



Cisco AnyConnect Secure Mobility Client integration with ISE & SCCM client for patch remediation on windows

This document is about how Cisco AnyConnect Secure Mobility client (aka AnyConnect) can be integrated with Cisco Identity Service Engine (aka ISE) and System Center Configuration Manager (SCCM) for patching Microsoft Windows platform with windows patches. This document would help in quick references on how integration is done and also configuration steps.

Table of Contents

1. Introduction	2
2. Patch Management Conditions	4
2.1 Installed check:.....	4
2.2 Enabled check:	4
2.3 Up-to-date:.....	4
3. Patch management remediation	5
3.1 Enable:	5
3.2 Up-to-date:.....	5
4. Configuration steps to remediate SCCM client, using AnyConnect:	5
5. Requirements	11
5.1 AnyConnect and ISE versions	11
5.2 SCCM	11
5.3 ISE Compliance Module	11

1. Introduction

In the ISE 1.4 and AnyConnect 4.1 release, Patch Management checks and remediation for System Center Configuration Manager (SCCM) support was added to ISE Posture features in respective products.

SCCM is the Microsoft's Patch management solution, which manages patch updates on Microsoft endpoints. The SCCM server deploys a configuration manager client on endpoints that it controls, this client is responsible for notifying the end-user that there are patches that are missing on endpoint, the client also lets the user install the patches that are deployed at the server.

The SCCM server does a Software Update Scan at configured intervals, which causes it to probe for the patch update status of the endpoints administered by the SCCM server. The SCCM server then notifies the SCCM client that there are patches/updates that need to install. (If there were patches uninstalled manually on client or there are new patches/updates deployed on the Software Update Groups on the SCCM server).

AnyConnect 4.1 and ISE1.4 integration with SCCM client, provides the ability, to verify if the SCCM client is pending install of CRITICAL severity patches (as classified by Microsoft®), in case there are CRITICAL severity patches available for install, AnyConnect client can remediate by installing all the CRITICAL severity patches before providing full network access to the endpoint.

