *pr_WSUSRule* というダミー条件が使用されています。つまり、修復が必要な場合

（[Critical] 更新プログラム）の条件を確認するために、WSUS に接続します。

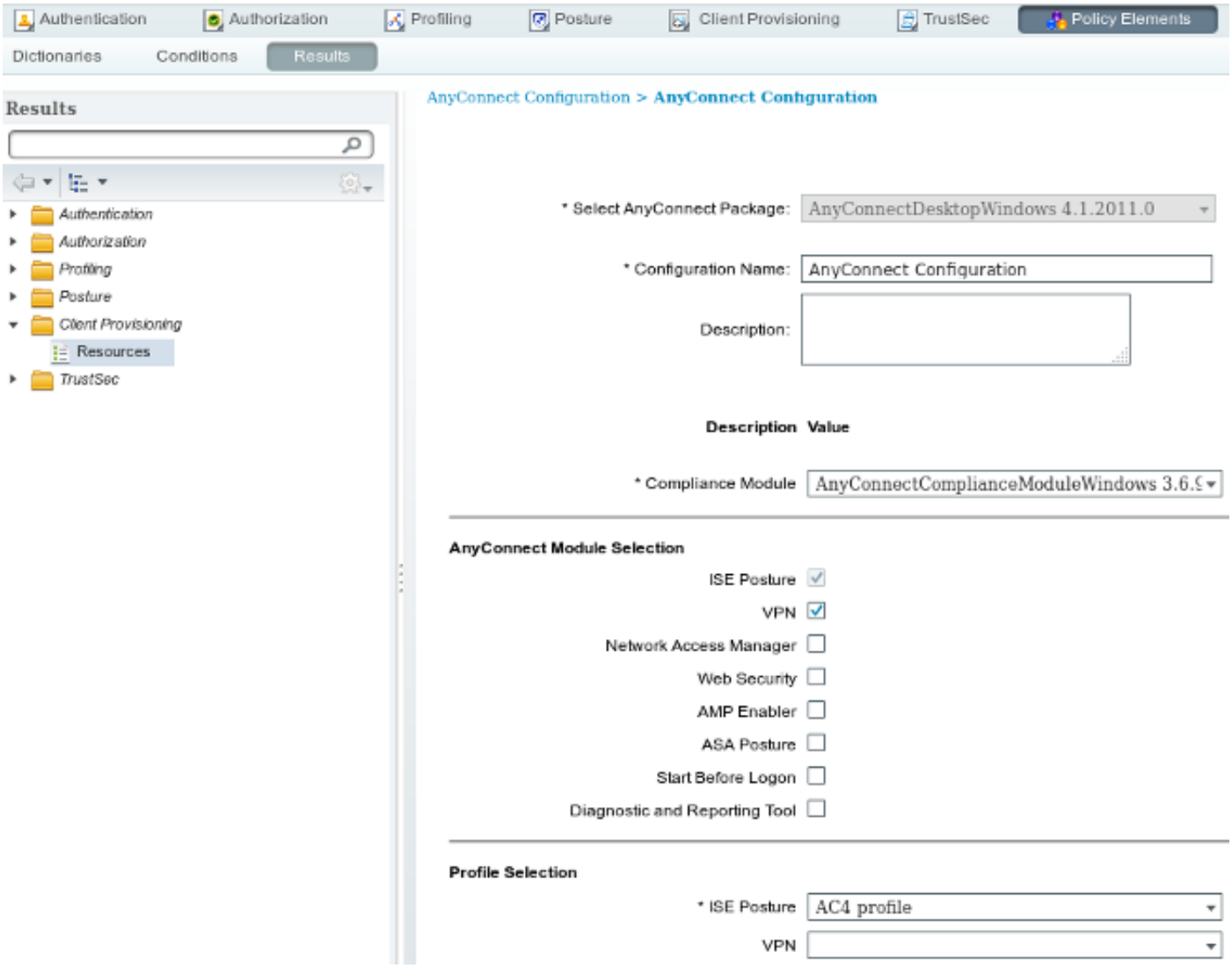
この条件に一致する場合、その PC に対して設定されている更新プログラムが WSUS によりインストールされます。 これには重大度レベルが低い更新プログラムをはじめ、あらゆるタイプの更新プログラムが含まれます。

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

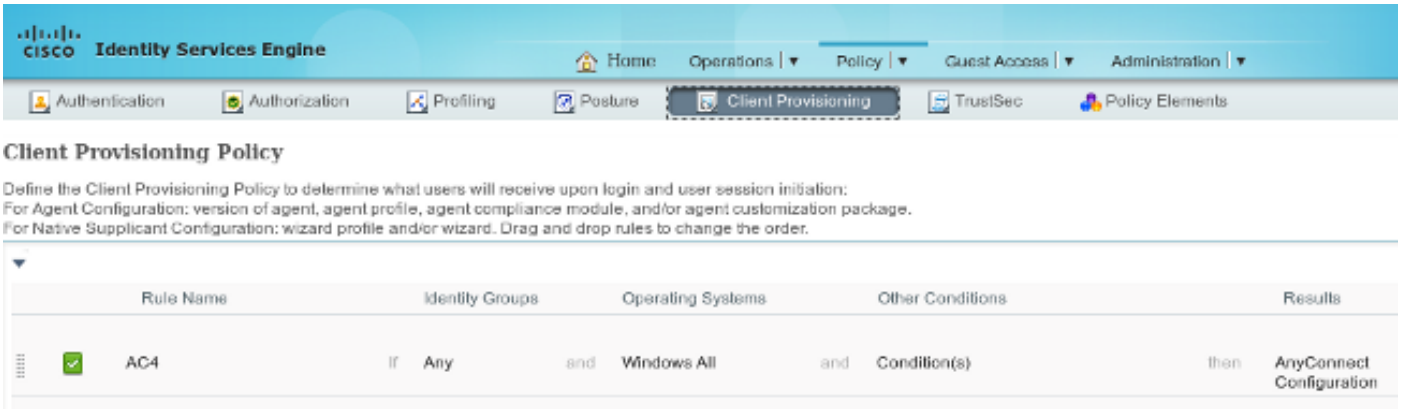
AnyConnect プロファイル

ポスチャ モジュール プロファイルと AnyConnect 4 プロファイルを設定します（「AnyConnect 4.0 と ISE バージョン 1.3 の統合：設定例」を参照）。



