

# What is NAP?

- **NAP stands for Network Access Protection.**
- **NAP is used to evaluate the “health” of a computer and compare it against a corporate policy to determine what level of access that computer can have to the network.**
- **If a computer does not meet the requirements to access the internal network it can be sent to a remediation network to give it the opportunity to fix its health status (sometimes automatically).**

# NETWORK ACCESS PROTECTION

Network Access Protection (NAP) is a technology that allows you to restrict network access on the basis of a client's health. System Health Agents (SHAs) and System Health Validators (SHVs) are the components that validate a computer's health against a configured set of benchmarks.

# NAP Enforcement Types – IPSEC, 802.1S, VPN, DHCP

- **IPSec** If you don't meet the requirement then you are not connected
  - **Requires clients to meet health requirements before connecting to IPSec protected hosts.**

IPsec enforcement works by applying IPsec rules. Only computers that meet health Compliance requirements are able to communicate with each other. IPsec enforcement can be applied on a per-IP address, per-TCP port number, or per-UDP port number basis.

IPsec enforcement applies after computers have received a valid IP address, either from DHCP or through static configuration. IPsec is the strongest method of limiting network Access communication through NAP.

To deploy IPsec enforcement, a network environment must have a Windows Server 2008 or 2008 R2 Health Registration Authority (HRA) and a Windows Server 2008 or Windows Server 2008 R2 CA. Clients must be running Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, or Windows XP SP3

## 802.1x (Wired or Wireless)

- **Complete control over access to the network!**

If you don't meet the requirement you can be sent to a remediation network

If you meet the requirements you are allowed into the network. Flexibility

802.1X enforcement uses authenticating Ethernet switches or IEEE 802.11 Wireless Access Points. These compliant switches and access points grant unlimited network access only to computers that meet the compliance requirement. Computers that do not meet the Compliance requirement are limited in their communication and are sent to a Remediation network where they will get the necessary updates. Once the client is ok A certificate of Health is received and the client can join the network.

A computer running Windows Server 2008 or Windows Server 2008 R2 with the Network Policy Server role is necessary to support 802.1X NAP enforcement. It is also necessary to have switch or Wireless Access Point hardware that is 802.1X-compliant. Clients must be running Windows 7, Windows Vista, Windows Server 2008 R2, Windows Server 2008, or Windows XP SP3.

- **VPN** Allows you to control access for remote clients. Gives filtering and control.
  - **Controls access from remote clients.**

VPN enforcement is used on connecting VPN clients as a method of ensuring that clients granted access to the internal network meet system health compliance requirements. VPN enforcement works by restricting network access to noncompliant clients through the use of packet filters. Rather than being able to access the entire network, incoming VPN Clients that are noncompliant have access only to the remediation server group.

If a noncompliant client becomes compliant, packet filters restricting network access will be removed. VPN enforcement requires an existing remote access Infrastructure and an NPS server. The enforcement method uses the VPN EC, which is Included with Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

- **DHCP**

- **Allows only compliant computers to receive IP addresses.**

DHCP NAP enforcement works by providing unlimited-access IPv4 address information to compliant computers and limited-access IPv4 address information to noncompliant computers.

To deploy DHCP NAP enforcement, you must use a DHCP server running Windows Server 2008 or Windows Server 2008 R2 because this includes the DHCP Enforcement Service (ES). The DHCP EC is included in the DHCP Client service on Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

# SHAs and SHVs

- **System Health Agents (SHAs)** → Resides on the client computer
  - **The client component which validates the health of a client computer and creates a SoH to be sent to the SHV.** Statement of Health
  - **Requires Vista, Server 2008, or XP with Service Pack 3** Server 2008R2, Windows 7
- **System Health Validators (SHVs)**
  - **The server component which analyzes the information presented by the SHA and produces a SoHR which is then used by the policy server to determine the level of access to be granted.**  
Statement of Health Response

# Health Requirement Policies

It is the Health Requirement policies that are going to determine who or what types of clients meet certain requirements, what those certain health requirements are, and what you are going to do about it if they do not meet those requirements.

- **Health requirement policies are made up of the following:**
  - **Connection request policy** Determines whether or not the policy will be processed
  - **System health validators** Used to check whether the client has actually met the requirements
  - **Remediation server group** Group of servers used to correct the Health Status of clients
  - **Health policy** Defines the actual Health Requirements needed for access using the SHV settings for Compliant and non-compliant clients
  - **Network policy**  
Defines the level of network access clients will get based on Whatever policy they match



## EXAMPLE SETTING UP DHCP ENFORCEMENT

1. Check to make sure that the DHCP Role is added and functioning
2. Check to make sure that Network Policy Server role is added
3. Open Network Policy Server from Administrative Tools

**NPS (Local)**

- RADIUS Clients and Servers
- Policies**
- Network Access Protection
- Accounting

### Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

#### Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

#### Network Access Protection (NAP)

When you configure NPS as a NAP policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

[Configure NAP](#) [Learn more](#)

#### Advanced Configuration


Network Policy Server Configure NAP NY-DLT-2N8

File Action View

← → [Calendar] [?] [NPS (Local)]

- [-] [Folder] RADIUS Client
- [-] [Document] Policies
- [-] [Network Access] Network Access
- [-] [Accounting] Accounting

## Select Network Connection Method For Use with NAP




**Network connection method:**  
Select the network connection method that you want to deploy on your network for NAP-capable client computers. Created policies will work with this network connection type only. To create policies for additional network connection methods, you can run the wizard again.

