Simple Configuration of Microsoft NPS as Radius for Navigating 802.1X Networks with Intel AMT (Wired & Wireless AMT)

If you are not familiar with 802.1X networks please review my 802.1X Overview

http://communities.intel.com/docs/DOC-3866

Simple Configuration of Microsoft NPS as Radius for Navigating 802.1X Networks with Intel AMT

•In Windows 2008 Microsoft NPS (Network Policy Server) replaces the Microsoft IAS (Internet Authentication Service) in Windows 2003 as their Radius (AAA Server) component for granting access to secure networks.

•Additionally, NPS can implement extensive health checks to ensure clients comply with your secure policy and can quarantine clients to remediation network to bring them up to compliance (out of scope for just using as Radius).

•Here we will review how to install and configure NPS as a simple Radius for gaining access to secure networks. This document will assist in setting up a pilot for testing your AMT clients OOB (out of band) connectivity with 802.1X enabled networks with NPS as the Radius.

•We will review how to configure a wired 802.1X switch & a Cisco Aironet 1200 wireless AP as AAA clients with NPS to provide OOB access to AMT clients.

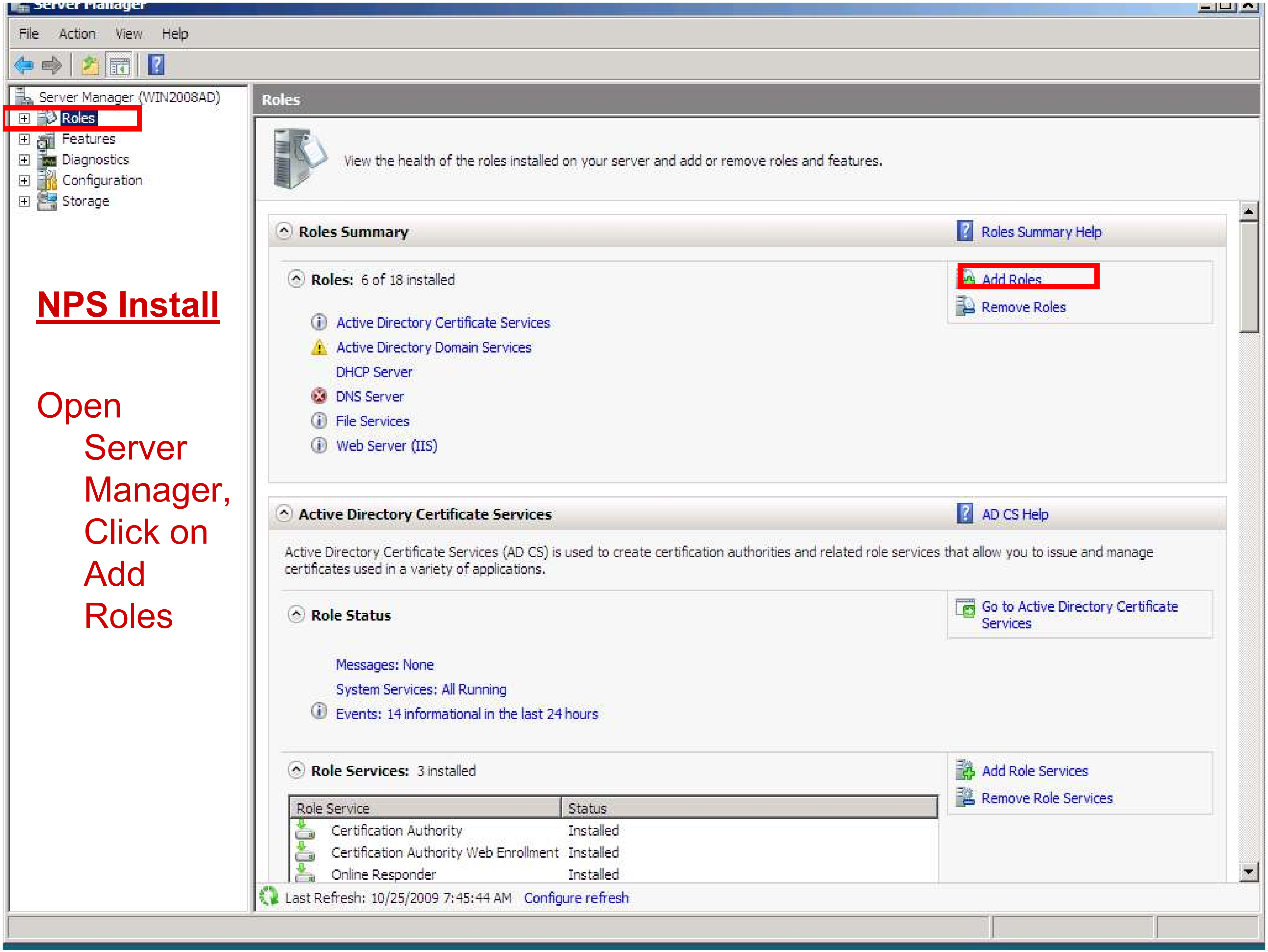
•We will setup a simple policy to allow all authenticated domain users and domain computers on your 802.1X enabled network.