クライアント プロビジョニング ルール

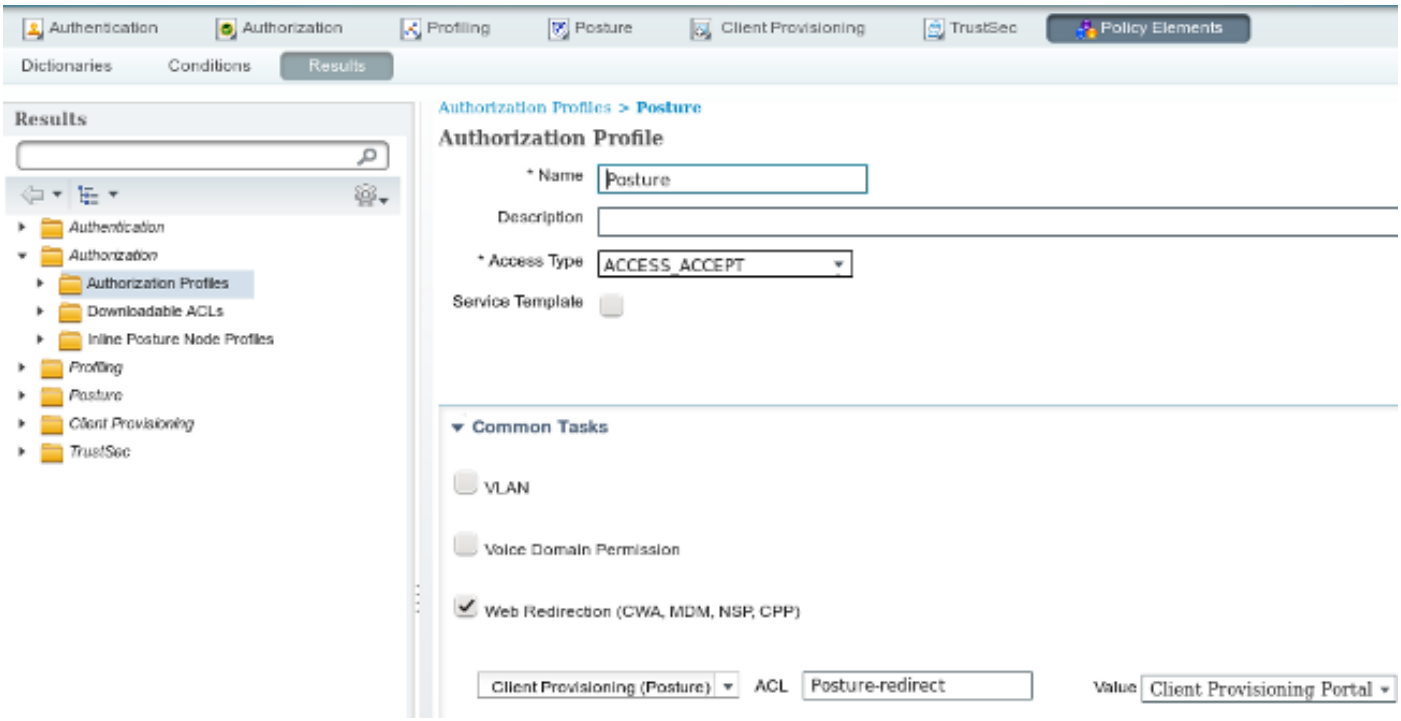
AnyConnect プロファイルの準備ができたら、[Client Provisioning] ポリシーからこのプロファイルを参照できます。



アプリケーション全体と設定がエンドポイントにインストールされ、エンドポイントが [Client Provisioning] ポータル ページにリダイレクトされるようになります。 AnyConnect 4 がアップグレードされ、追加のモジュール（ポスチャ）がインストールされることがあります。

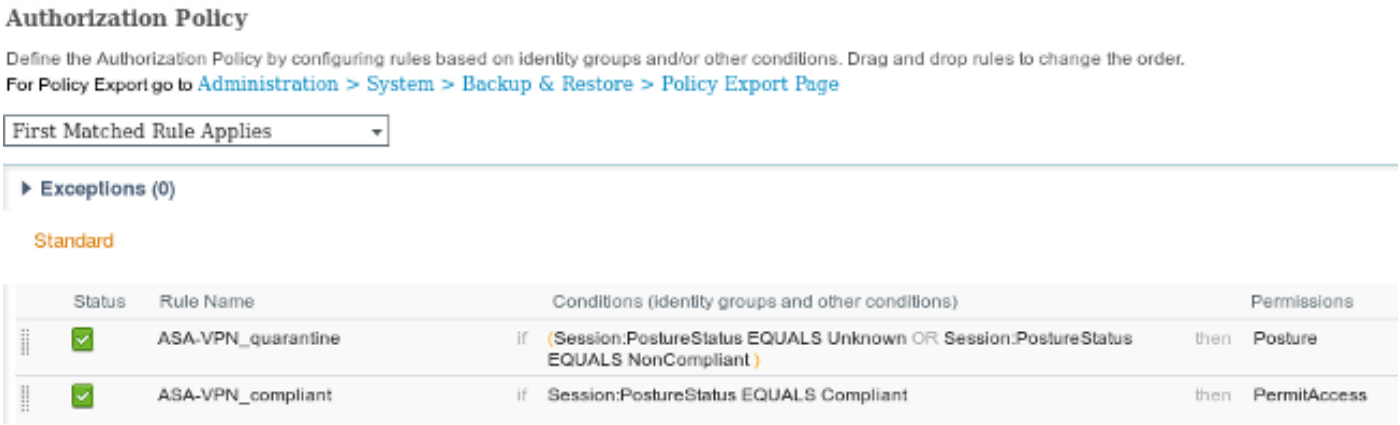
許可プロファイル（Authorization Profiles）

Client Provisioning プロファイルへのリダイレクトのための認可プロファイルを作成します。



認可規則

次の画像は認可ルールを示します。



最初に *ASA-VPN_quarantine* ルールが使用されます。 その結果、[Posture] 認可プロファイルが返され、エンドポイントが AnyConnect 4（ポスチャ モジュール付き）プロビジョニングのために Client Provisioning ポータルにリダイレクトされます。

