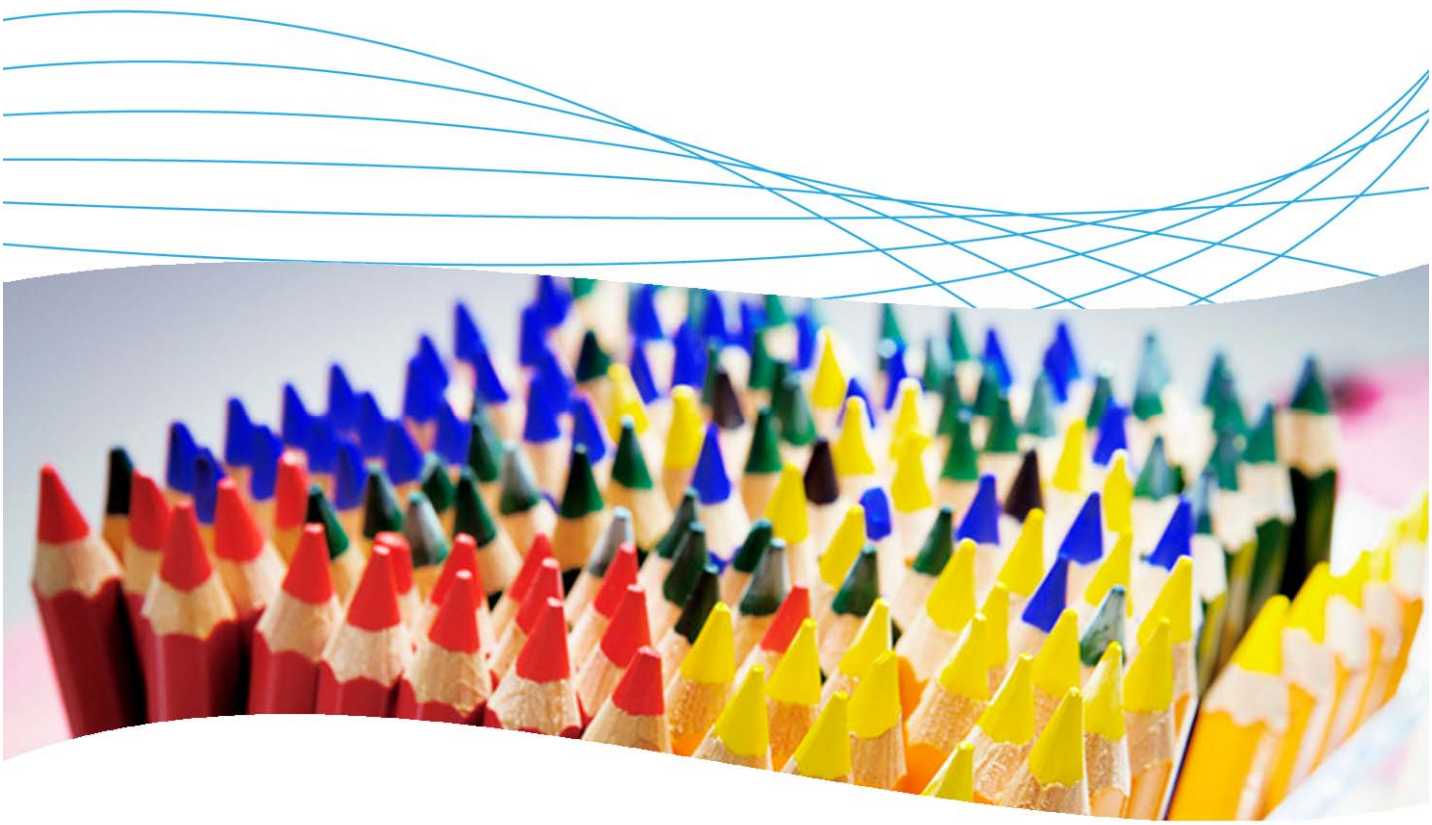
An HP ProCurve Networking Application Note

Integrating ProCurve IDM and Windows NAP



Contents

1. Introduction

This application note illustrates how to integrate a ProCurve network and ProCurve Manager and Identity Driven Manager (PCM and IDM) with Windows Server 2008. It focuses on Windows Network Access Protection (NAP), the policy enforcement platform built into Microsoft Windows Vista and Windows Server 2008.

2. Prerequisites

This procedure assumes you have an already configured Windows Server 2008 installed, along with PCM/IDM, and connected to a ProCurve Switch 5400zl.

3. Network and Active Directory tree diagrams

Figure 1 details the hardware configuration referenced in this section.

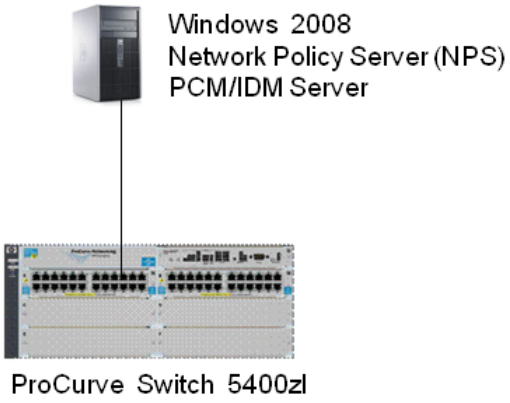


Figure 1. Setup for integrating PCM/IDM and Windows NAP

4. Microsoft NAP architecture

With Windows Server 2008, Microsoft introduced Network Access Protection (NAP). This client-server architecture has three layers, as in the Trusted Network Connect (TNC) model. (Figure 2 shows TNC components in black, NAP in red.)