Dynamic Host Configuration Protocol (DHCP)

**Policy name:**  
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.

NAP DHCP

**Additional requirements:**  
 You must perform additional actions to set up NAP. View additional NAP requirements by clicking on the link below.  
[Additional Requirements](#)



## Specify NAP Enforcement Servers Running DHCP Server

RADIUS clients are network access servers, not client computers. If the local computer is running DHCP Server, you can skip this step and click Next.

If you want to add remote DHCP servers as RADIUS clients, click Add. All remote DHCP servers that you add must also run NPS. Also, remote DHCP/NPS servers must forward connection requests to this NPS server (the local computer).

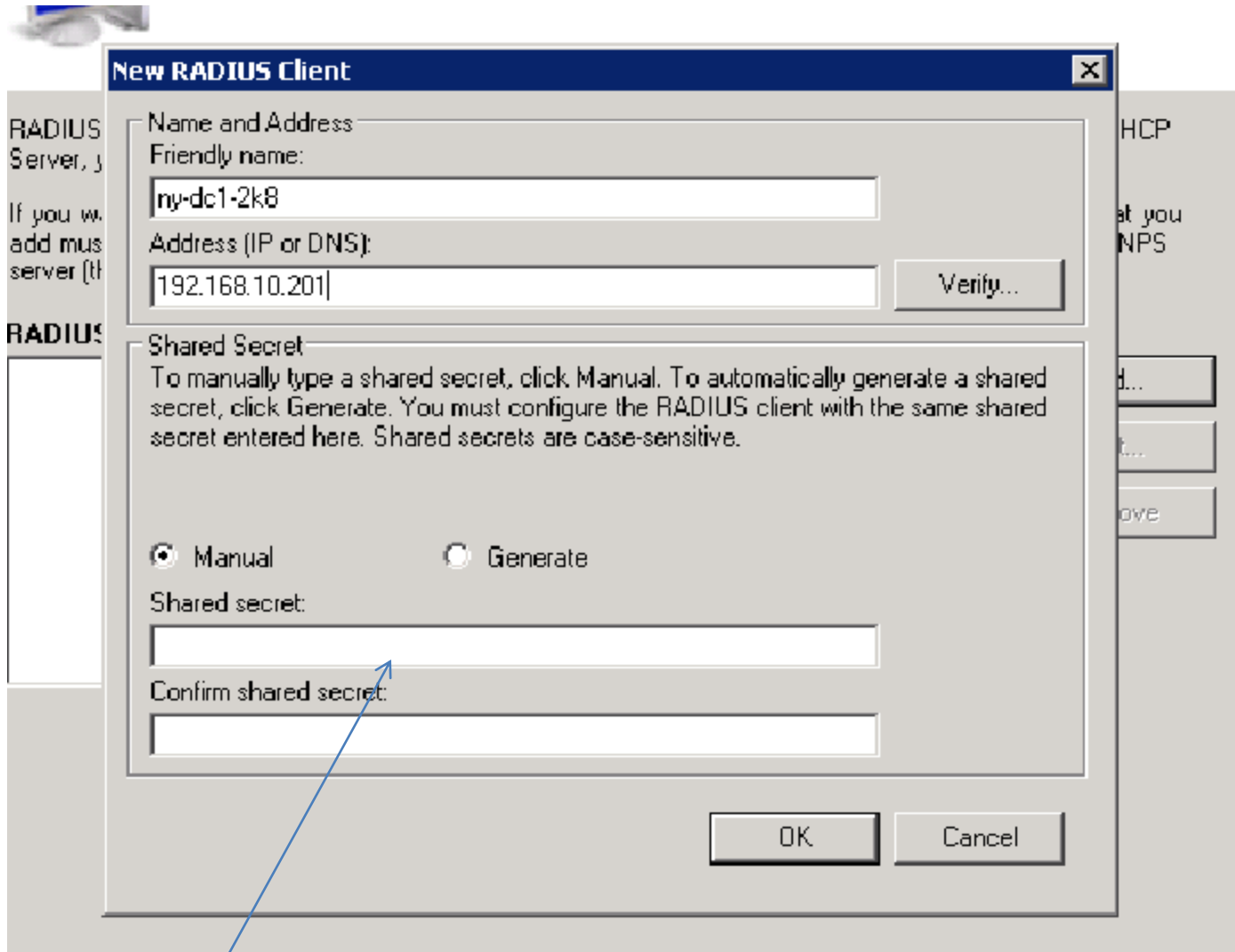
### RADIUS clients:

You need to add the DHCP Servers on your network  
That will participate in DCHP enforcement

Add...

Edit...

Remove



Shared secret not necessary here- only when you are setting up Radius



## Specify NAP Enforcement Servers Running DHCP Server

RADIUS clients are network access servers, not client computers. If the local computer is running DHCP Server, you can skip this step and click Next.