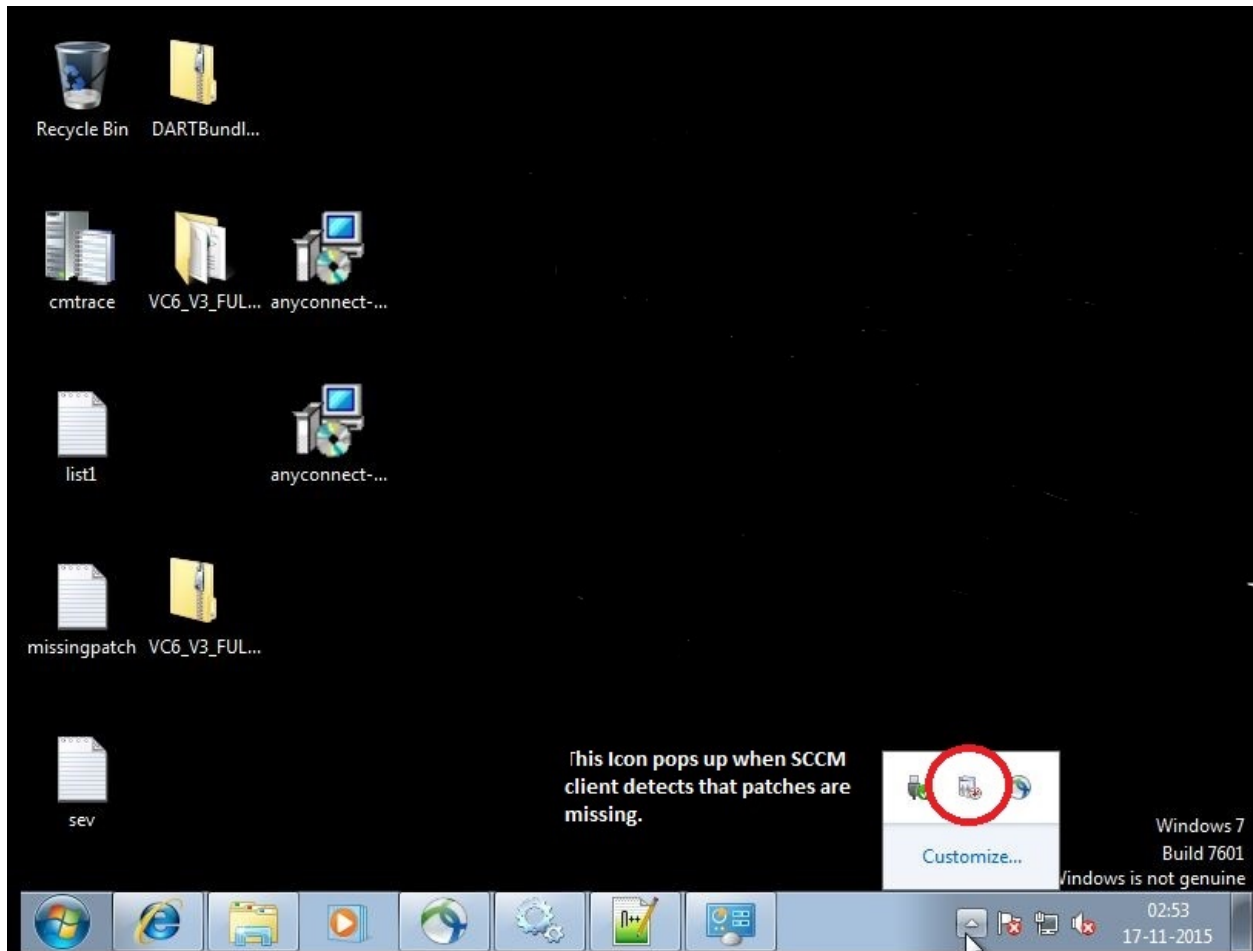


Figure 1:

*** When the SCCM client is notified by the SCCM server about missing patches, it prompts user with the notification icon highlighted in the screenshot).*

The PM up-to-date check will deem the client COMPLIANT, if the SCCM Client does not have any notifications from SCCM server that there are CRITICAL patches pending for installation.

Note: There might be pending patches with lower severity when up-to-date PM check is evaluated, the check will pass in that case. As mentioned earlier, the check looks only for missing Critical patches and remediates Critical severity patches only.

The PM check will deem the client NONCOMPLIANT, if the SCCM Client has got notifications from server that there are pending CRITICAL patches / updates for install and the user has not yet installed those critical patches.

2. Patch Management Conditions

PM posture checks that are supported with ISE 1.4 and above

2.1 Installed check:

Check evaluates if supported Patch Management client software is installed.

Passes when, finds a supported PM client software (as in support charts), installed on endpoint.

Fails when, does not find a supported PM client software installed on endpoint

2.2 Enabled check:

Check evaluates if supported Patch Management client software is enabled

Passes when, it finds that the supported PM client service is running.

Fails when, it finds that the supported PM client service is not running.

2.3 Up-to-date:

Check for the SCCM Client's patch update status. The check passes when the SCCM client installed on the endpoint indicates that there are no pending **Critical severity patches/updates to be installed**. The PM up-to-date check looks for **Critical** severity patches (classified by Microsoft), missing on the endpoint.

Passes when, SCCM client on endpoint indicates that there no Critical patches, pending for install. There might be pending patches with lower severity, the check will pass it that case. As mentioned earlier, the check looks only for missing Critical patches.

Fails when, SCCM client on endpoint indicates that there is at least one Critical patch, pending for install.

3. Patch management remediation

PM posture remediation actions that are supported with ISE 1.4 and above

3.1 Enable:

Remediation action starts the required services for the supported PM client software.

3.2 Up-to-date:

This directs the installed and supported PM client software, to download the Critical patch or patches that were found while evaluating the PM up-to-date check.

4. Configuration steps to remediate SCCM client, using AnyConnect:

Below are steps to configure ISE and Endpoint for AnyConnect to check/remediate windows patches via SCCM.

Steps:

1. On the SCCM server, configure a software update group containing at least 1 CRITICAL patch from Microsoft for the target endpoints. And deploy this software update group for target group of computers. Please refer to screenshot below.