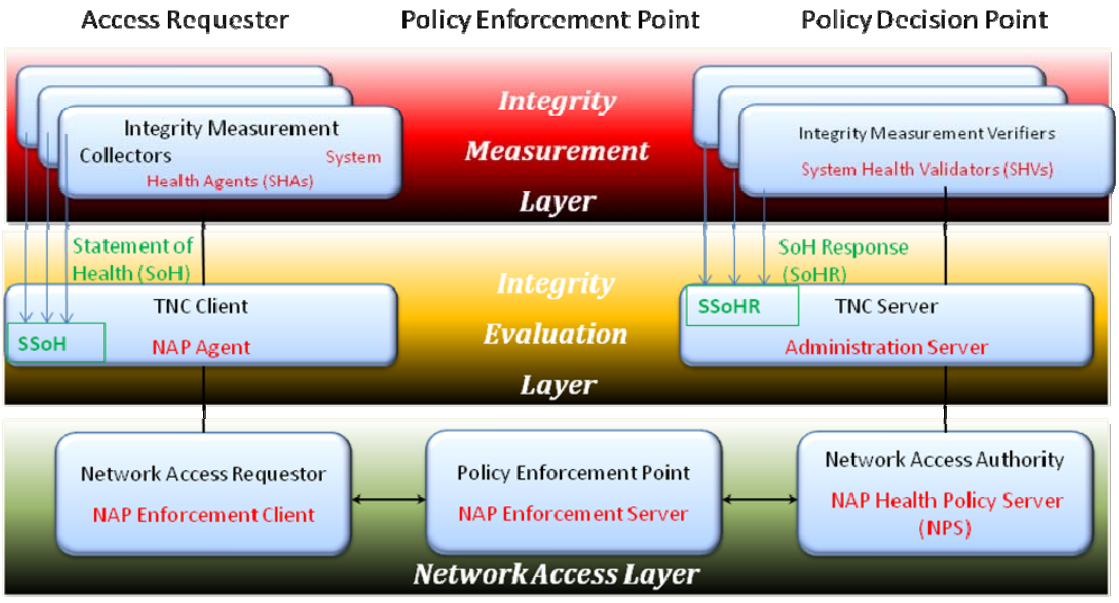


Figure 2. TNC and NAP

- **Integrity Measurement Layer**: This corresponds to the different tests that can be enforced on the endpoint and validated by the server; for example, antivirus test, Windows update test, and so forth. It contains, on the client side, the System Health Agents (SHAs) that collect health information. A built-in Windows SHA is available for Windows Vista and Windows XP SP3. Their counterparts on the server are the System Health Validators, which validate the health state provided by SHAs.

- **Integrity Evaluation Layer**: This corresponds to the security policy, the result of a set of tests done by the SHAs and SHVs. The NAP Agent coordinates and exchanges information between the SHA and Enforcement Client. The NAP Agent is available on Windows 2008, Vista, and XP SP3, and does continuous monitoring for ongoing policy enforcement. On the server side, the Administration Server coordinates and exchanges information between SHVs and the NAP Policy Server (NPS).

- **Network Access Layer**: This layer contains on the client side the NAP Enforcement Client (EC)—one for each connection mechanism (IPSec, DHCP, VPN, TS Gateway, 802.1X)—and handles access requests based on connection type. Its counterpart on the server is the NAP Enforcement Server. The NPS Service (RADIUS) receives information from the Enforcement Server, authenticates user identity and extracts system health information, and evaluates the validated health state for policy conformance. The NAP Enforcement Server enforces specific access capabilities specified by the NPS.

These different elements uses several types of messages to communicate:

- **Statement of Health (SoH)**: Defines the state of the monitored component. Created by SHA and passed to NAP Agent.
- **System SoH (SSoH)**: Complete set of SoHs from all SHAs. Packaged by Agent and sent by Enforcement Client to NPS through the Enforcement Server.
- **SoH Response (SoHR)**: Can be healthy/unhealthy Response based on SoH claim.
- **System SoHR (SSoHR)**: Complete set of SoHRs from all SHVs. Packaged by Administration Server for evaluation by NPS.

5. Configuration procedure

This section illustrates an example configuration procedure.

5.1 Add the NPS Server role on your Windows 2008 Server

To add the NPS Server role on your Windows 2008 Server:

1. Click Start, and then click Server Manager.
2. Under Roles Summary, click Add Roles, and then click Next.
3. Select the Network Policy and Access Services check box, and then click Next twice.
4. Select the Network Policy Server check box, click Next, and then click Install.

5.2 Install the IDM Agent

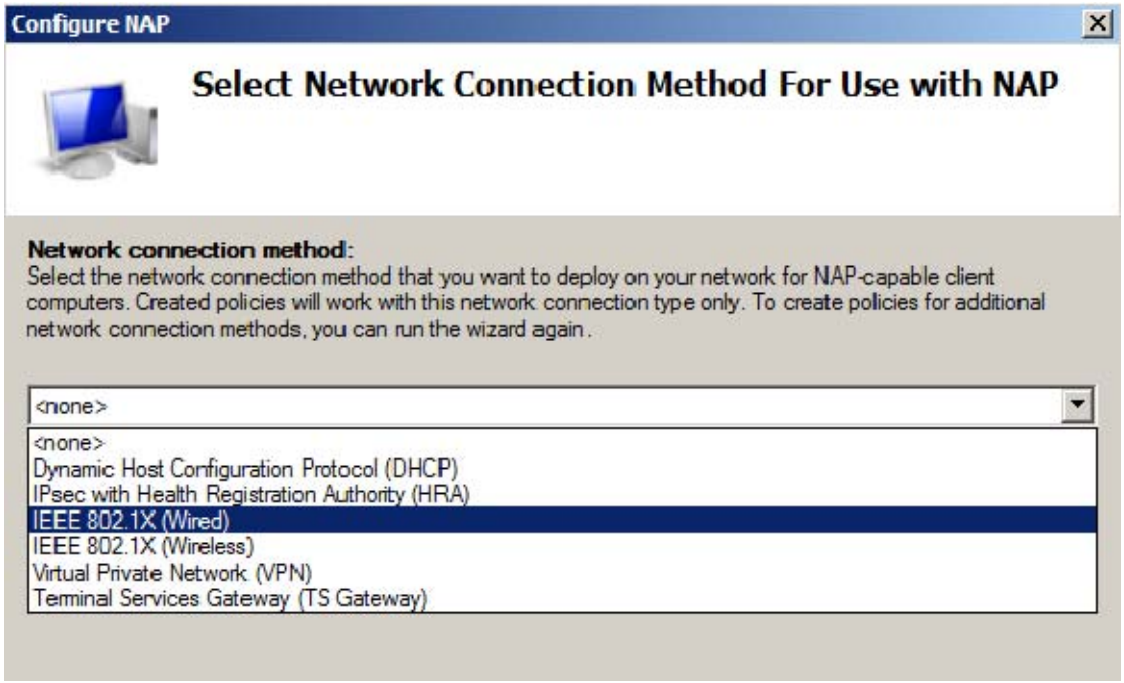
Install the IDM Agent from http://server-ip:8040. This operation must be performed on the client.