If you want to add remote DHCP servers as RADIUS clients, click Add. All remote DHCP servers that you add must also run NPS. Also, remote DHCP/NPS servers must forward connection requests to this NPS server (the local computer).

### RADIUS clients:

ny-dc1-2k8

Add...

Edit...

Remove

Although it says Radius clients this is your DHCP Server



## Specify DHCP Scopes

When you specify one or more NAP-enabled scopes, NPS evaluates client health and performs authorization for client computers requesting an IP address from the designated scopes.

If you do not specify any scopes, the policy applies to all NAP-enabled scopes at the selected DHCP servers. If you specify a scope that is not NAP-enabled, you must enable NAP for the scope after completing this wizard.

To specify one or more scopes, click Add.

**DHCP scopes:**

Add...

Edit...

Remove

If you wanted to use specific scopes you could add them here but since you are using all the scopes just go ahead and leave this blank



If you wanted to specify certain groups of computers that you could apply this to, then you could do this here, if you leave it blank then it just goes to everybody.

The screenshot shows the 'Configure NAP' window in Network Policy Server (NPS). The window title is 'Configure NAP' and it has a yellow background. The main content area is titled 'Specify a NAP Remediation Server Group and URL' and features a computer icon. The left sidebar shows the NPS (Local) tree with folders for RADIUS Client, Policies, Network Access, and Accounting. The main area contains the following text:

**Remediation Server Group:**  
Remediation servers store software updates for NAP clients that need them. Remediation Server Groups contain one or more remediation servers.

Select a Remediation Server Group that you have already configured or, to create a new group, click **New Group**.

A dropdown menu shows '<none>' and a 'New Group...' button is visible with a mouse cursor pointing to it.

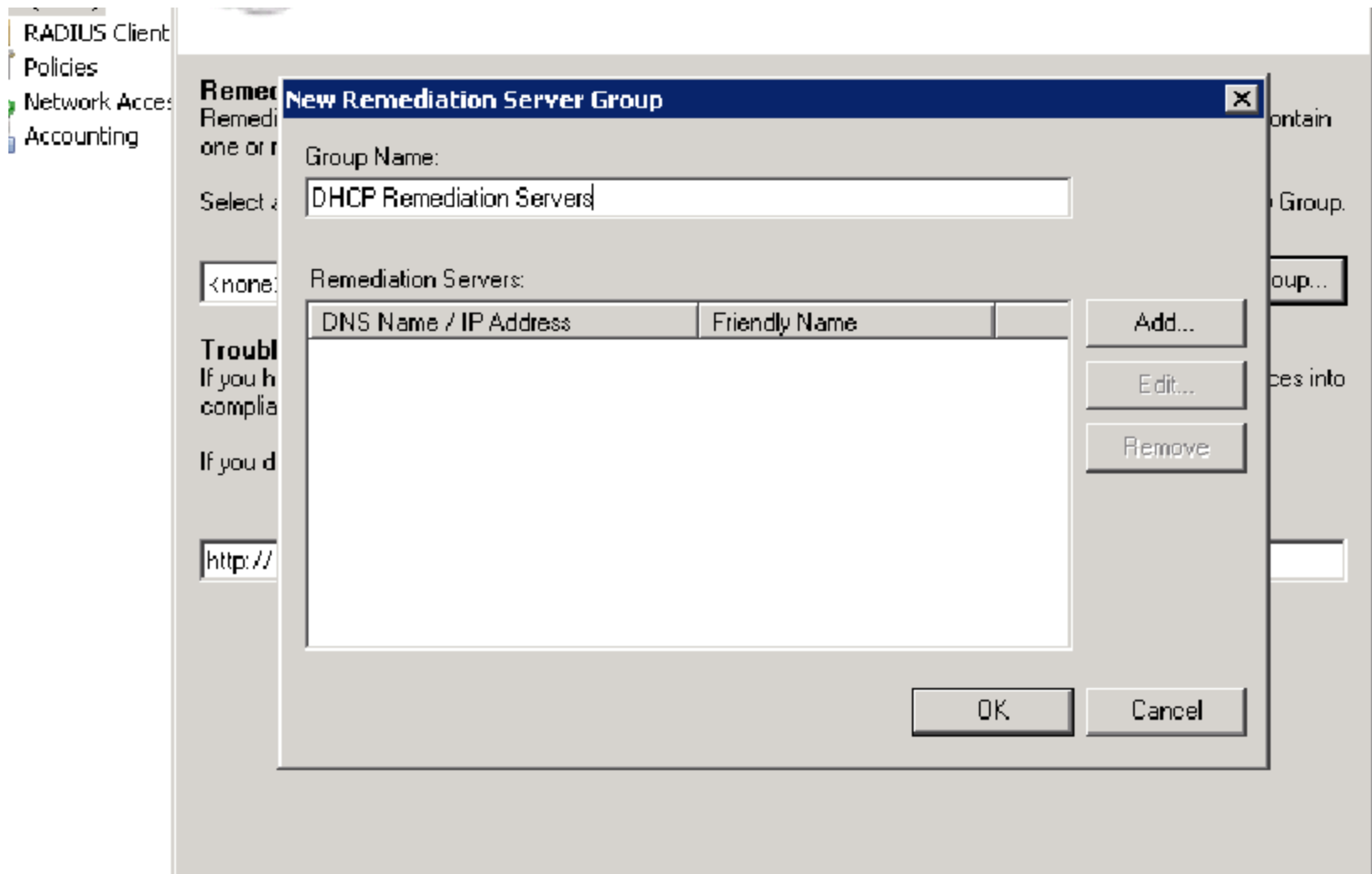
**Troubleshooting URL:**  
If you have a Web page that provides users with instructions to users on how to bring computers and devices into compliance with NAP health policy, type the Uniform Resource Locator (URL) for the Web page.