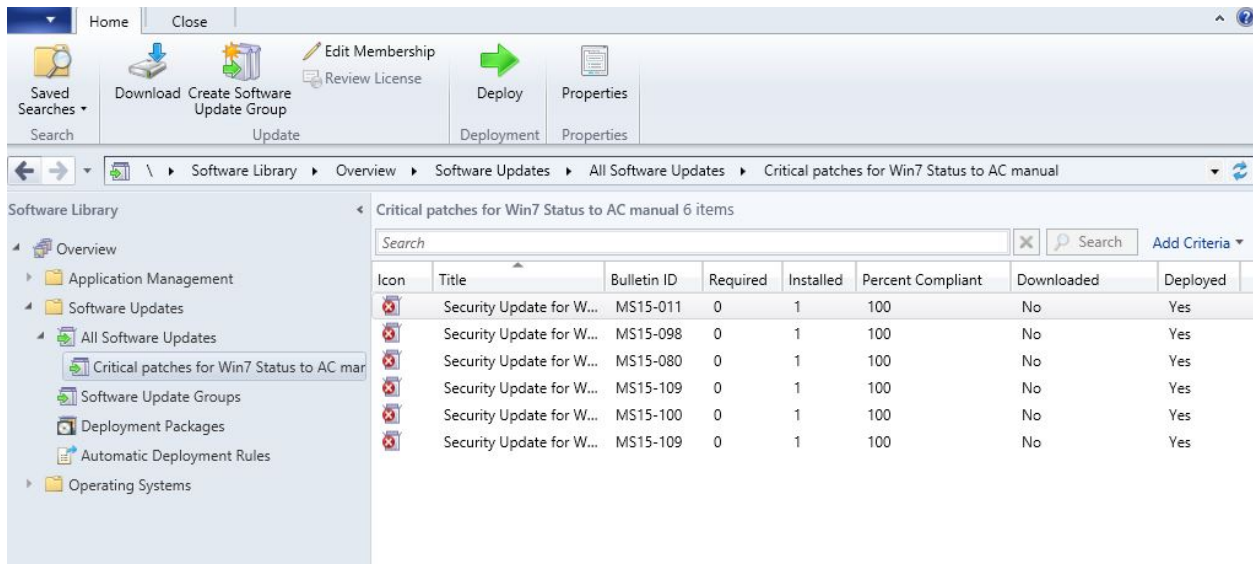


Figure 2: Collection of CRITICAL patches to be deployed for Win7 endpoints

2. Patch Management configuration on ISE

2.1. On ISE configure conditions to check for 'up-to-date' patch status, this check causes Anyconnect to query the SCCM client, if there are any missing patches on the client.

Patch-Management Conditions List > **PM_SCCM**

Patch Management Condition

* Name: PM_SCCM

Description:

* Operating System: Windows All

* Vendor Name: Microsoft Corp.

Check Type: Installation Enabled Up to Date

▼ **Products for Selected Vendor**

Product Name	Version	Enabled Checked Support	Update Checked Support	Minimum Compliant Module Support
<input type="checkbox"/> Microsoft SMS 2003 Advanced ...	7.x	YES	NO	3.6.9845.2
<input type="checkbox"/> Microsoft Windows AutomaticUp...	7.x	YES	YES	3.6.9845.2
<input type="checkbox"/> Microsoft Windows Update Agent	7.x	YES	YES	3.6.9845.2
<input type="checkbox"/> System Center Configuration Ma...	4.x	YES	YES	3.6.8963.2
<input checked="" type="checkbox"/> System Center Configuration Ma...	5.x	YES	YES	3.6.9759.2

Figure 3: SCCM condition configuration on ISE

Note: this condition will pass if there are no missing CRITICAL patches or the missing patches do not include a CRITICAL patch from Microsoft.

2.2. Configure a Patch management remediation action to trigger SCCM remediation if the up-to-date condition (configured above), fails.

Patch Management Remediations List > **Remediate_PM_WIN_SCCM**

Patch Management Remediation

* Name: Remediate_PM_WIN_SCCM

Description:

Remediation Type: Automatic

* Interval: 0 (Valid Range 0 to 9999)

* Retry Count: 0 (Valid Range 0 to 99)

Operating System: Windows

* Patch Management Vendor Name: Microsoft Corp.