5.3 Configure an NPS policy

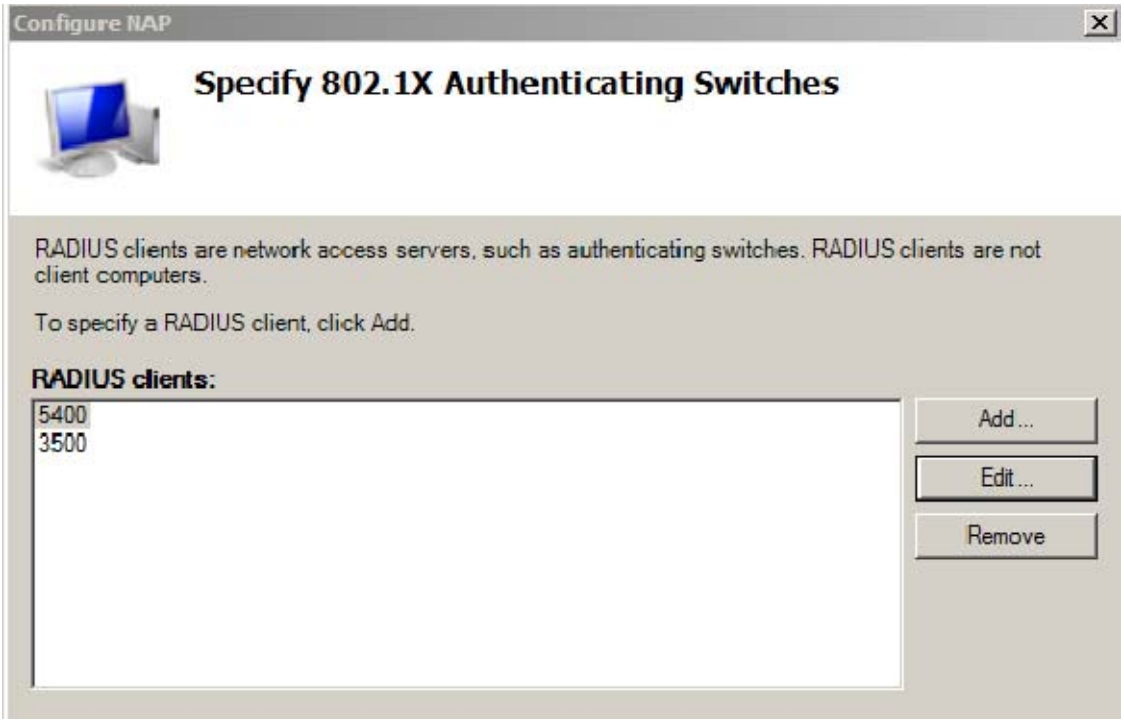
To configure an NPS policy:

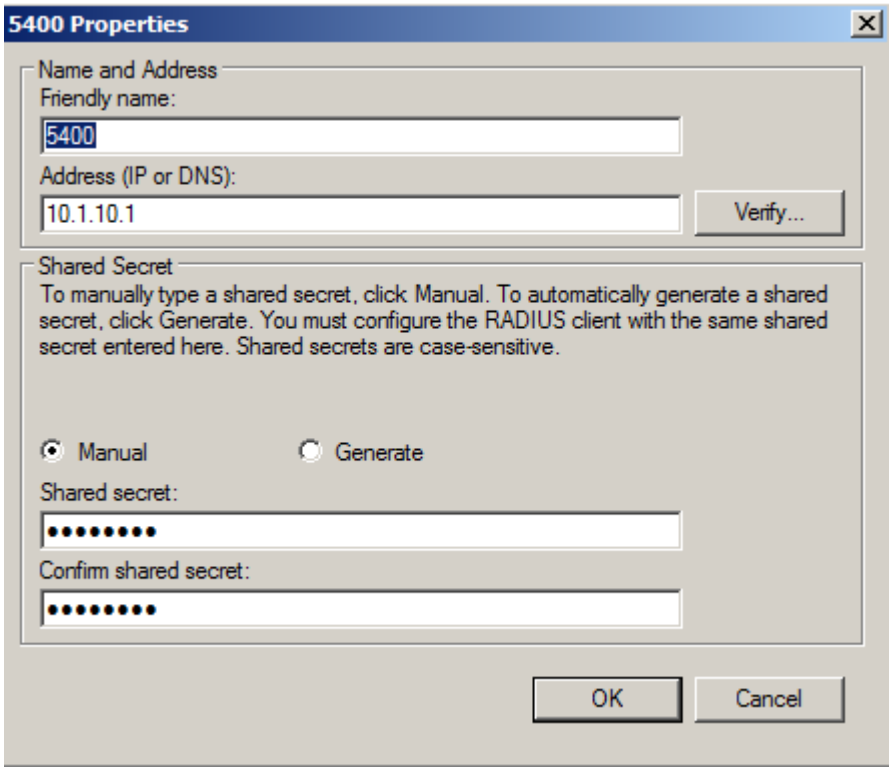
1. From the Start Menu | Administrative Tools, open Network Policy Server.

2. In the Getting Started window, click on Configure NAP to launch the NAP Configuration Wizard.
3. Choose a network connection method. In this case, the method is IEEE 802.1X Wired. Assign a name to this method (or simply leave the default name).