If you do not have a Help Web page, do not type a URL.

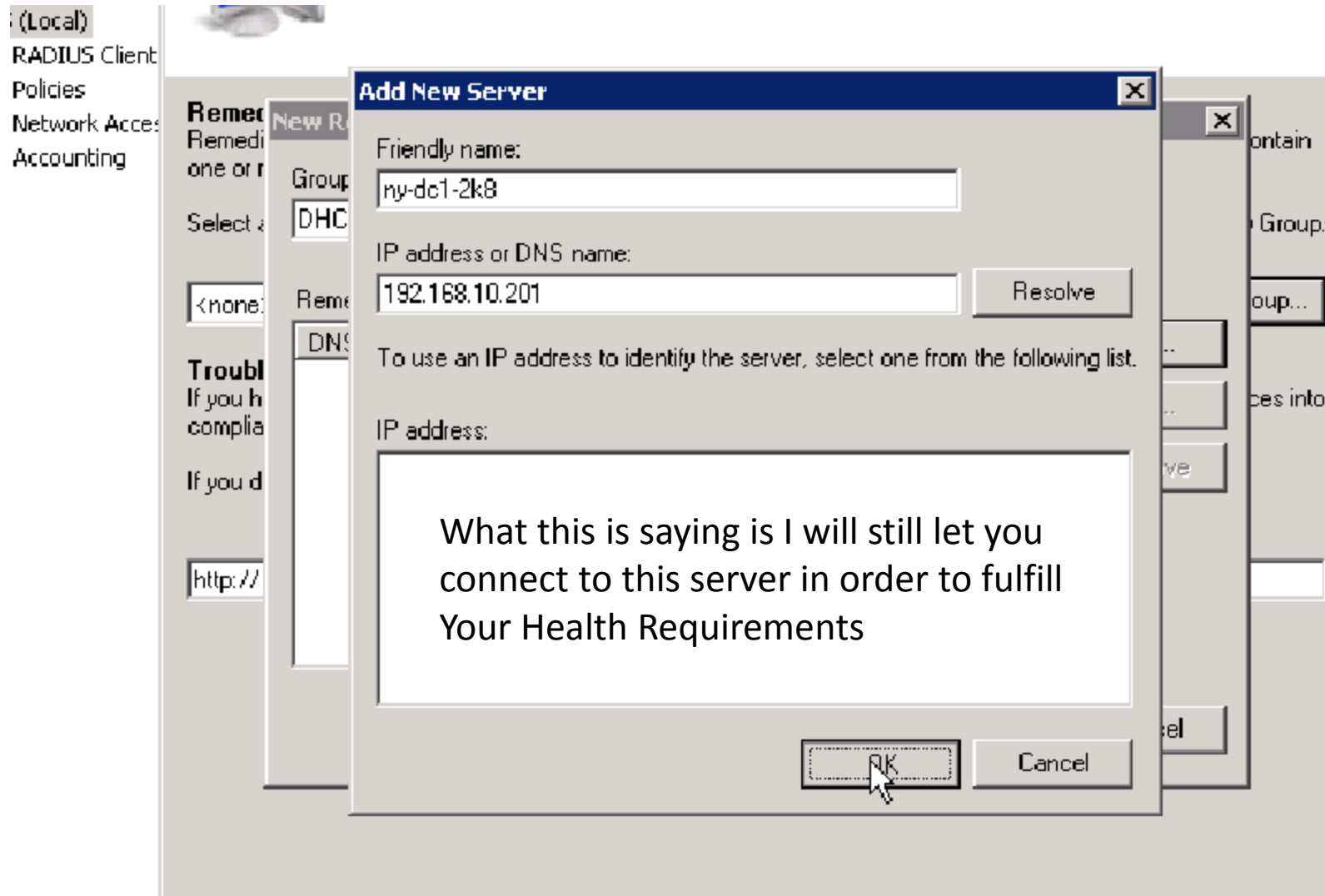
A text input field contains 'http://'.

Here you can choose a NAP remediation Server or group to allow the client to still gain access in an effort to correct its Health Requirement shortcomings





Type in the Group name and click Add



Type in a friendly name and the IP address of the server

### Remediation Server Group:

Remediation servers store software updates for NAP clients that need them. Remediation Server Groups contain one or more remediation servers.

Select a Remediation Server Group that you have already configured or, to create a new group, click New Group.

DHCP Remediation Servers

New Group...