Remediation Option: Enable Install missing patches Activate patch management software GUI

▼ **Products for Selected Vendor**

Product Name	Version	Enabled Remediation Support	Update Remediation Support	Show UI Remediation Support
<input type="radio"/> Microsoft Windows AutomaticUp...	7.x	YES	NO	NO
<input type="radio"/> Microsoft Windows Update Agent	7.x	NO	YES	NO
<input type="radio"/> System Center Configuration Ma...	4.x	YES	YES	NO
<input checked="" type="radio"/> System Center Configuration Ma...	5.x	YES	YES	NO

Figure 4: SCCM remediation configuration on ISE

Select the SCCM client version that is installed on the endpoint. (In this example its 5.x)

2.3. Create a requirement from the condition and remediation action created.

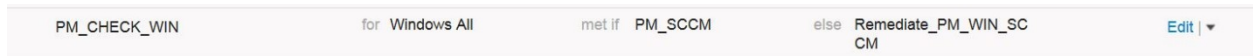


Figure 5: SCCM requirement configuration on ISE

Create a Posture policy with the requirement that was created and enforce it for windows endpoints that are managed by ISE.

3. On the endpoint, verify that SCCM client has missing patches, at least 1 CRITICAL patch should be missing for AnyConnect to remediate the SCCM client. Please note that the popup is shown only when SCCM clients detects missing patches on end point.