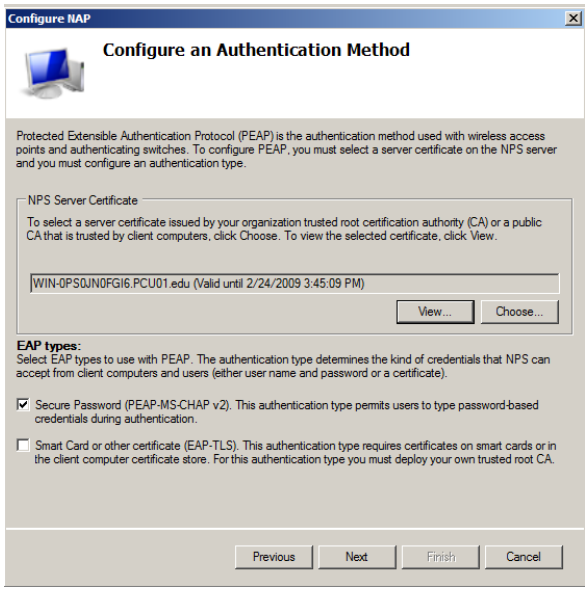
4. Configure the RADIUS clients (that is, the 802.1X authenticating switches). This is similar to IAS configuration on Windows 2003: you specify the IP address of the equipment and the shared secret.



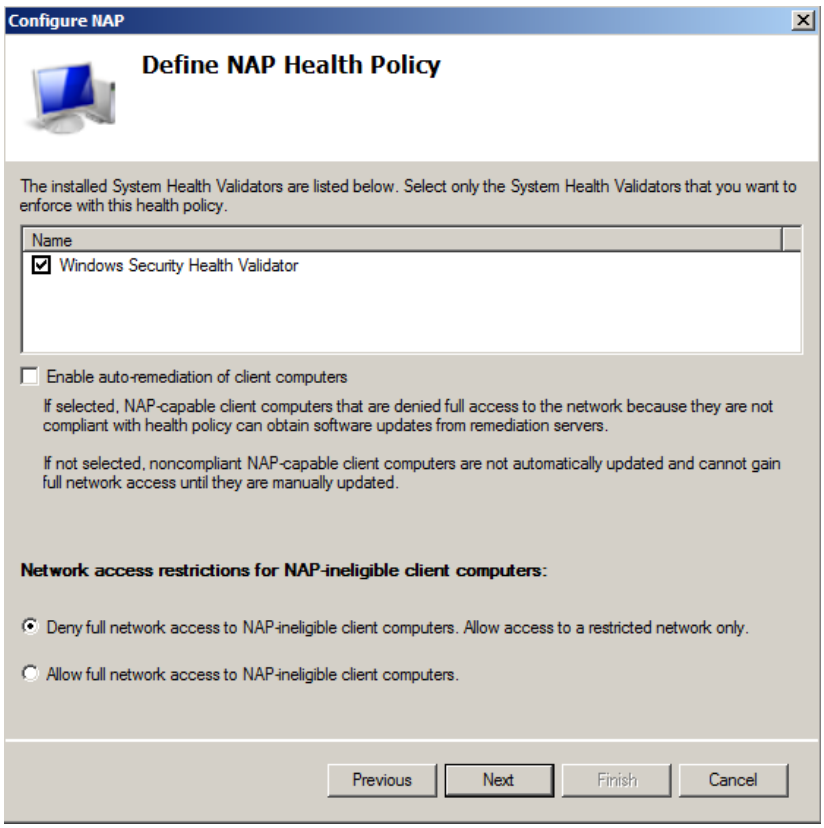


5. On the next screen you can configure users and/or machine groups. In this example, user configuration is done in Identity Driven Manager. So you can skip this step.

6. On the next screen you configure an authentication method. This step is also similar to Windows 2003/IAS configuration: You select the NPS Server Certificate (if it is not already there), and the EAP type (Secure Password or Smart card or certificate).

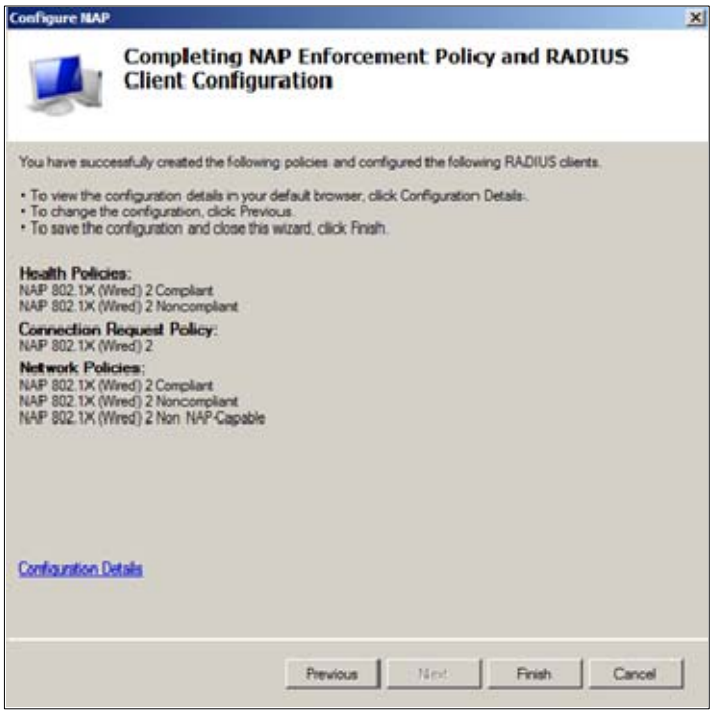


7. The next screen gives you the opportunity to configure VLANs using RADIUS attributes: an organization VLAN for users who have passed the endpoint integrity tests, and a restricted network VLAN. Since IDM will allocate the VLANs within the Access Profiles, you don't need to configure them under NPS. So skip this step.
8. Then you define the NAP Health Policy—that is, the set of tests that will be checked on the clients. In this example, the only available SHV is the built-in Windows Security Health Validator.



On this screen you also decide whether to enable auto-remediation on NAP-capable client computers (leave it unchecked for purposes of this example), and whether non-NAP-capable clients will be allowed or denied access to the network.