### Troubleshooting URL:

If you have a Web page that provides users with instructions to users on how to bring computers and devices into compliance with NAP health policy, type the Uniform Resource Locator (URL) for the Web page.

If you do not have a Help Web page, do not type a URL.

http://

Here is where you could put the address of a web page that would be presented to the users with instructions on what to do to get themselves in compliance with the policy.

Previous

Next

Finish

Cancel

Action View



PS (Local)

RADIUS Client

Policies

Network Access

Accounting



## Define NAP Health Policy

The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.

Name
<input checked="" type="checkbox"/> Windows Security Health Validator

Enable auto-remediation of client computers

If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.

If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.

### Network access restrictions for NAP-ineligible client computers:


Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.

Allow full network access to NAP-ineligible client computers.

You have successfully created the following policies and configured the following RADIUS clients

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

**RADIUS clients:**

ny-dc1-2k8 (192.168.10.201) 

**Health Policies:**

NAP DHCP Compliant

NAP DHCP Noncompliant

**Connection Request Policy:**

NAP DHCP

**Network Policies:**

NAP DHCP Compliant

NAP DHCP Noncompliant

NAP DHCP Non NAP-Capable

**Remediation Server Group:**

DHCP Remediation Servers

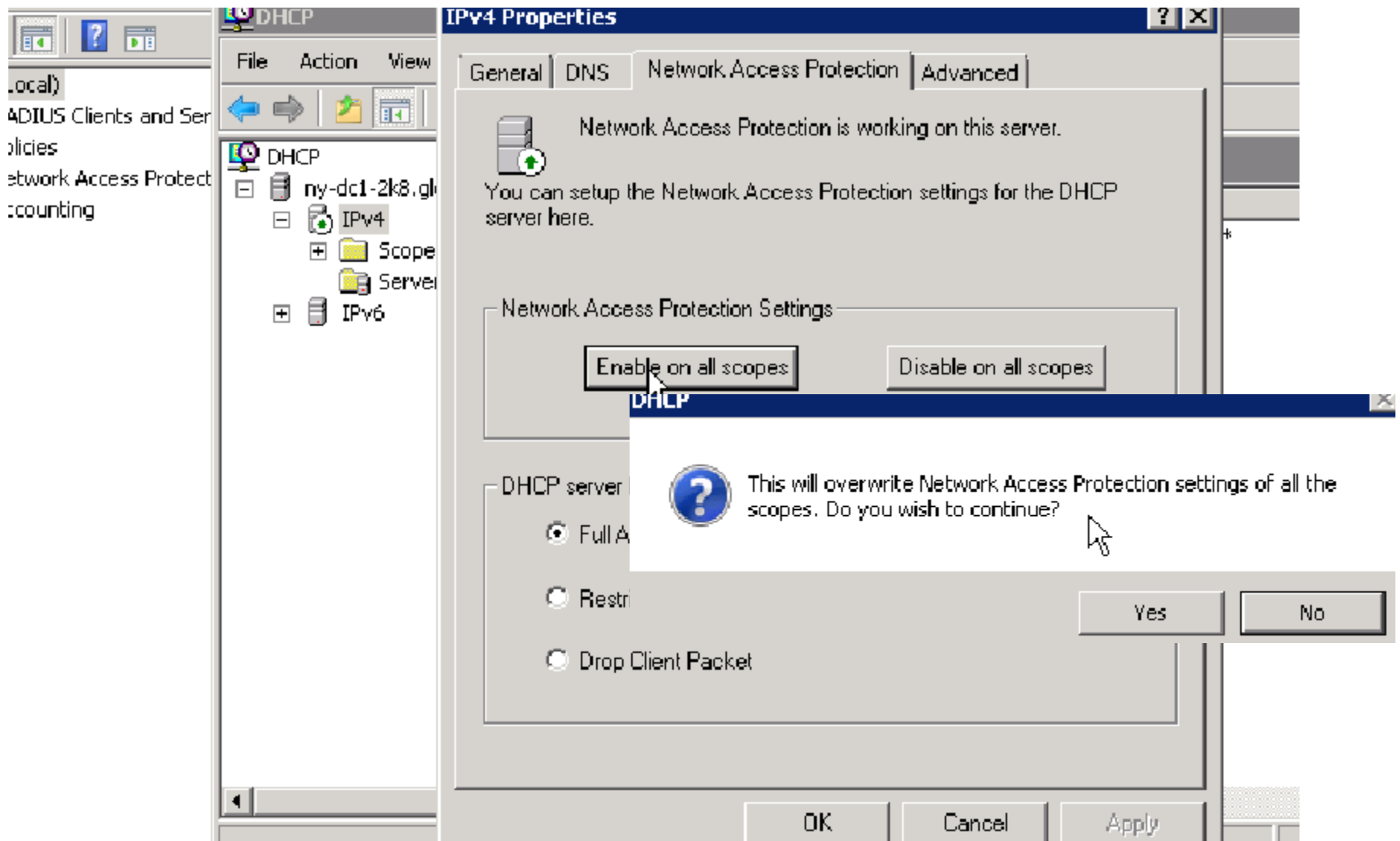
[Configuration Details](#)