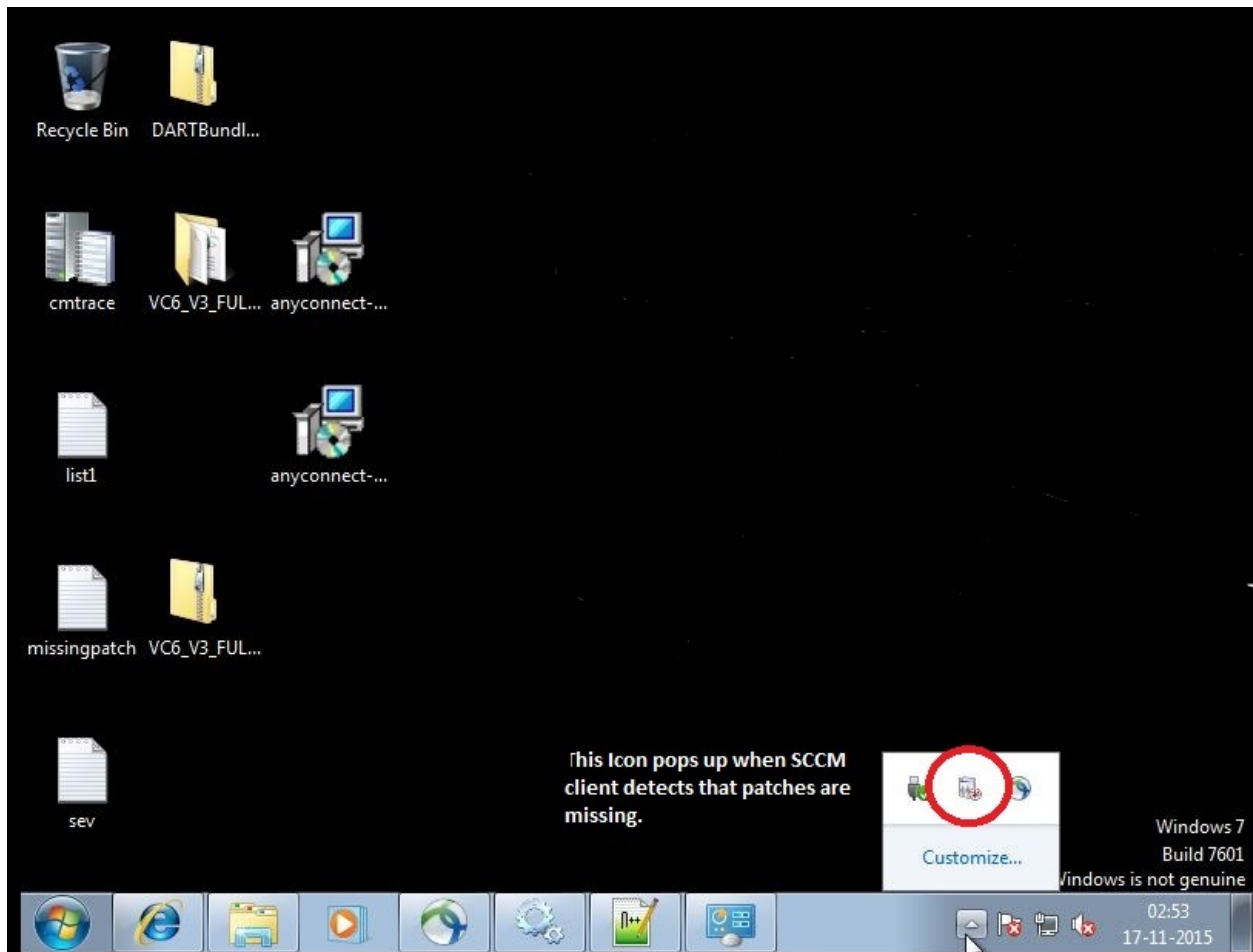


Figure 6:SCCM client popup for an update

4. At this point install Anyconnect (VPN and System Scan Modules), and connect to NAD, which is managed by ISE server on which Patch management policy is enforced.
5. At this instant, remediation is triggered by AnyConnect 'System Scan' component and in the process SCCM client downloads the missing critical patches required by the SCCM server's Software update group.
 - 5.1. SCCM Client Logs to monitor:
 - 5.1.1. C:\Windows\CCMLogs\ScanAgent.log (Scan requests for software updates)
 - 5.1.2. C:\Windows\CCMLogs\WUAHandler.log (Status of patch installation)
 - 5.1.3. C:\Windows\CCMLogs\UpdatesStore.log (patch details that are being installed during remediation)