•Without much ado, let’s get started reviewing screen shots for installation and configuration of NPS as the Radius in our Windows 2008 X64 environment with Microsoft CA installed for certificate services (certificate installation is out of scope).

•Just like IAS Radius, NPS could uses certificate installed on the local computer store on which NPS runs for EAP-PEAP and EAP-TLS authentication. However, make sure you point NPS to the right cert if you have multiple certs on the server. More on this inside when we look at EAP-PEAP setup.

NPS Install

Open Server Manager, Click on Add Roles



Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 6 of 18 installed

- Active Directory Certificate Services
- Active Directory Domain Services
- DHCP Server
- DNS Server
- File Services
- Web Server (IIS)

Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Role Status

Messages: None

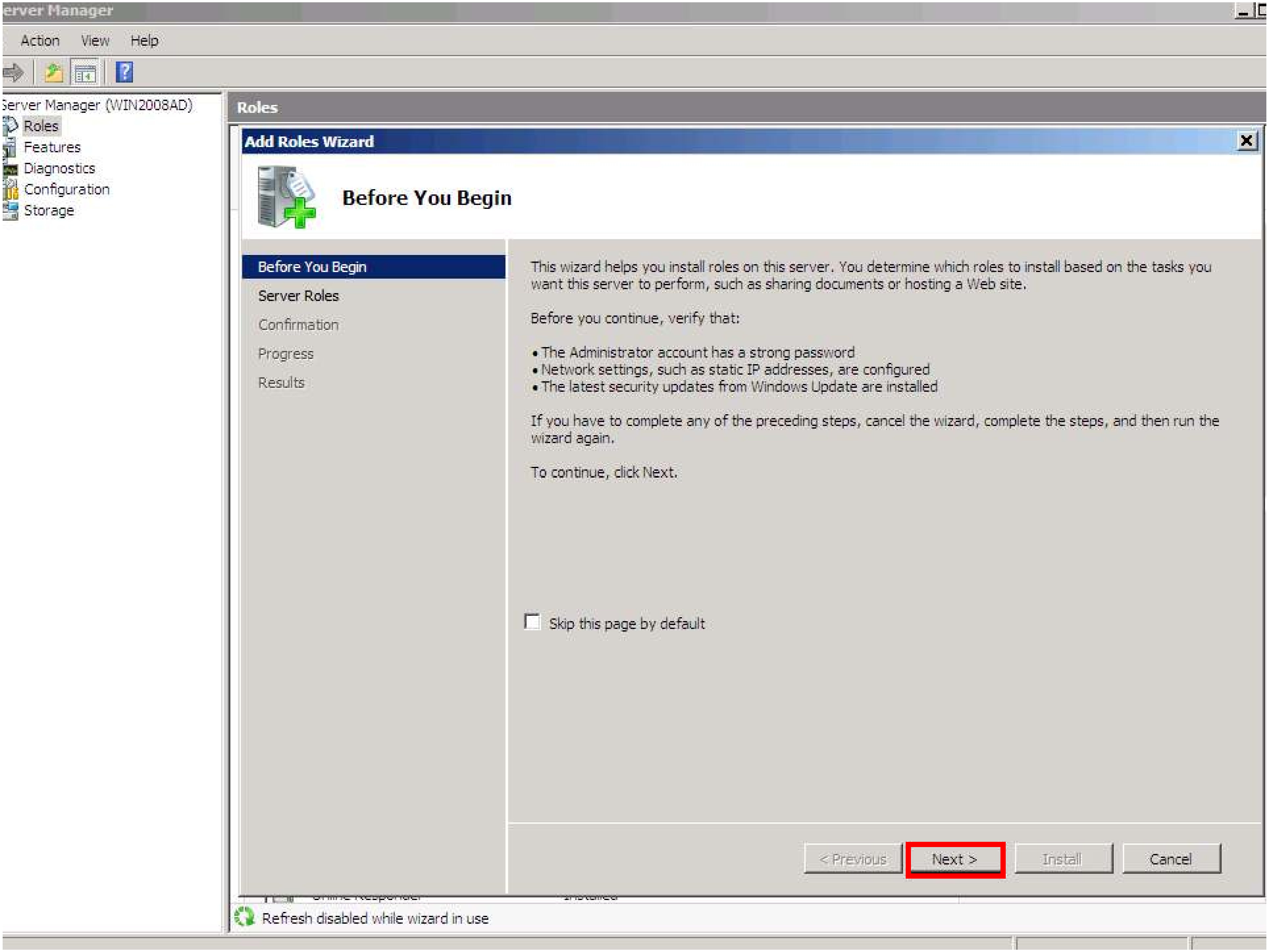
System Services: All Running

Events: 14 informational in the last 24 hours

Role Services: 3 installed

Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Installed
Online Responder	Installed