準拠すると、*ASA-VPN_compliant* ルールが使用され、フル ネットワーク アクセスが許可されます。

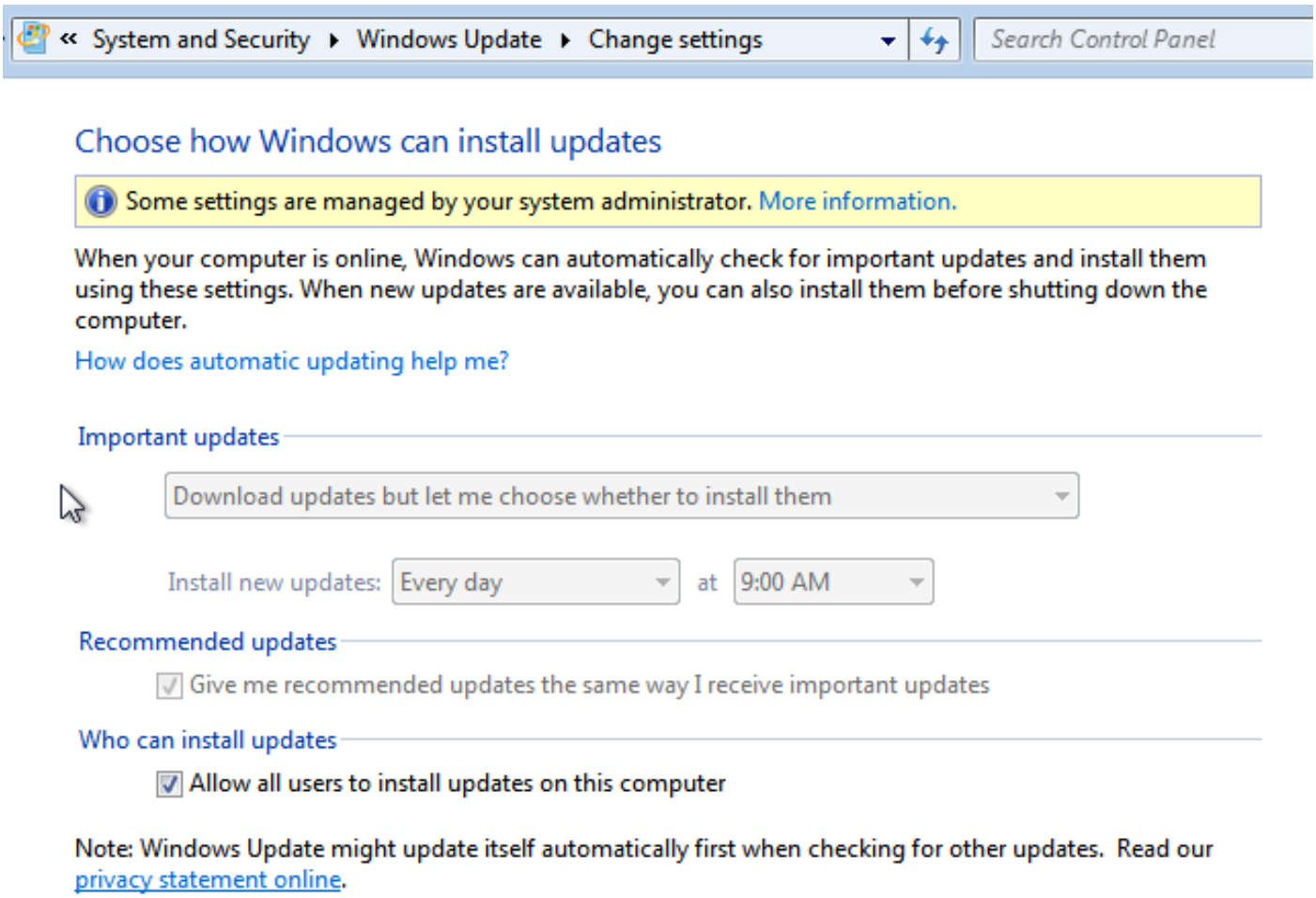
確認

ここでは、設定が正しく機能していることを検証するために使用できる情報を提供します。

GPO ポリシーが更新された PC

PC がドメインにログインした後で、ドメイン ポリシーと WSUS 設定をプッシュする必要があります。 これは、VPN セッションの確立前（アウト オブ バンド）に実行するか、または [Start Before Logon] 機能（この機能は 802.1x 有線/ワイヤレス アクセスにも使用可能）を使用している場合は確立後に実行できます。