Previous

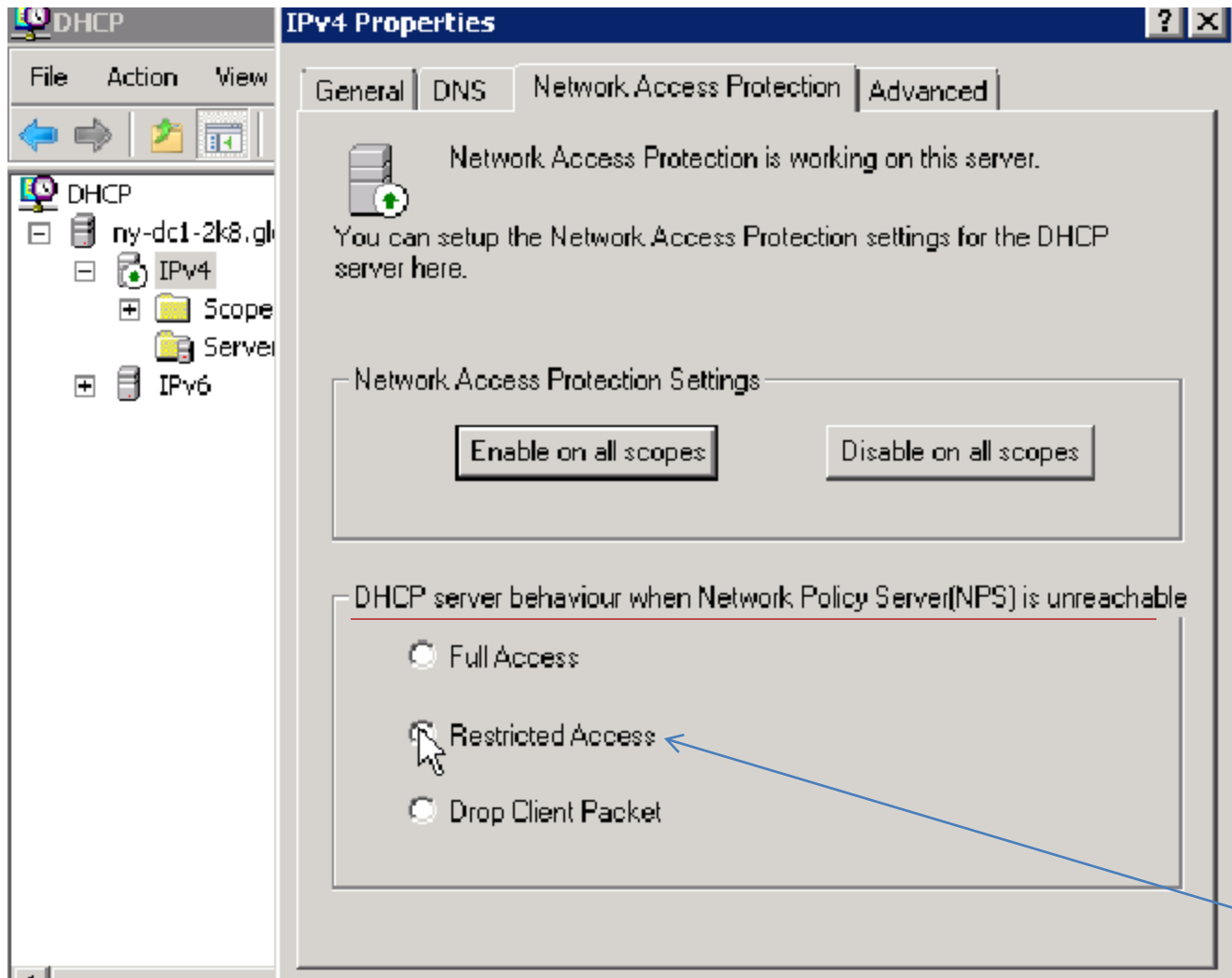
Next

Finish

Now that you have set up the NAP policies you need to go to the DHCP Server and Enable NAP



Right click on IPV4, click on properties and select the Network Access Protection tab.  
The click on Enable on all scopes, click on Yes to overwrite settings



Close out of DHCP and now you have to set up setting for the clients through Group Policy

Go into Group Policy Management and Edit the Default Domain Group Policy. Computer Configuration, Policies, Windows Settings, Security Settings, Network Access Protection, NAP client configuration, Enforcement Clients

The screenshot displays the Group Policy Management console. The left pane shows the tree structure: Computer Configuration > Policies > Windows Settings > Security Settings > Network Access Protection > NAP Client Configuration > Enforcement Clients. The right pane is titled "Enforcement Clients" and contains a table with the following data:

Name	Status
DHCP Quarantine Enforcement Client	Disabled
Remote Access Quarantine Enforcement Client	Disabled
IPSec Relying Party	Disabled
TS Gateway Quarantine Enforcement Client	Disabled
EAP Quarantine Enforcement Client	Disabled

Below the table, the "DHCP Quarantine Enforcement Client" is selected, and its properties are shown:

- ID: 79617
- Name: DHCP Quarantine Enforcement Client
- Description: Provides DHCP based enforcement for NAP
- Version: 1.0
- Vendor: Microsoft Corporation
- Status: Disabled