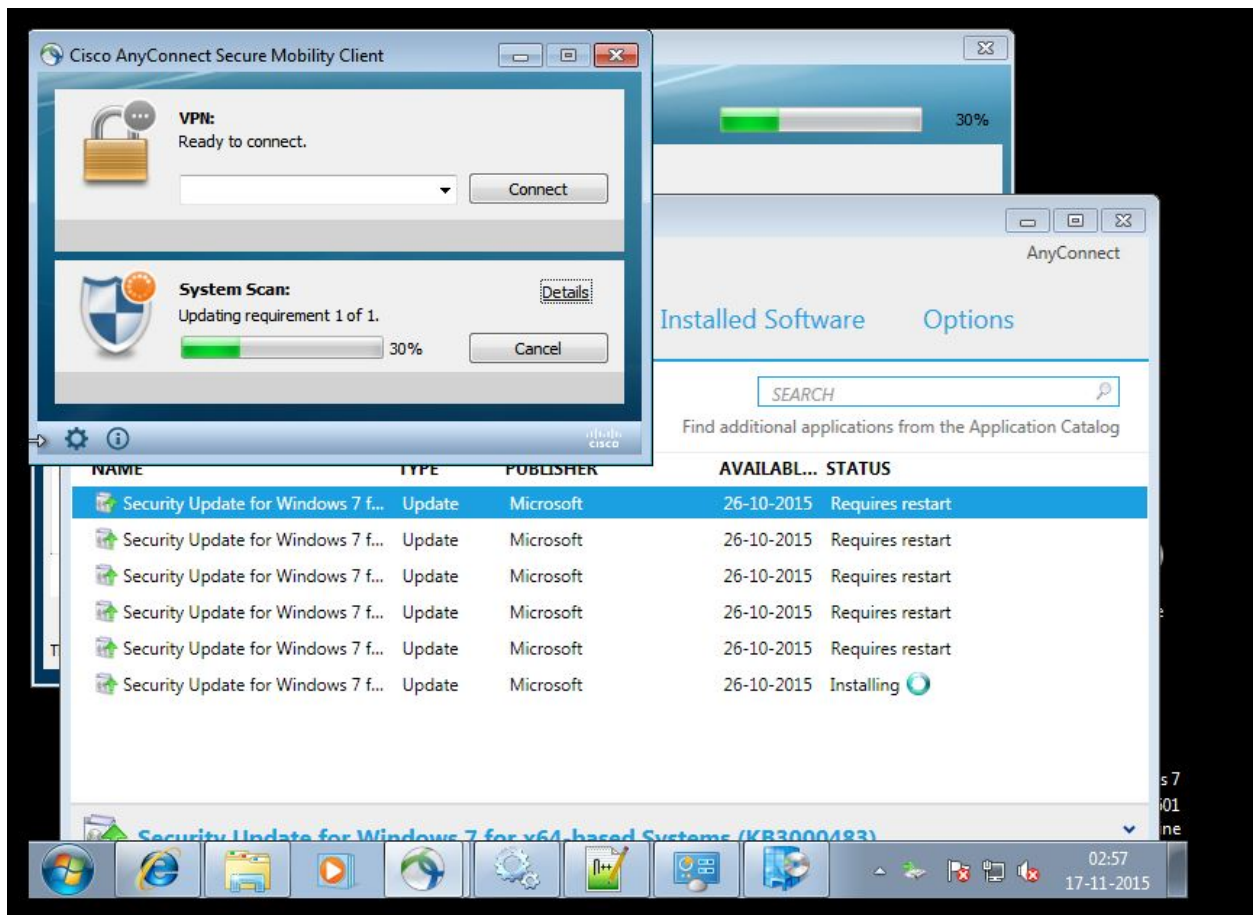


Figure 7: AnyConnect Remediation in progress

6. If a reboot is required after remediation to complete, please reboot the endpoint. Windows pop will show up on the taskbar indicating that a Reboot is required to update patches.

Note: Unless the system is rebooted the check for up-to-date patches will fail, and system scan will show Non-Compliant after the remediation timer expires, if reboot is still pending.