Microsoft Windows クライアントの設定が正しい場合、これは Windows Update の設定から反映できます。

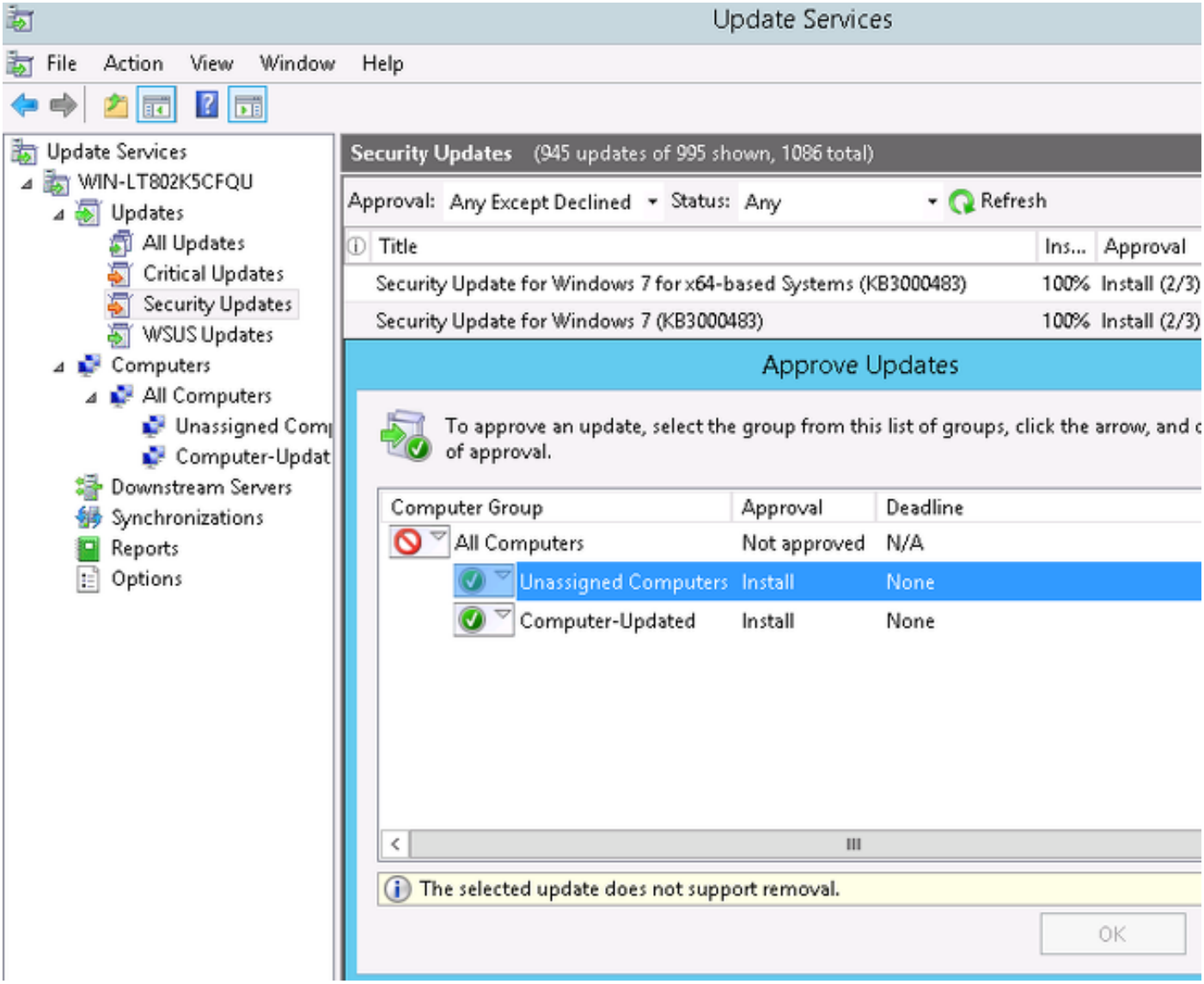


必要に応じて、グループ ポリシー オブジェクト（GPO）更新と Microsoft Windows Update Agent サーバ検出を使用できます。

```
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>
```