Right click and enable

Default Domain Policy [NY-DC1-2K8.globomantics.com] Poli

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
      - Local Policies
      - Event Log
      - Restricted Groups
      - System Services
      - Registry
      - File System
      - Wired Network (IEEE 802.3) Policies
      - Windows Firewall with Advanced Security
      - Network List Manager Policies
      - Wireless Network (IEEE 802.11) Policies
      - Public Key Policies
      - Software Restriction Policies
      - Network Access Protection
        - NAP Client Configuration
          - Enforcement Clients
          - User Interface Settings
          - Health Registration Settings
      - ID Security Policies on Active Directory

### Enforcement Clients

Name	Status
DHCP Quarantine Enforcement Client	Enabled
Remote Access Quarantine Enforcement Client	Disabled
IPSec Relying Party	Disabled
TS Gateway Quarantine Enforcement Client	Disabled
EAP Quarantine Enforcement Client	Disabled

---

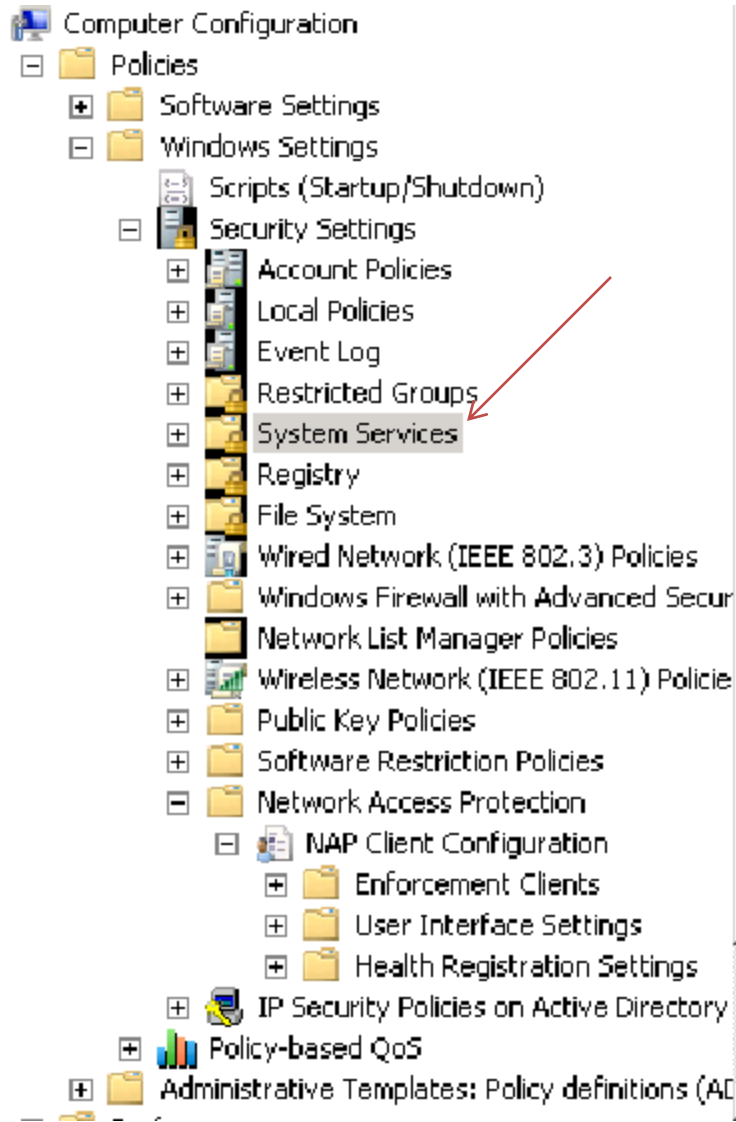
#### DHCP Quarantine Enforcement Client

ID: 79617

Name: DHCP Quarantine Enforcement Client

Description: Provides DHCP based enforcement for NAP

Version: 1.0



Microsoft .NET Framework ...	Not Defined	Not Defined
Microsoft Fibre Channel Plat...	Not Defined	Not Defined
Microsoft iSCSI Initiator Ser...	Not Defined	Not Defined
Microsoft Software Shadow...	Not Defined	Not Defined
Multimedia Class Scheduler	Not Defined	Not Defined
Netlogon	Not Defined	Not Defined
Network Access Protection Agent	Not Defined	Not Defined
Network Connections	Not Defined	Not Defined
Network List Service	Not Defined	Not Defined
Network Location Awareness	Not Defined	Not Defined
Network Policy Server	Not Defined	Not Defined
Network Store Interface Se...	Not Defined	Not Defined
Offline Files	Not Defined	Not Defined
Performance Logs & Alerts	Not Defined	Not Defined
Plug and Play	Not Defined	Not Defined
PnP-X IP Bus Enumerator	Not Defined	Not Defined
Portable Device Enumerator...	Not Defined	Not Defined
Print Spooler	Not Defined	Not Defined
Problem Reports and Soluti...	Not Defined	Not Defined
Protected Storage	Not Defined	Not Defined
Remote Access Auto Conne...	Not Defined	Not Defined
Remote Access Connection ...	Not Defined	Not Defined
Remote Procedure Call (RPC)	Not Defined	Not Defined
Remote Procedure Call (RP...	Not Defined	Not Defined
Remote Registry	Not Defined	Not Defined
Resultant Set of Policy Prov	Not Defined	Not Defined