Last Refresh: 10/25/2009 7:45:44 AM



Before You Begin

This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

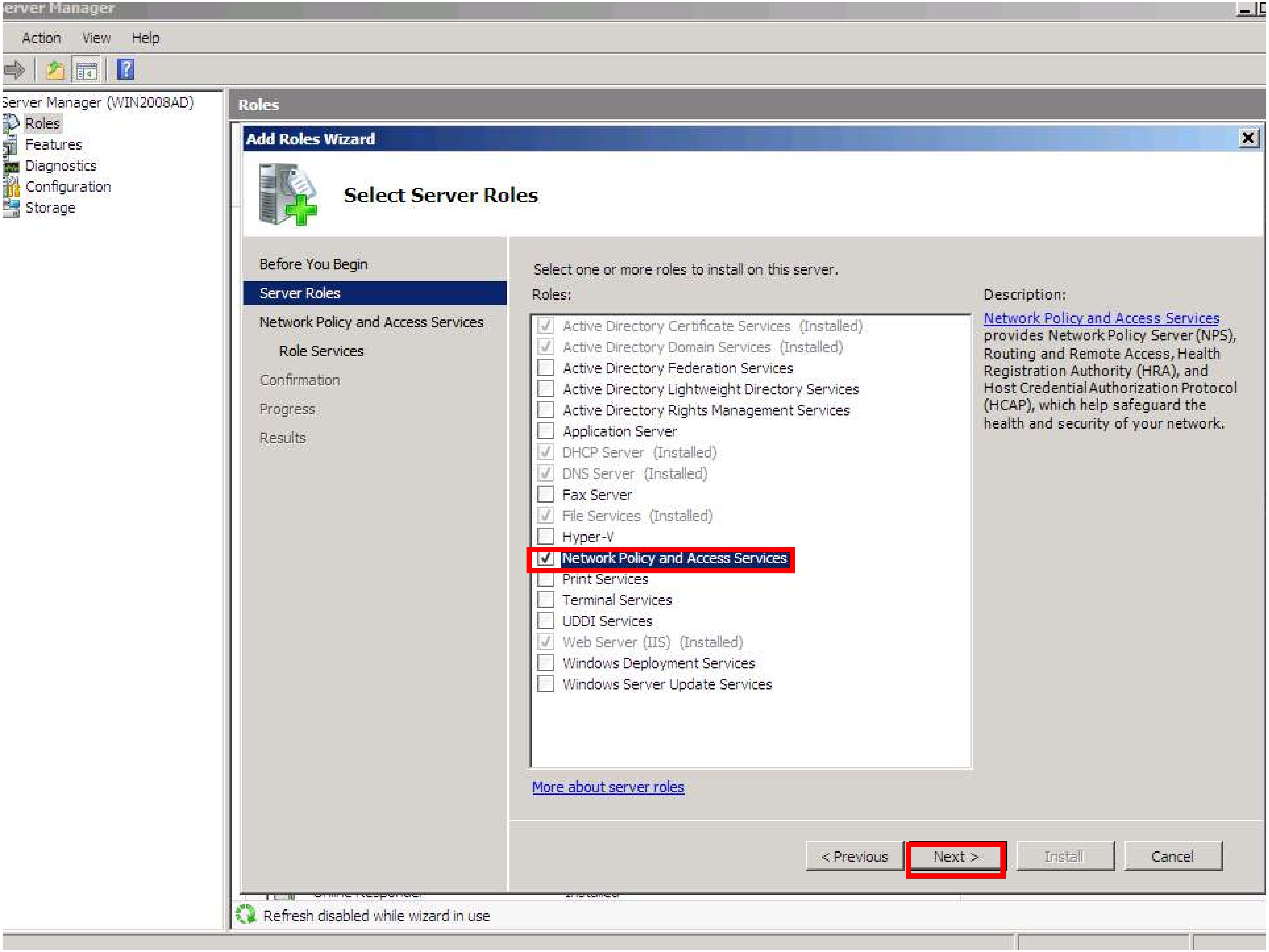
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Refresh disabled while wizard in use



Select Server Roles

Select one or more roles to install on this server.

Roles:

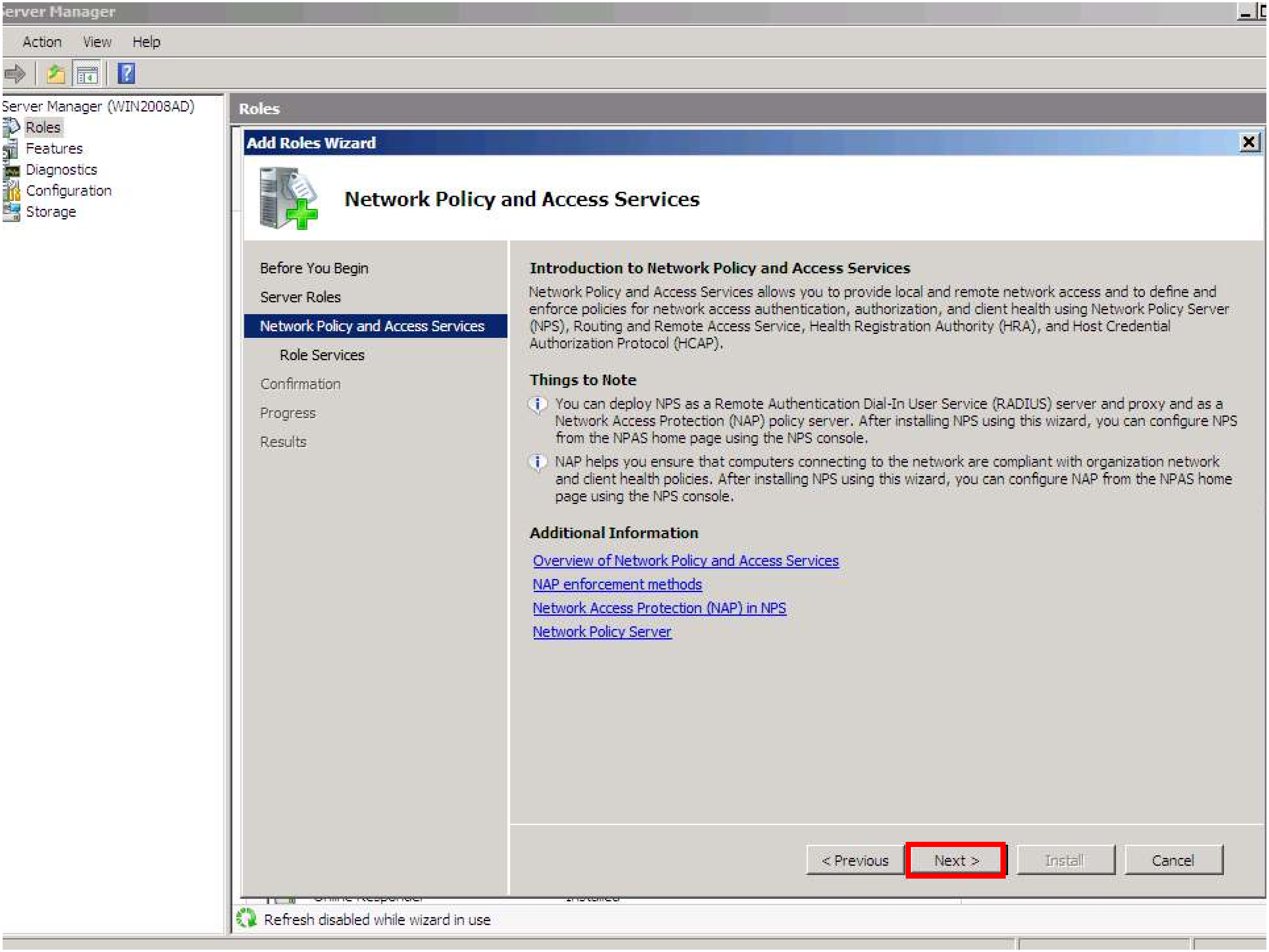
- ☑ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- ☑ File Services (Installed)
- □ Hyper-V
- ☑ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- ☑ Web Server (IIS) (Installed)
- □ Windows Deployment Services
- □ Windows Server Update Services

More about server roles

Description:

Network Policy and Access Services provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

Refresh disabled while wizard in use



Network Policy and Access Services

Introduction to Network Policy and Access Services

Network Policy and Access Services allows you to provide local and remote network access and to define and enforce policies for network access authentication, authorization, and client health using Network Policy Server (NPS), Routing and Remote Access Service, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).

Things to Note

- You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy and as a Network Access Protection (NAP) policy server. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.
- NAP helps you ensure that computers connecting to the network are compliant with organization network and client health policies. After installing NPS using this wizard, you can configure NAP from the NPAS home page using the NPS console.