WSUS での重要な更新プログラムの承認

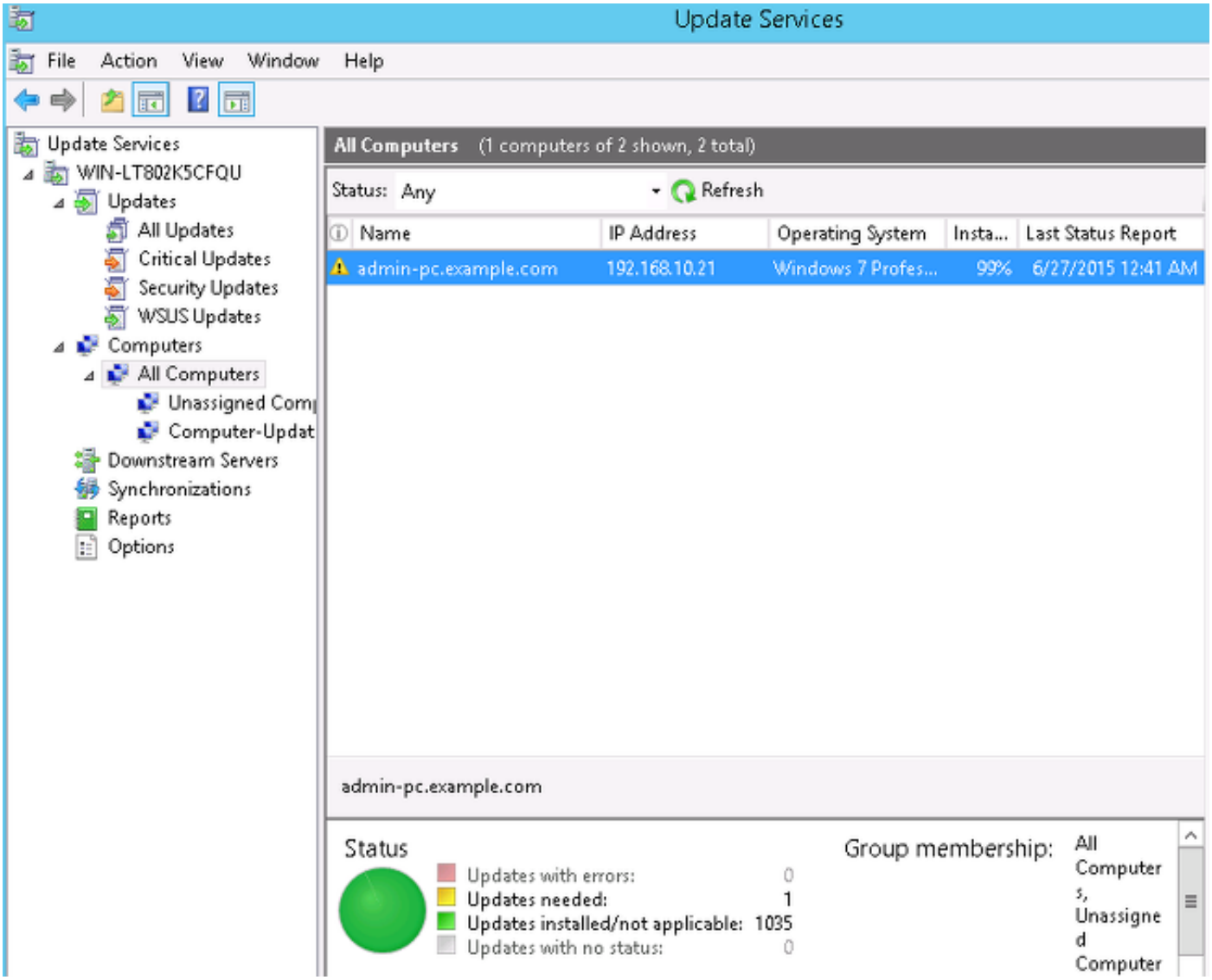
承認プロセスは、クライアントサイト ターゲティングを利用できます。



必要に応じて、*wuauclt* を使用してレポートを再送信します。

WSUS での PC ステータスの確認

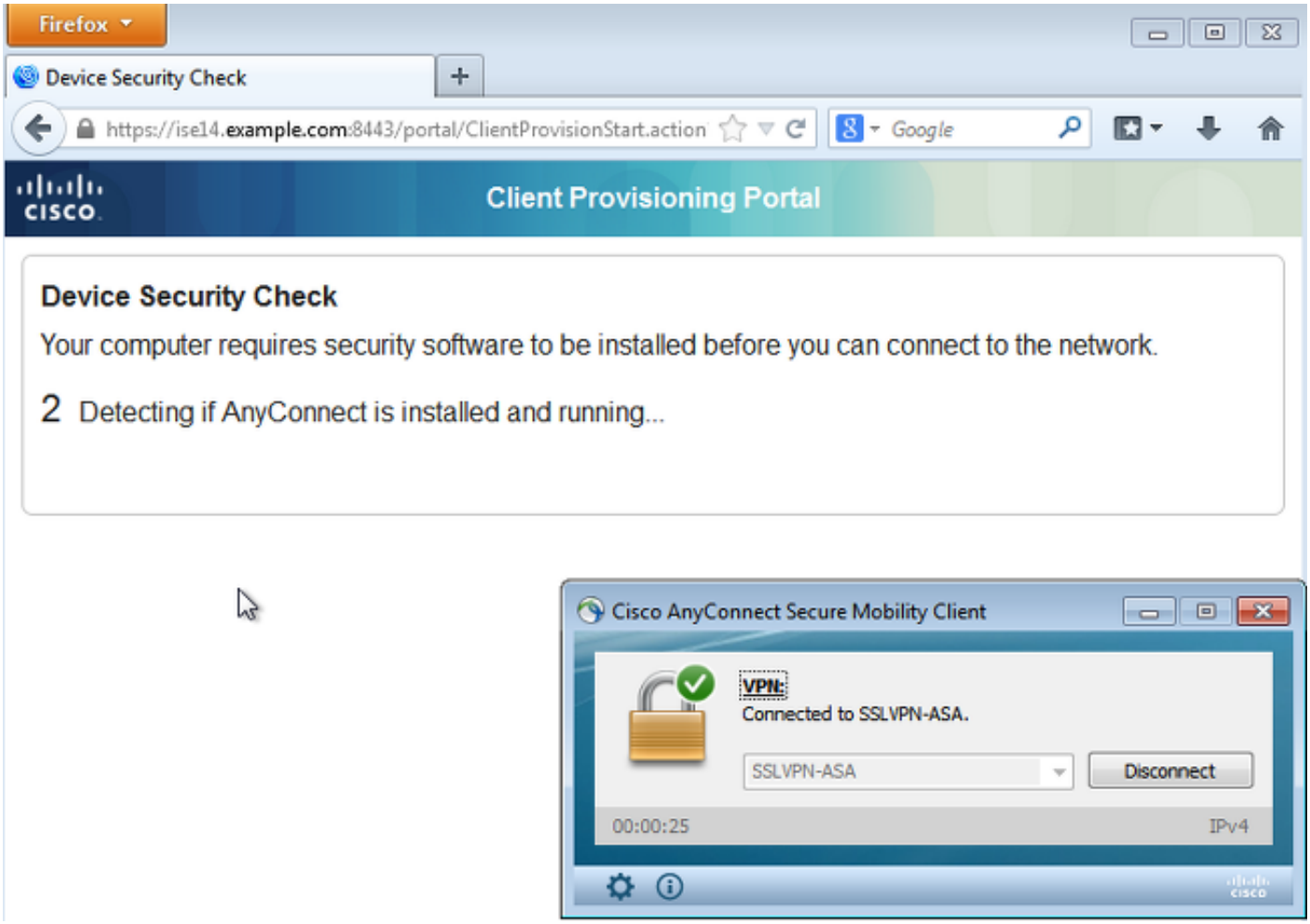
次の画像は、WSUS での PC ステータスの確認方法を示します。



WSUS の次回更新時に 1 つの更新プログラムがインストールされる必要があります。

VPN セッションの確立

VPN セッションの確立後、*ASA-VPN_quarantine* ISE 認可ルールが使用され、*Posture* 認可プロファイルが返されます。 その結果、AnyConnect 4 の更新とポスチャ モジュール プロビジョニングのために、エンドポイントからの HTTP トラフィックがリダイレクトされます。



この時点で ASA のセッション ステータスは、HTTP トラフィックの ISE へのリダイレクトにおいてアクセス権限が制限されていることを示します。

```
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-redirec
```