Default Domain Policy [NY-DC1-2K8.globomantics.com] Poli


Service Name	Startup	Permis
Remote Procedure Call (RPC)	Not Defined	Not De

Computer Configuration

- Policies
  - Software Settings
  - Windows Settings
  - Scripts (Startup/Sh
  - Security Settings
    - Account Policies
    - Local Policies
    - Event Log
    - Restricted Grou
    - System Service
    - Registry
    - File System
    - Wired Network
    - Windows Firew
    - Network List Ma
    - Wireless Netwo
    - Public Key Polici
    - Software Restr
    - Network Access
      - NAP Client
      - Enforce
      - User In
      - Health
  - IP Security Policies on Active Directory

### Network Access Protection Agent Properties

Security Policy Setting

 Network Access Protection Agent

Define this policy setting

Select service startup mode:

Automatic

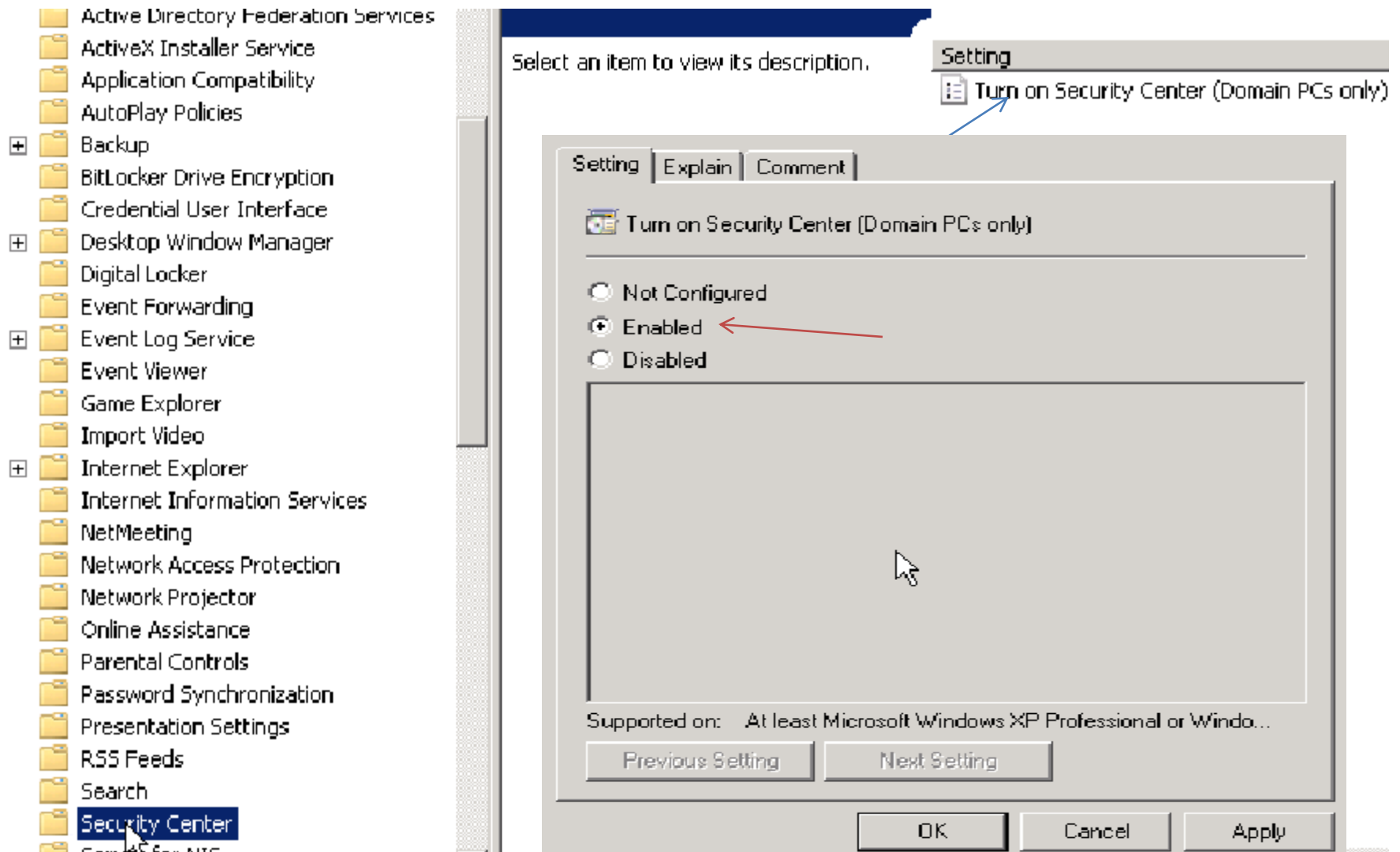
Manual

Disabled

Edit Security...

OK Cancel Apply

The last thing you need to do is to go to Administrative Templates, Windows Components, Security Center



The clients now have all they need to communicate with the Network Policy Server