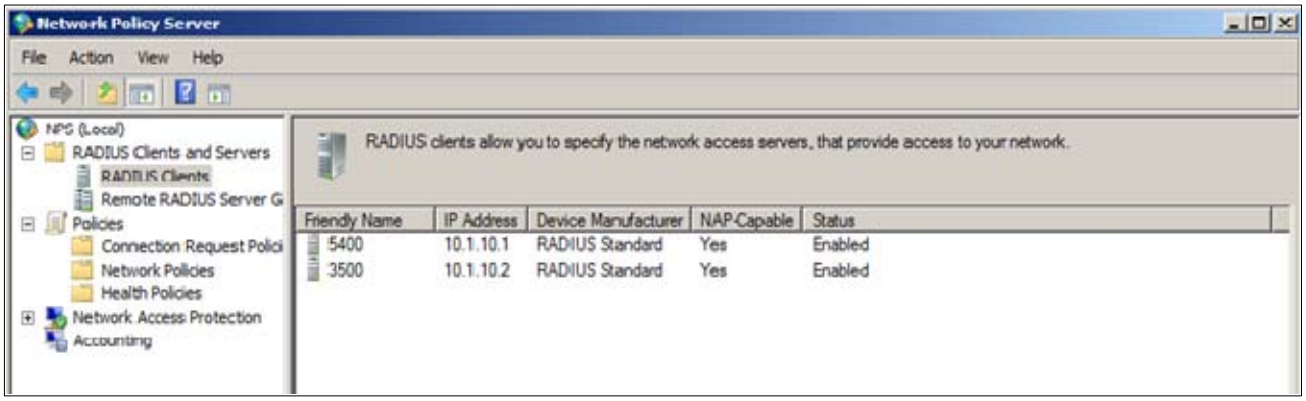
9. Finally you see a summary of the different Health, Connection Request and Network Policies that have been defined:



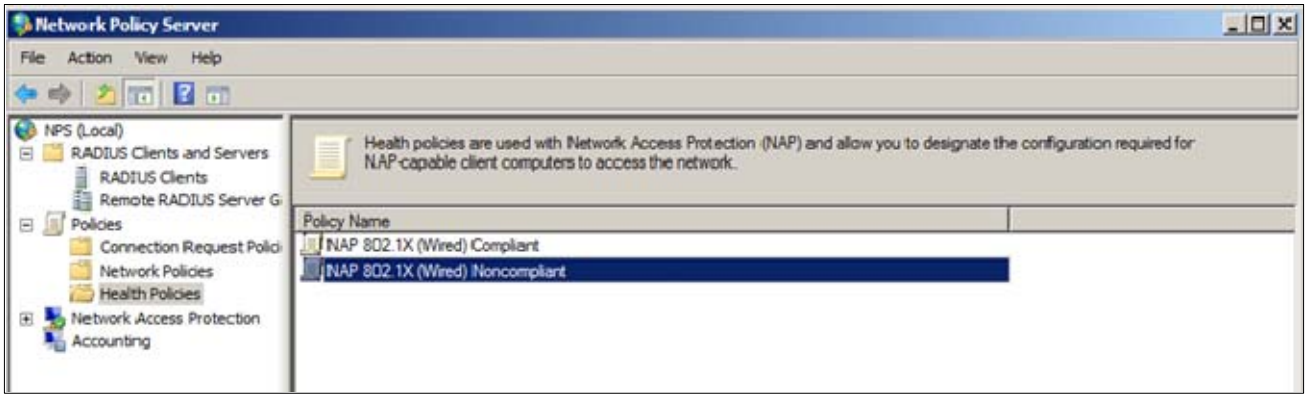
5.4 Finish configuring NPS

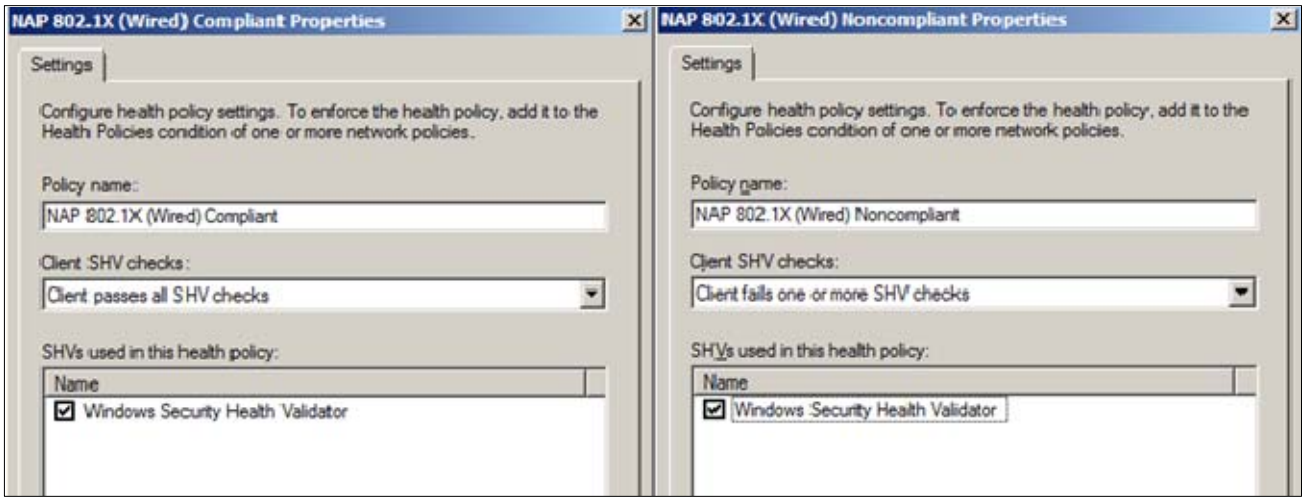
Once the policy has been created, you still have a few steps to complete in NPS:

1. Go to RADIUS Clients and Servers | RADIUS Clients, edit the clients, and configure them as NAP-Capable.



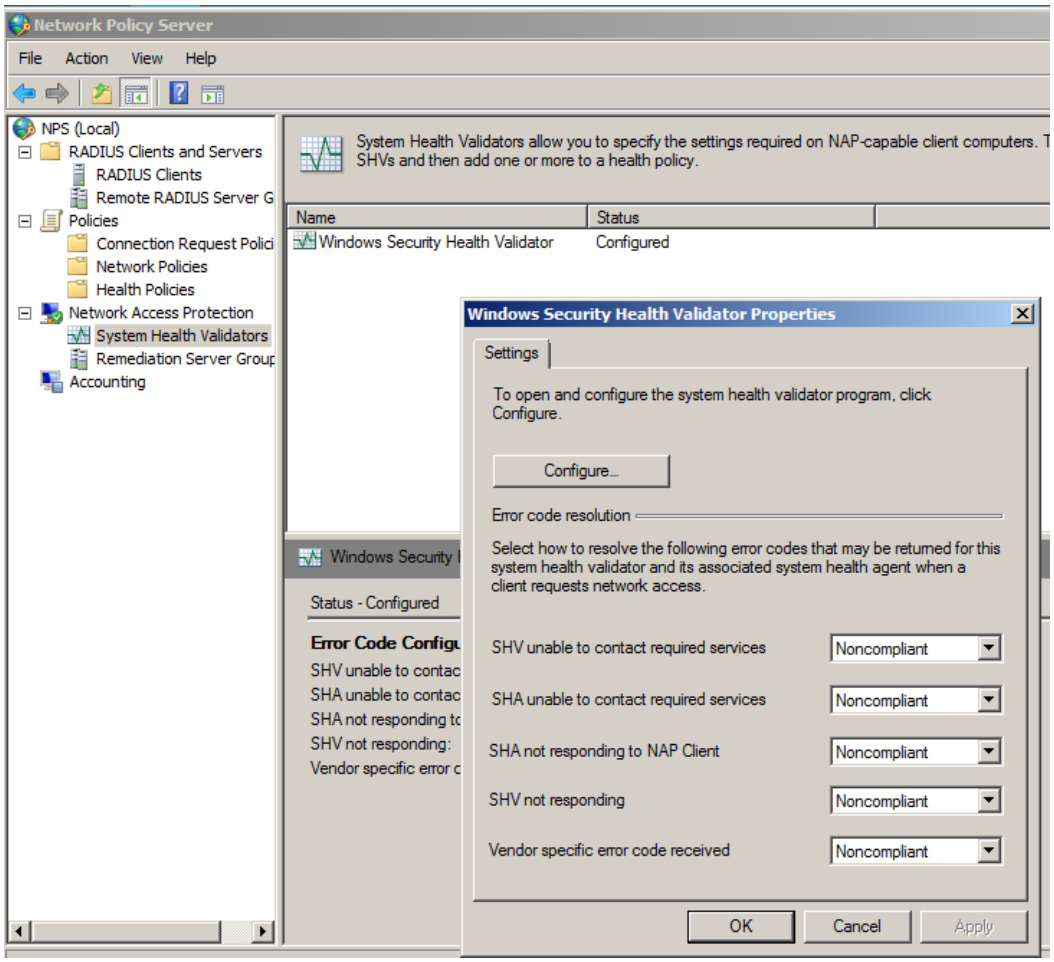
2. Go to Policies | Health Policies. You have two Policies: NAC 802.1X (Wired) Compliant and NAC 802.1X (Wired) Noncompliant. Edit both and check the conditions for the SHV. Specify the Client SHV checks as:
    - Client passes all SHV checks for the Compliant policy.
    - Client fails one or more SHV checks for the NonCompliant policy.





3. In Network Access Protection, edit the Windows Security Health Validator. On the Settings tab, click on Configure. You obtain, for Windows Vista and Windows XP, the list of tests that the Windows SHV performs on the endpoints:
    - **For Windows Vista**: Firewall, Antivirus protection, Spyware protection, Automatic Updating, Security Updates Protection
    - **For Windows XP (SP3)**: Same except no Spyware protection

    For this example, uncheck everything except the Firewall test, so the SHAs will only check if a firewall is enabled on the client.



5.5 Define an IDM policy

This example illustrates defining a simple IDM policy, with two groups of users: Marketing and Finance.

Identity Management Configuration:

- Locations: none
- Times: none
- Network Resources:
- Marketing Intranet: tcp 81 on 10.1.10.10
- Finance Intranet: tcp 82 on 10.1.10.10

Access Profiles:

Access Profile	VLAN	QoS	Bandwidth	Network Resources
Marketing	20	Don't override	Don't override	Deny Finance Intranet Permit any
Finance	30	Don't override	Don't override	Deny Marketing Intranet Permit any
NonCompliant	40	Don't override	Don't override	Deny Marketing Intranet Deny Finance Intranet Permit any

Access Policy Groups:

Finance and Marketing groups have been synchronized with Active Directory.

Finance: user jane

Location	Time	System	WLAN	Endpoint Integrity	Access Profile
ANY	ANY	ANY	ANY	PASS	Finance
ANY	ANY	ANY	ANY	FAIL	NonCompliant

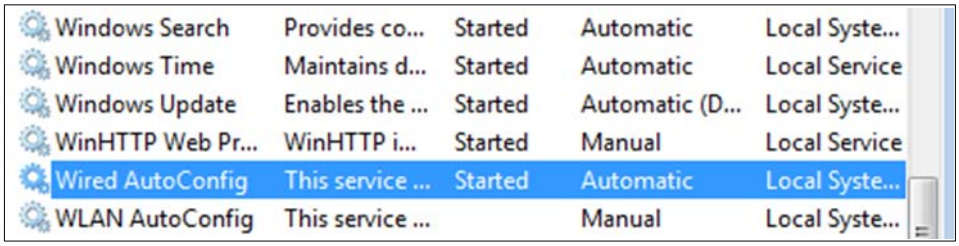
Marketing: user john

Location	Time	System	WLAN	Endpoint Integrity	Access Profile
ANY	ANY	ANY	ANY	PASS	Marketing
ANY	ANY	ANY	ANY	FAIL	NonCompliant

6. Configuring the Vista client

The configuration of a Vista client is quite similar to the configuration of an XP client. With Vista, however, there are some additional considerations:

- In order to enable authentication to a port-authenticator (and obtain the Authentication tab on the client), the Wired AutoConfig service must be started. (Under Windows XP, it was the Wireless Zero Config service, for both wired and wireless.)