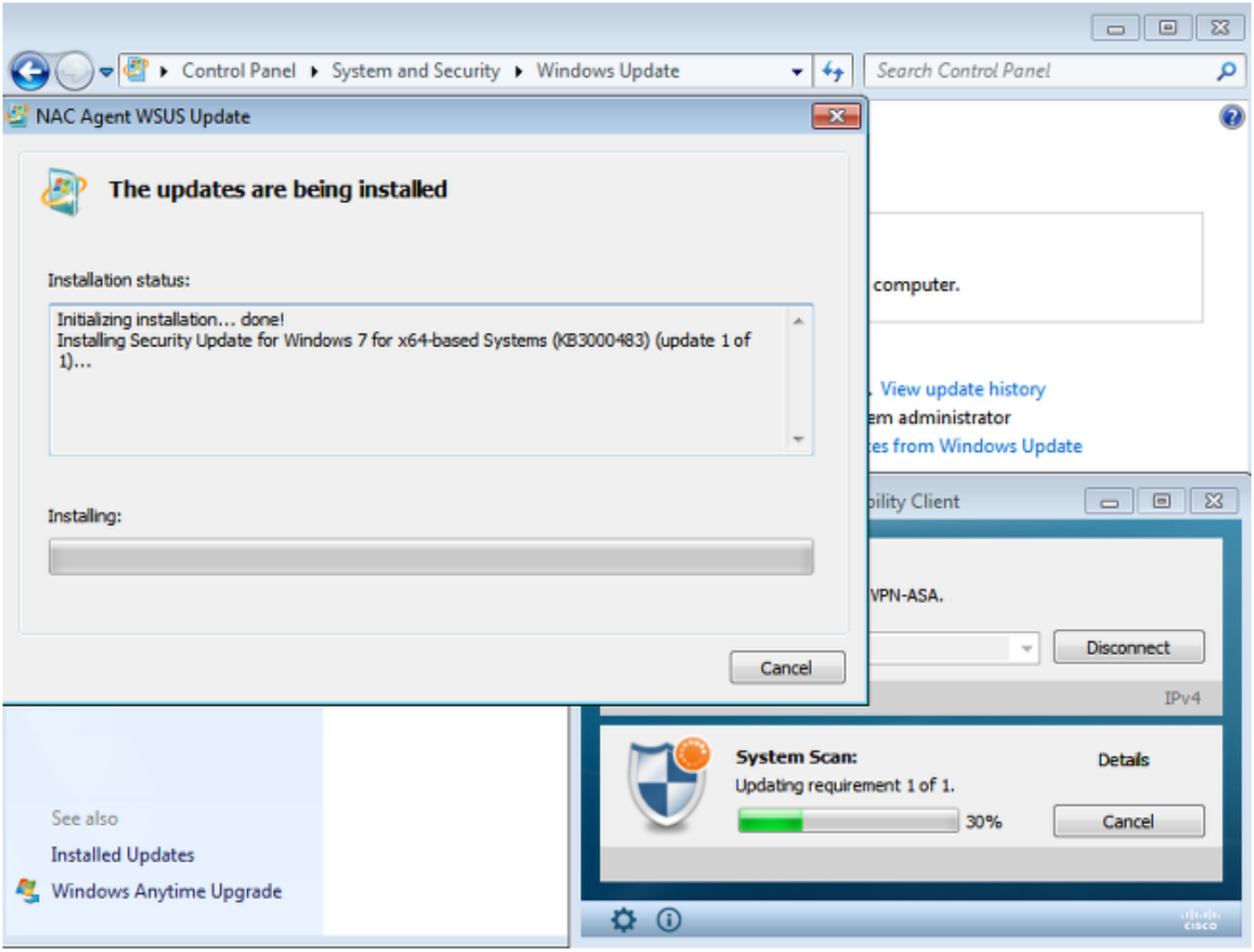
ポスチャ モジュールが ISE からポリシーを受信し修復を実行する

ポスチャ モジュールは ISE からポリシーを受け取ります。 ise-psc.log デバッグにより、ポスチャ モジュールに送信された要件が示されます。

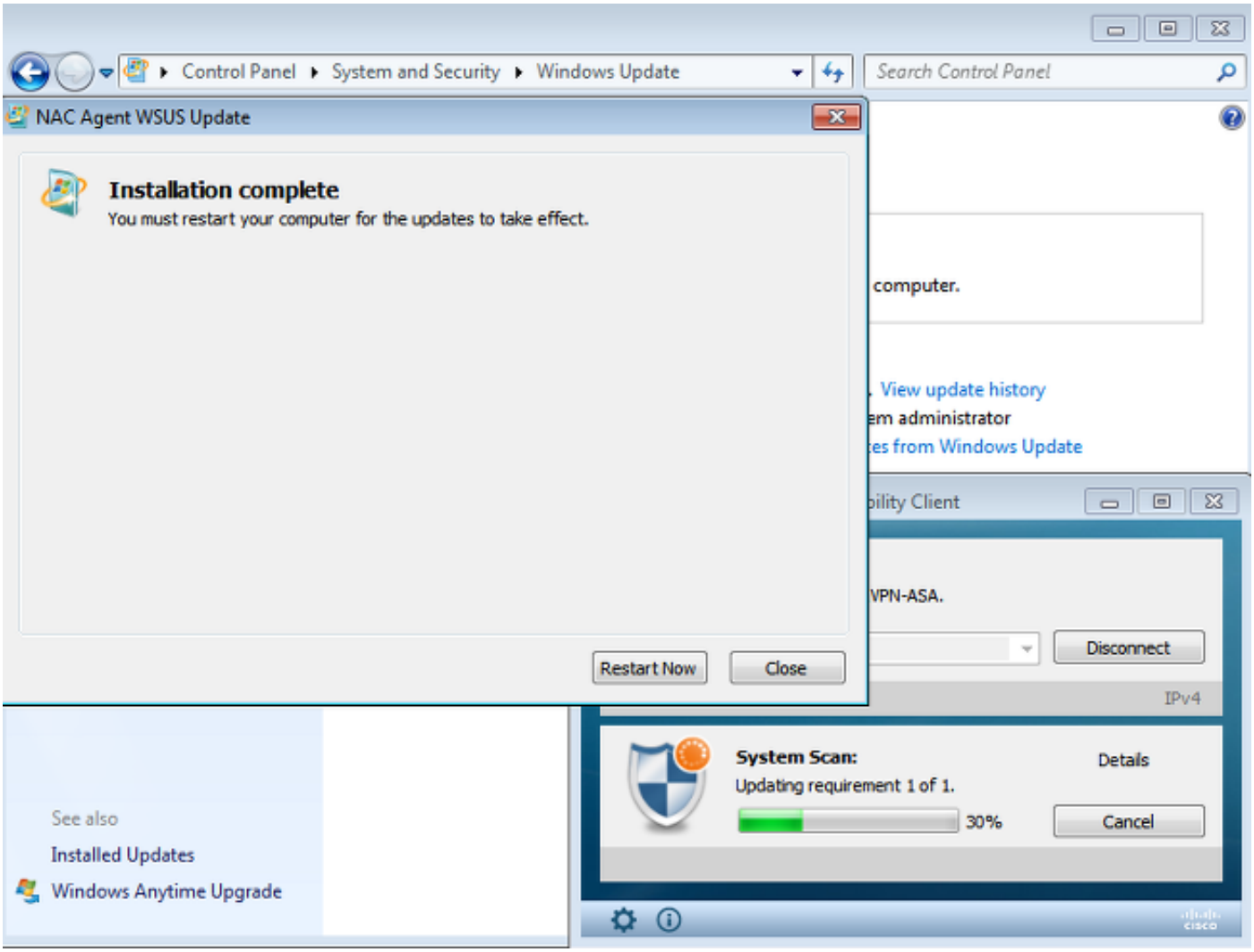
```
2015-06-05 07:33:40,493 DEBUG  [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1:::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
 <version>2</version>
 <encryption>0</encryption>
```

```
 <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>
```

ポスチャ モジュールがトリガーになり、Microsoft Windows Update Agent が自動的に WSUS に接続し、WSUS ポリシーの設定に従って更新プログラムをダウンロードします（すべてユーザの介入なしで自動的に実行されます）