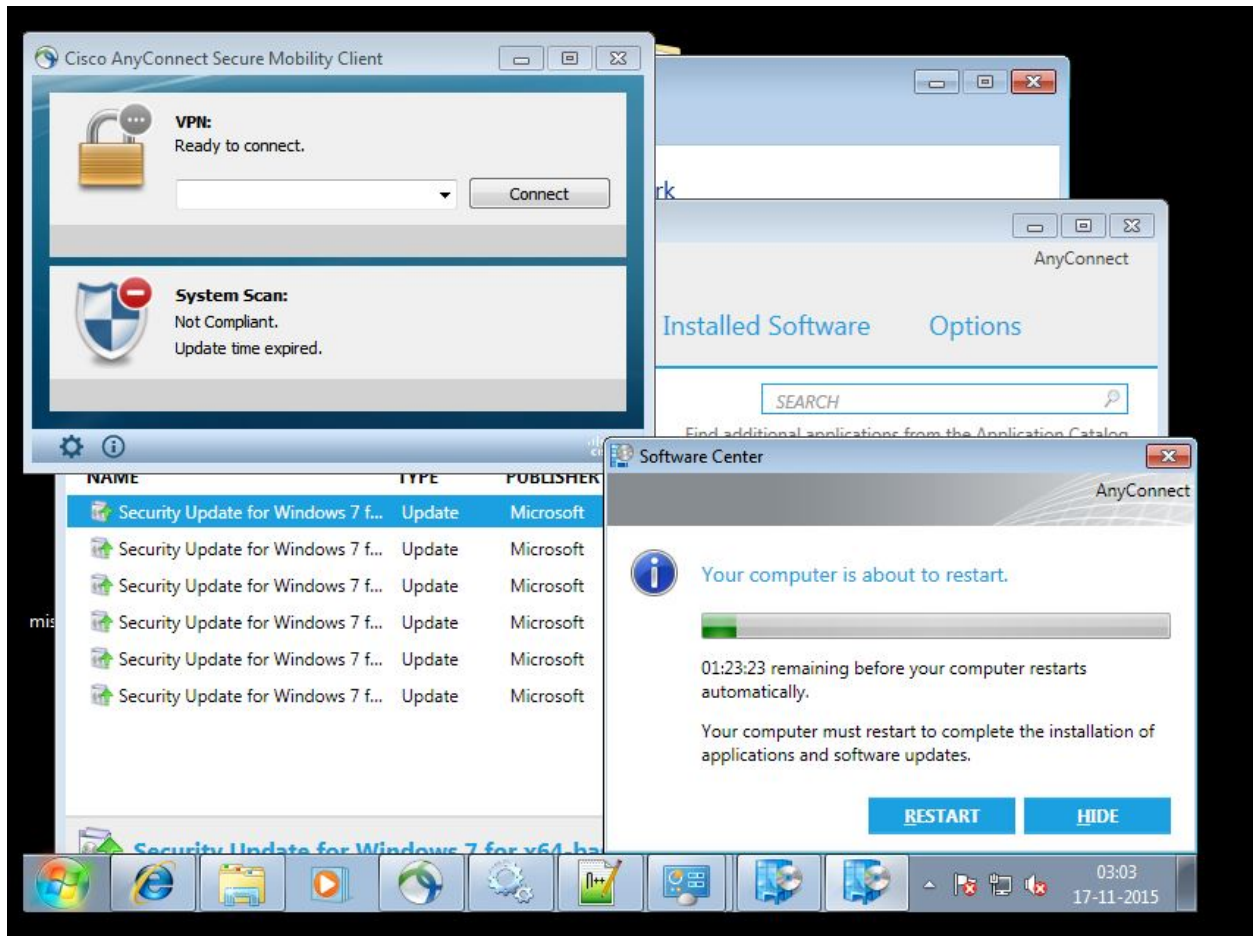


Figure 8: Requesting for windows reboot

After reboot, when Anyconnect connects back to NAD, it evaluates the PM condition for 'up-to-date' checks again and finds all patches required by SCCM installed on endpoint. At this point the Patch management condition passes and endpoint is deemed compliant. Please refer to screen shots below.