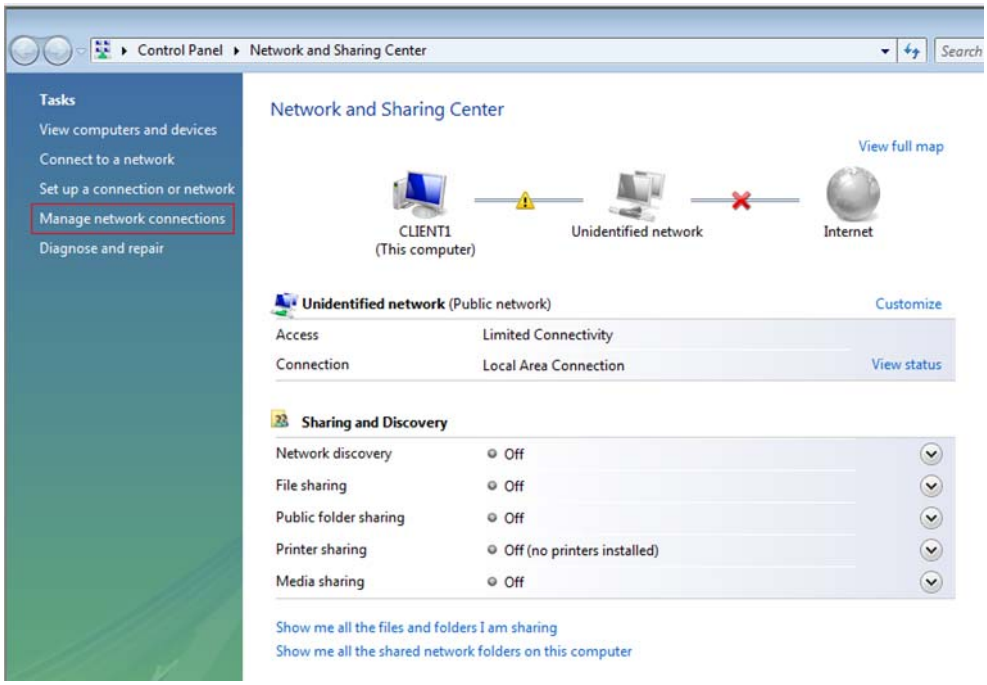
- For the Endpoint Integrity tests, the Network Access Protection Agent service must be also be started.

Before configuring the Vista client, check that these two services are started on the client machine. You can define a Group Policy on the domain to automatically start these services on each computer. For more information on how to configure it, please refer to the *NAP_802.1X_StepByStep.doc* document, available from Microsoft.

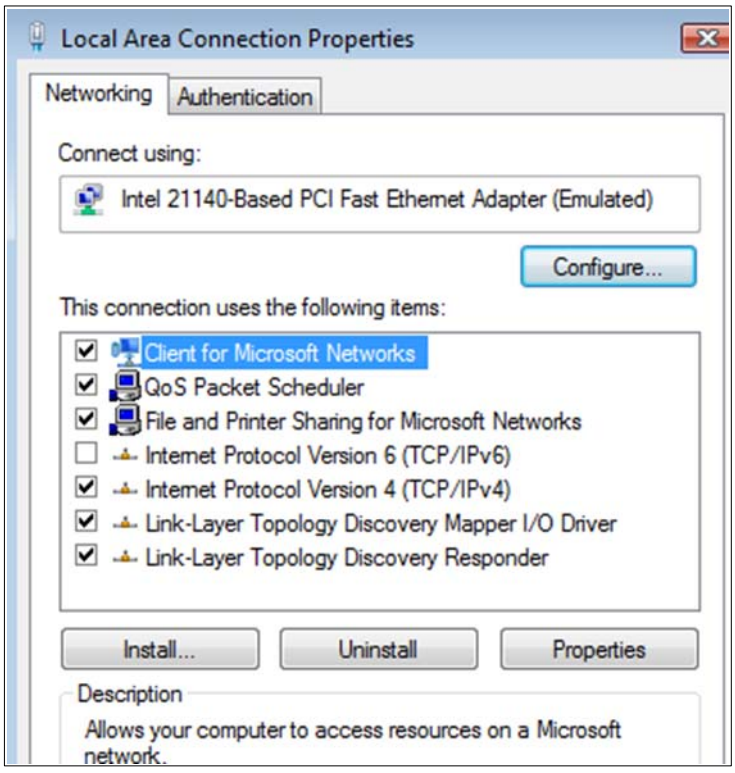
6.1 Configure the Vista client

To access the Network Connections under Vista:

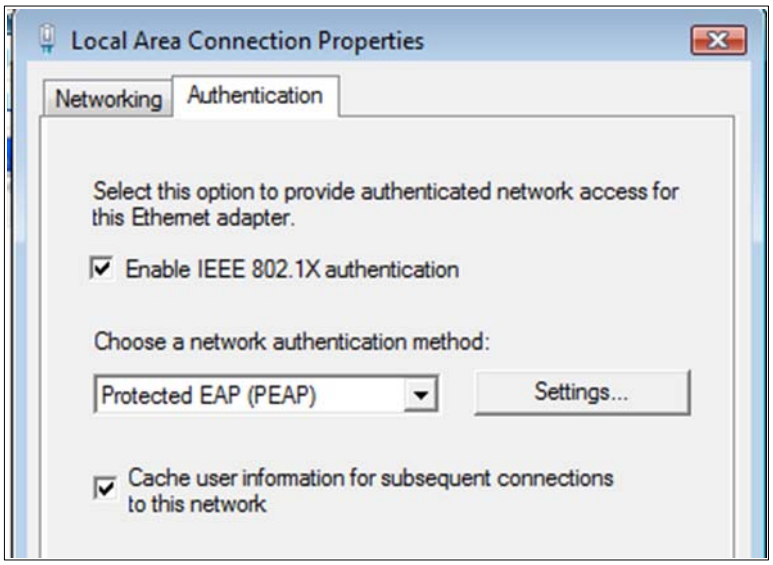
1. From the Start Menu go to Network.
2. In Network, choose Network and Sharing Center:



3. From there, click on Manage Network Connections. You obtain the list of your connections.
4. Right-click on your LAN connection and choose Properties, then choose the Network tab.
5. On the Network tab, disable IPv6:

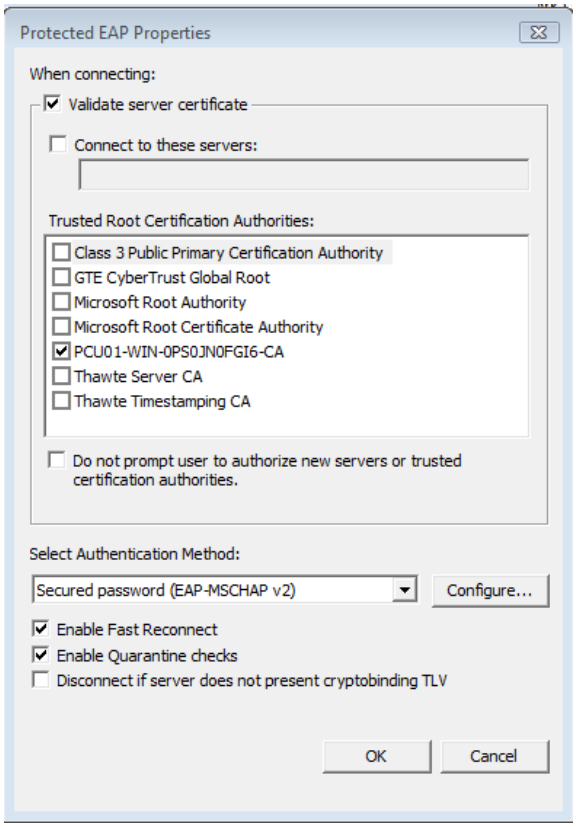


6. On the Authentication tab, enable IEEE 802.1X and choose Protected EAP as the network authentication method:

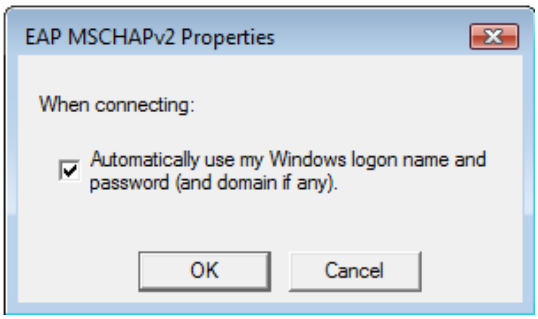


7. Click on Settings to configure the PEAP properties. Put a check mark in the Validate server certificate box, choose the server certificate from your certification authority, and select EAP-MSCHAPv2 as the authentication method.

   Then click Configure.



8. In the EAP MSCHAPv2 Properties box, select Automatically use my Windows logon name and password, and click OK.

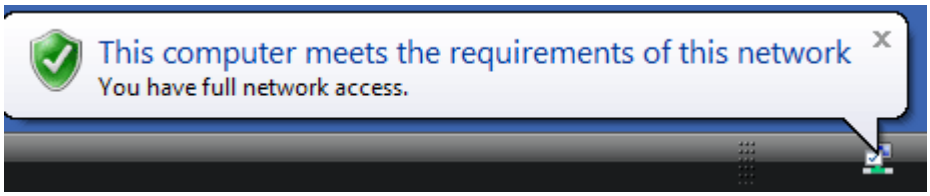


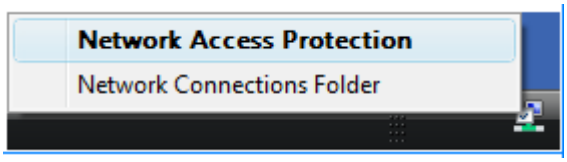
9. In the Protected EAP Properties window, select Enable Fast Reconnect and Enable Quarantine Checks. Click on OK twice.

6.2 Show authentication in the Vista client

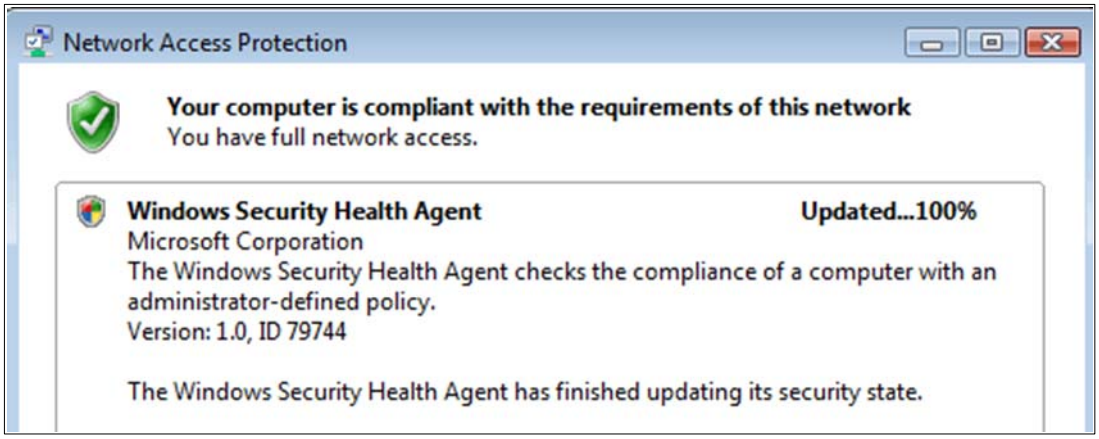
To show an authentication from the Vista Client:

1. Start a Windows 2008 Server image.
2. Plug the Vista client into a port authenticator and log on as john/hp. (Log off your Vista session and log on again if you were logged as another user). You should obtain the following message:





3. If you click on this message, or if you right-click on the icon and choose Network Access Protection, you obtain more details:



7. Reference documents

This concludes the procedure for integrating ProCurve IDM and Windows NAP.

For further information about how to configure ProCurve switches and ProCurve IDM to support security, please refer to the following links:

- For the *ProCurve Identity Driven Manager User's Guide* for Software Release 2.3:
  http://cdn.procurve.com/training/Manuals/IDM_UG-59908851-0508.pdf

- For other PCM+ and IDM manuals:
  http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm
  http://www.hp.com/rnd/support/manuals/IDM.htm

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches:
  http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm

- For ProCurve Switch 2610 series manuals:
  http://www.hp.com/rnd/support/manuals/2610.htm

For further information, please visit www.procurve.eu

4AA2-1625EEE, July 2008