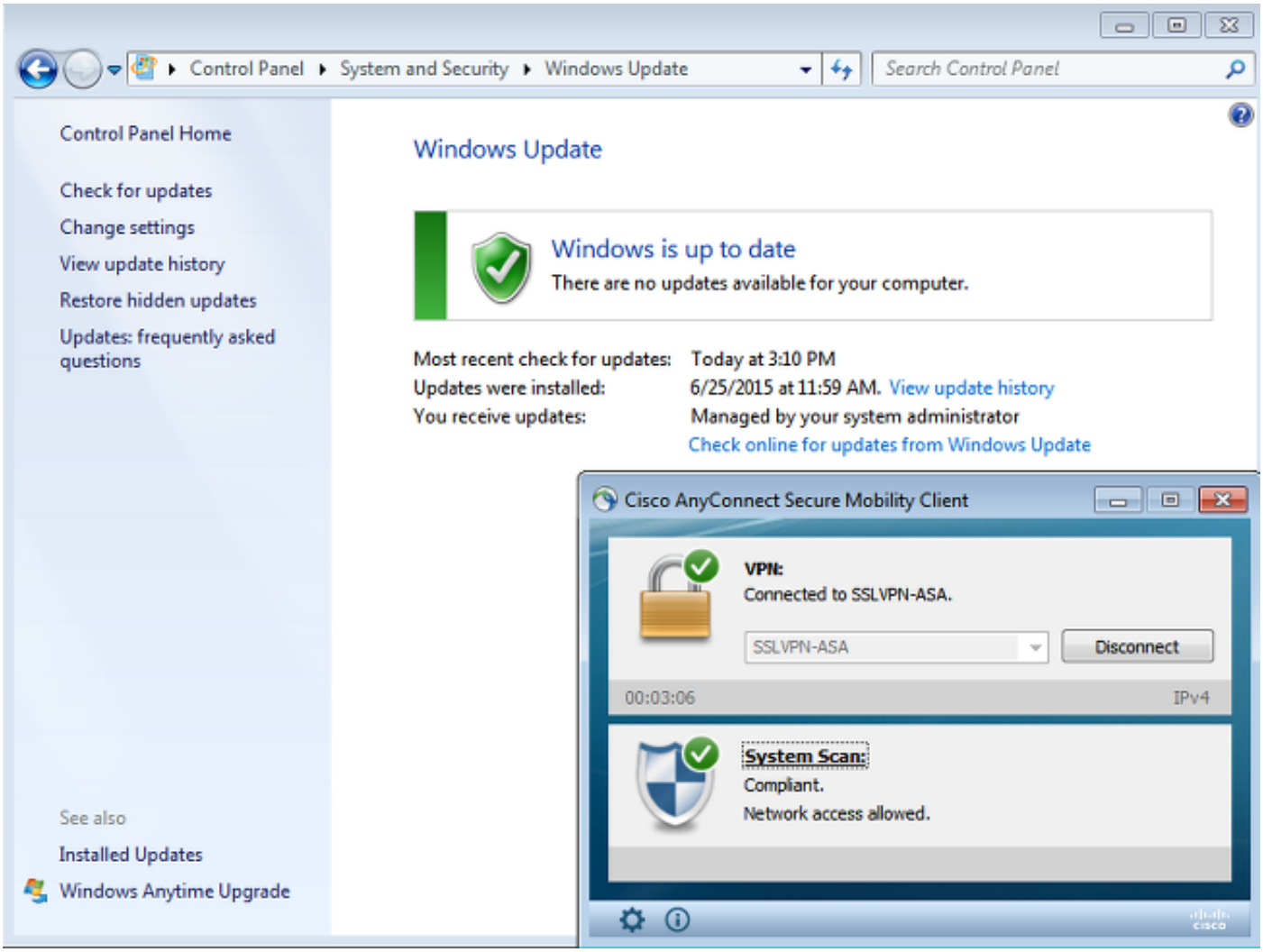


注: 一部の更新プログラムでは、システムを再起動する必要があります。

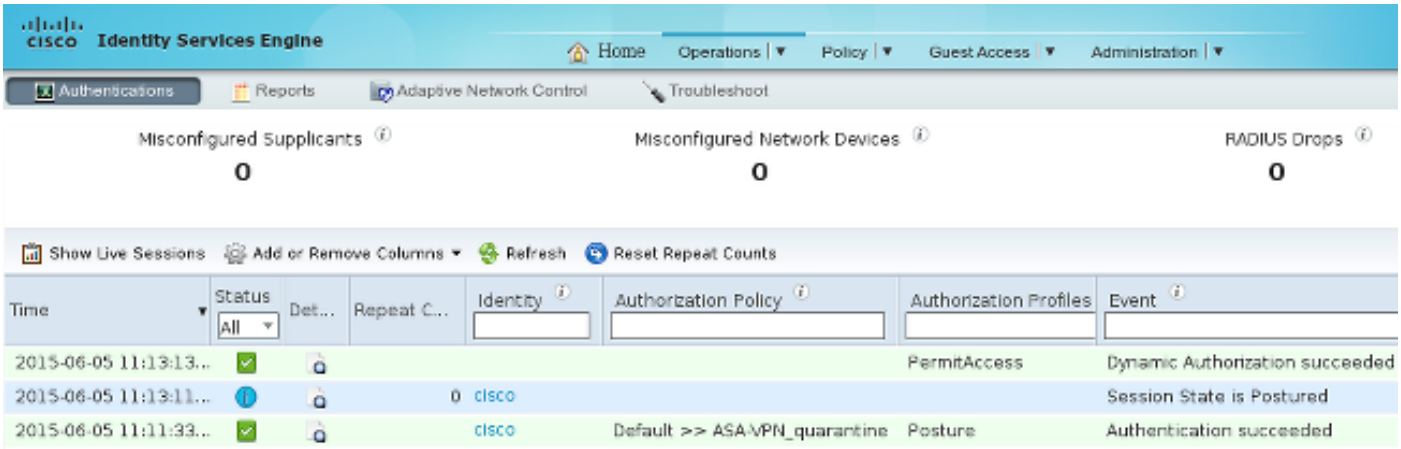


フル ネットワーク アクセス

AnyConnect ポスチャ モジュールによりステーションが準拠として報告された後で、以下のような画面が表示されます。



レポートが ISE に送信され、ISE がポリシーを再評価し、*ASA-VPN_compliant* 認可ルールに一致します。 これにより、フル ネットワーク アクセスが（Radius CoA 経由で）付与されます。 これを確認するには、[Operations] > [Authentications] に移動します。