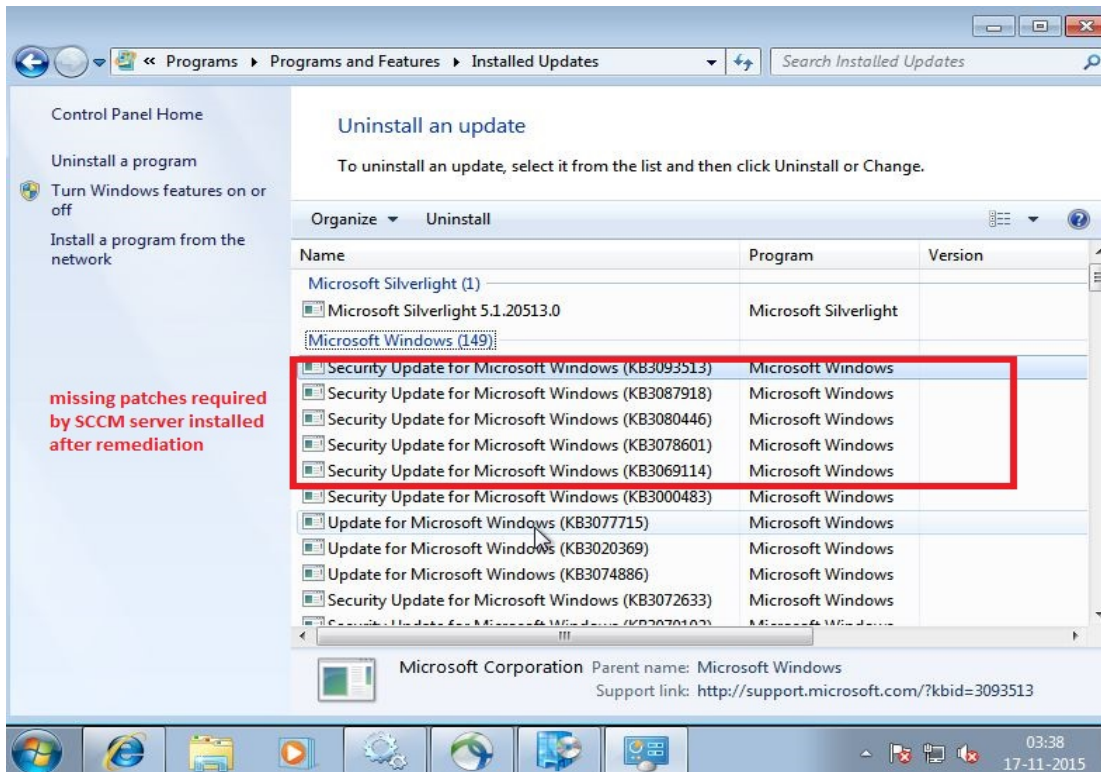


Figure 9: View of Installed Patches

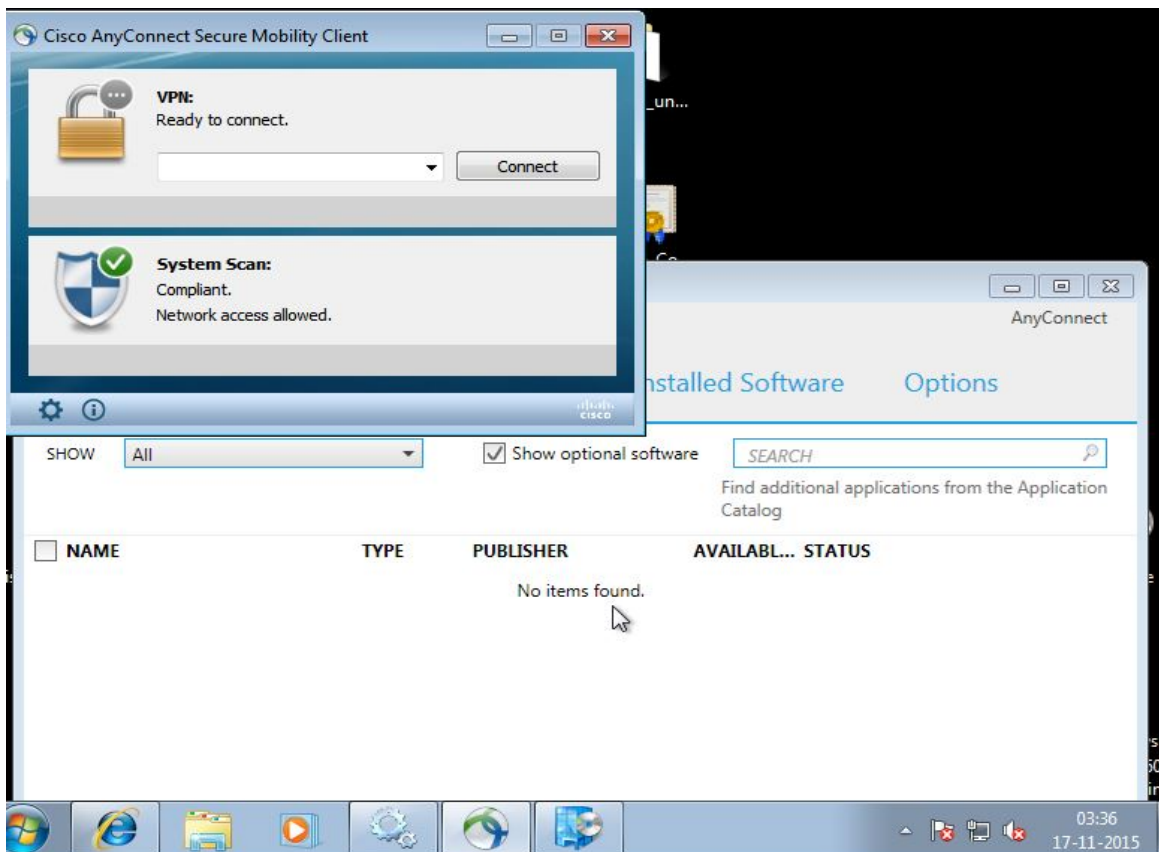


Figure 10: System Scan in Complaint state

5. Requirements

5.1 AnyConnect and ISE versions

Cisco AnyConnect Secure Mobility Client 4.1.x and Cisco Identity Services Engine 1.4.

Refer to below link to learn how to set up policy conditions on ISE

http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010010.html#task_A0E2F8D2BF5F4F2EA75B6E6E67CA393D

For further information on patch management remediation

http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_011110.html#reference_E6D05562981847AFAC2BCE9D1E4A22F8

5.2 SCCM

All supported versions of System Center Configuration Manager (SCCM) based on the support charts. From the link below you can view support charts for respective compliance module version. Its under NAC currently.

<http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html>

5.3 ISE Compliance Module

The support for Patch management remediation needs minimum ISE compliance module version of 3.6.10294.2. The ISE compliance modules can be downloaded from CCO as well as update from Perfigo public facing server.

The ISE administrator needs to deploy this ISE compliance module in the AnyConnect configuration on ISE to get it installed on the endpoint. Please refer to ‘System Scan’ administration guide for the configuration steps.

Admin guide for ISE

http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010010.html#task_A0E2F8D2BF5F4F2EA75B6E6E67CA393D

Admin guide for AnyConnect

http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect41/administration/guide/b_AnyConnect_Administrator_Guide_4-1/configure-posture.html