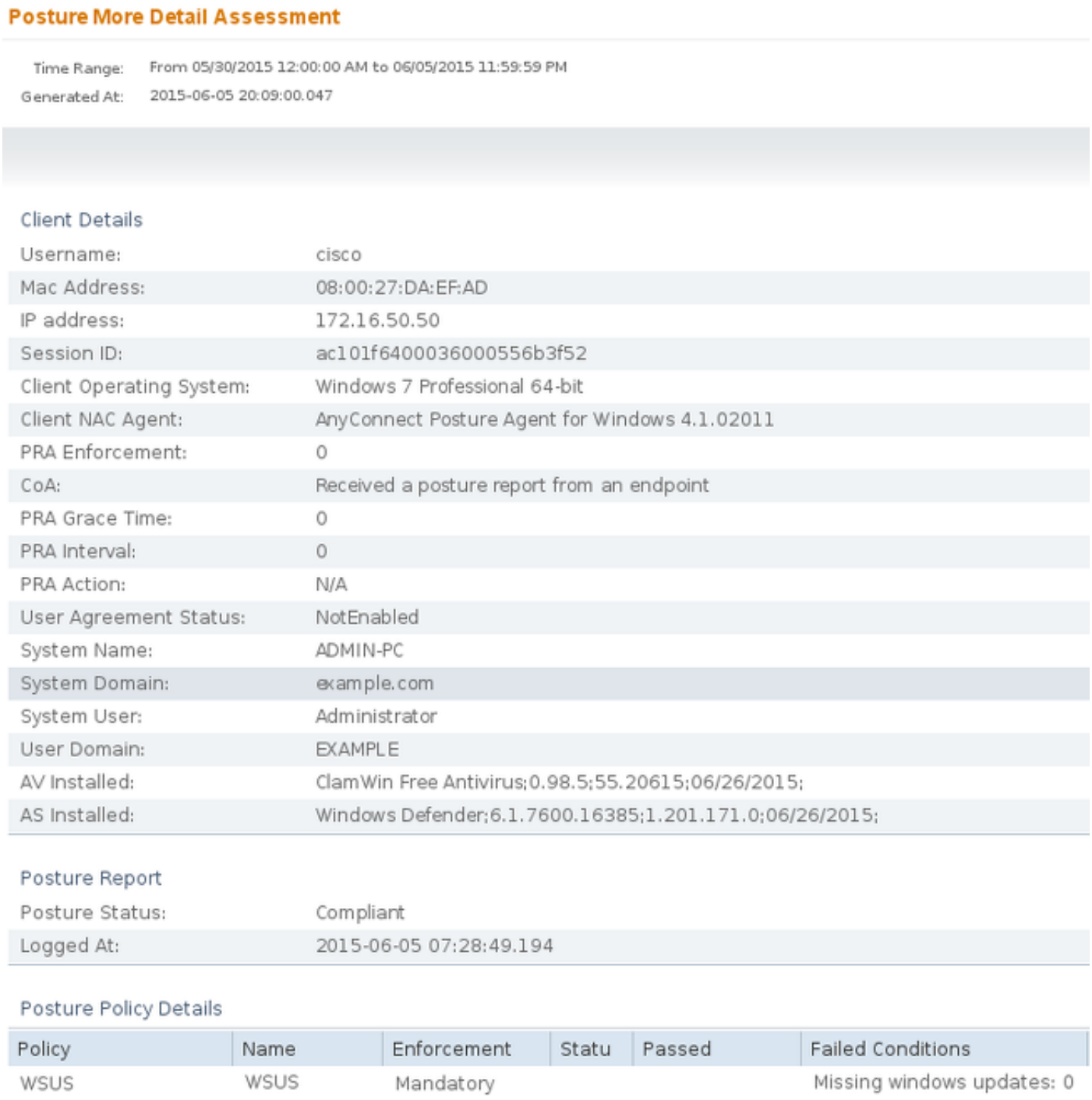


デバッグ（ise-psc.log）でも準拠ステータス、CoA トリガー、およびポスチャの最終設定が確認されます。

```
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]
```

また、[ISE Detailed Posture Assessment] レポートで、ステーションが準拠していることを確認できます。



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

注: ACIDEX 拡張により、Microsoft Windows PC の物理ネットワーク インターフェイスの Media Access Control（MAC）アドレスが判明します。

トラブルシューティング

現在のところ、この設定に関するトラブルシューティング情報はありません。

重要事項

ここでは、このドキュメントで説明する設定に関する重要な点について説明します。

WSUS 修復のオプションの詳細

要件の条件と修復を区別することが重要です。 AnyConnect は Microsoft Windows Update Agent をトリガーし、Microsoft Windows Update Agent は修復設定を使用して [Validate Windows updates using] に応じて準拠を確認します。

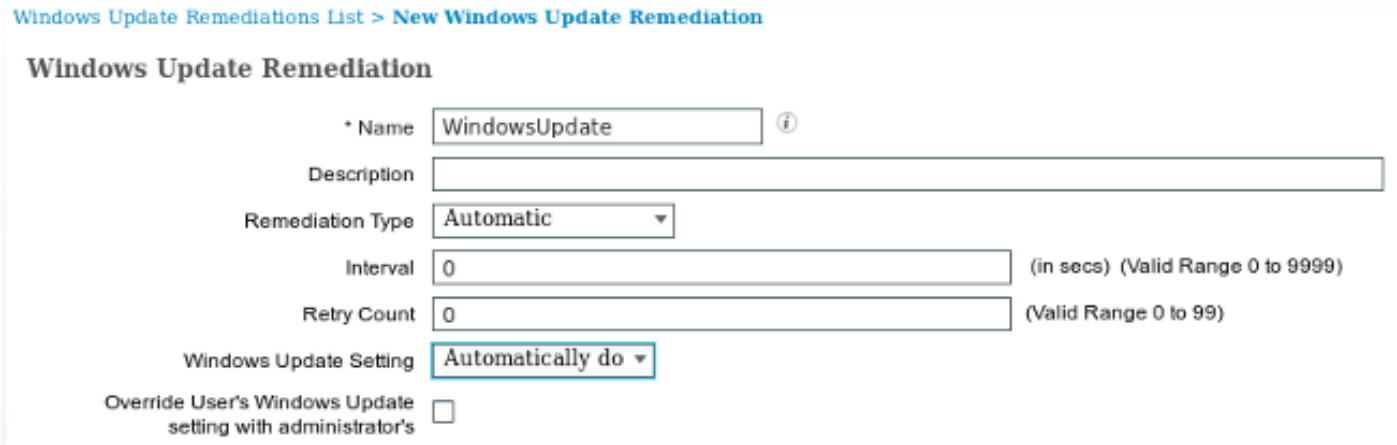
この例では、[Severity Level] を使用しています。 [Critical] 設定では、保留中の（インストールされていない）重要な更新プログラムがあるかどうかを Microsoft Windows Agent がチェックします。 存在する場合は、修復が開始されます。

修復プロセスでは、WSUS の設定に基づいて、重要な更新プログラムと、それほど重要ではない更新プログラムがすべてインストールされます（特定のマシンを対象として承認された更新プログラム）。

[Validate Windows updates using] が [Cisco Rules] に設定されている場合、要件で詳しく設定されている条件によって、ステーションが準拠しているかどうかが判別されます。

Windows Update Service

WSUS サーバを使用しない導入には、*Windows Update Remediation* と呼ばれる別の修復タイプを使用できます。



この修復タイプでは、Microsoft Windows Update 設定を制御でき、即時更新を実行できます。 この修復タイプで使用する一般的な条件は *pc_AutoUpdateCheck* です。 これにより、エンドポイントで Microsoft Windows Update の設定が有効になっているかどうかを確認できます。 有効にな

っていない場合は、有効にして更新プログラムを実行します。

SCCM 統合

ISE バージョン 1.4 の新機能であるパッチ管理により、複数のサードパーティ ベンダーと統合できます。 ベンダーによっては、条件と修復の両方を対象とした複数のオプションが使用可能です。

Microsoft では、Systems Management Server（SMS）と System Center Configuration Manager（SCCM）の両方がサポートされます。

関連情報

- Cisco ISE コンフィギュレーション ガイドのポスチャ サービス
- Cisco Identity Services Engine 管理者ガイド リリース 1.4
- Cisco Identity Services Engine 管理者ガイド リリース 1.3
- Windows Server Update Services を組織に展開する
- テクニカル サポートとドキュメント – Cisco Systems