Additional Information

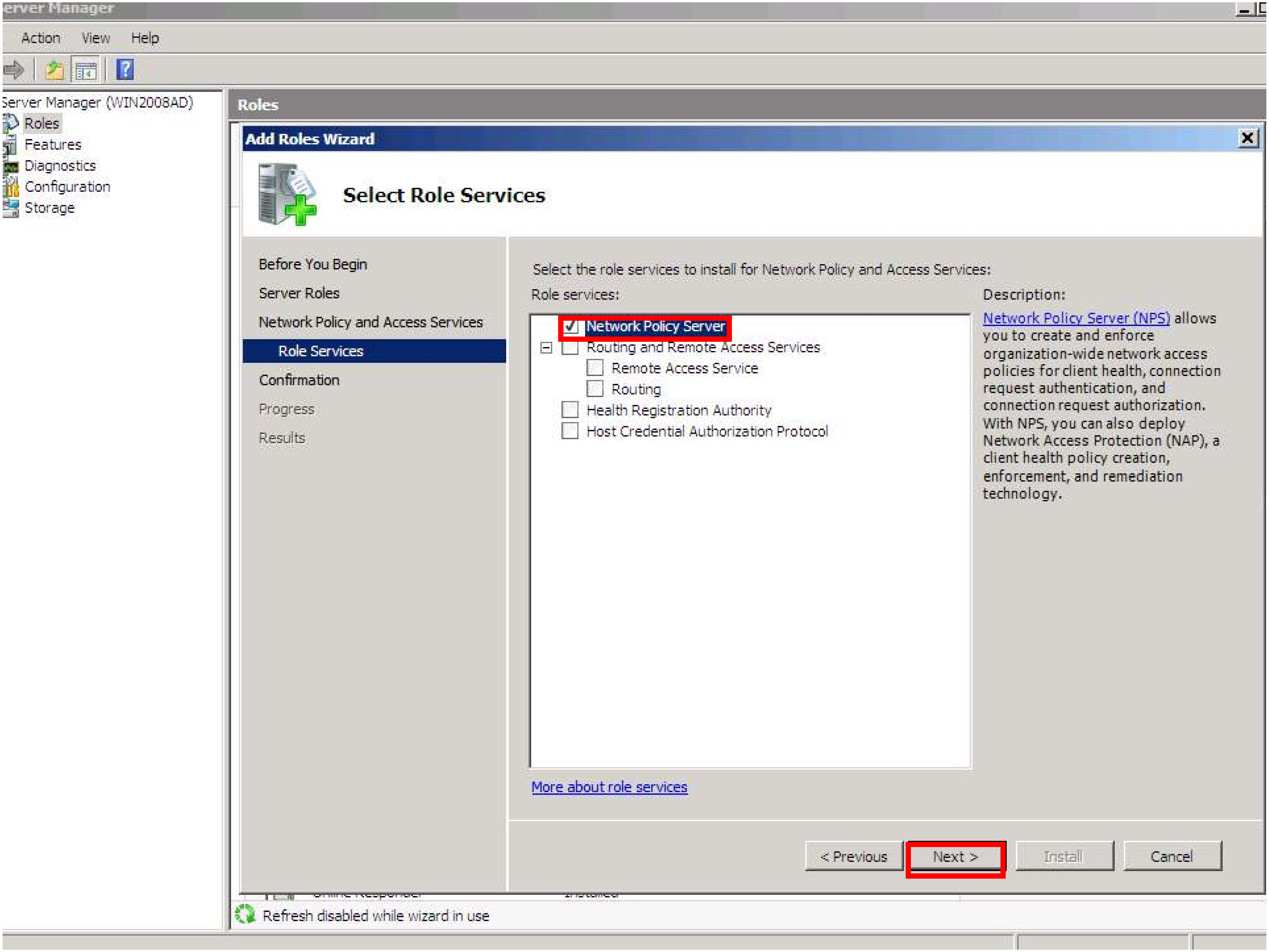
Overview of Network Policy and Access Services

NAP enforcement methods

Network Access Protection (NAP) in NPS

Network Policy Server

Refresh disabled while wizard in use



Select Role Services

Select the role services to install for Network Policy and Access Services:

Role services:

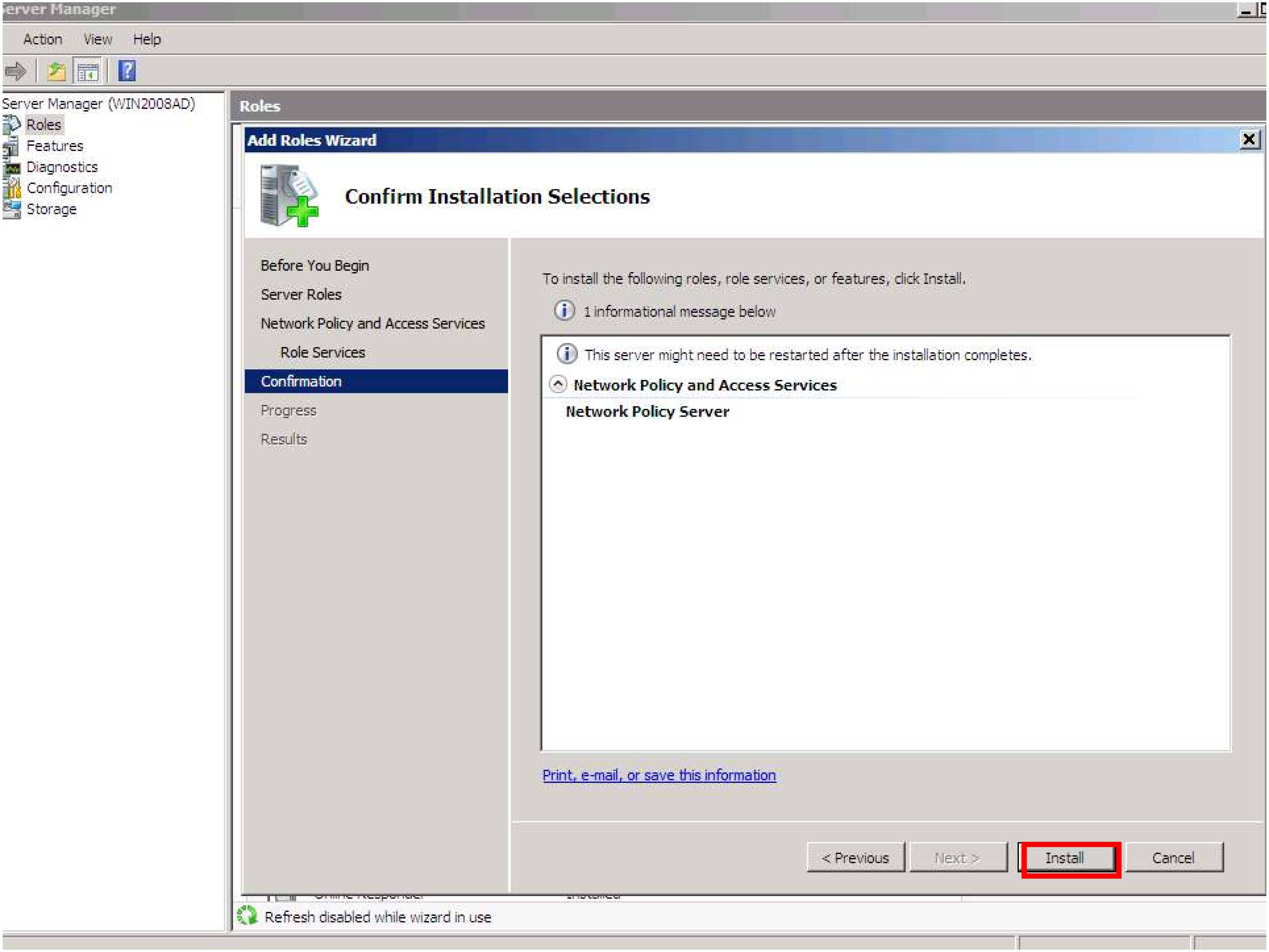
☑ Network Policy Server
⊟ □ Routing and Remote Access Services
  □ Remote Access Service
  □ Routing
□ Health Registration Authority
□ Host Credential Authorization Protocol

More about role services

Description:

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. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

Refresh disabled while wizard in use



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

ⓘ 1 informational message below

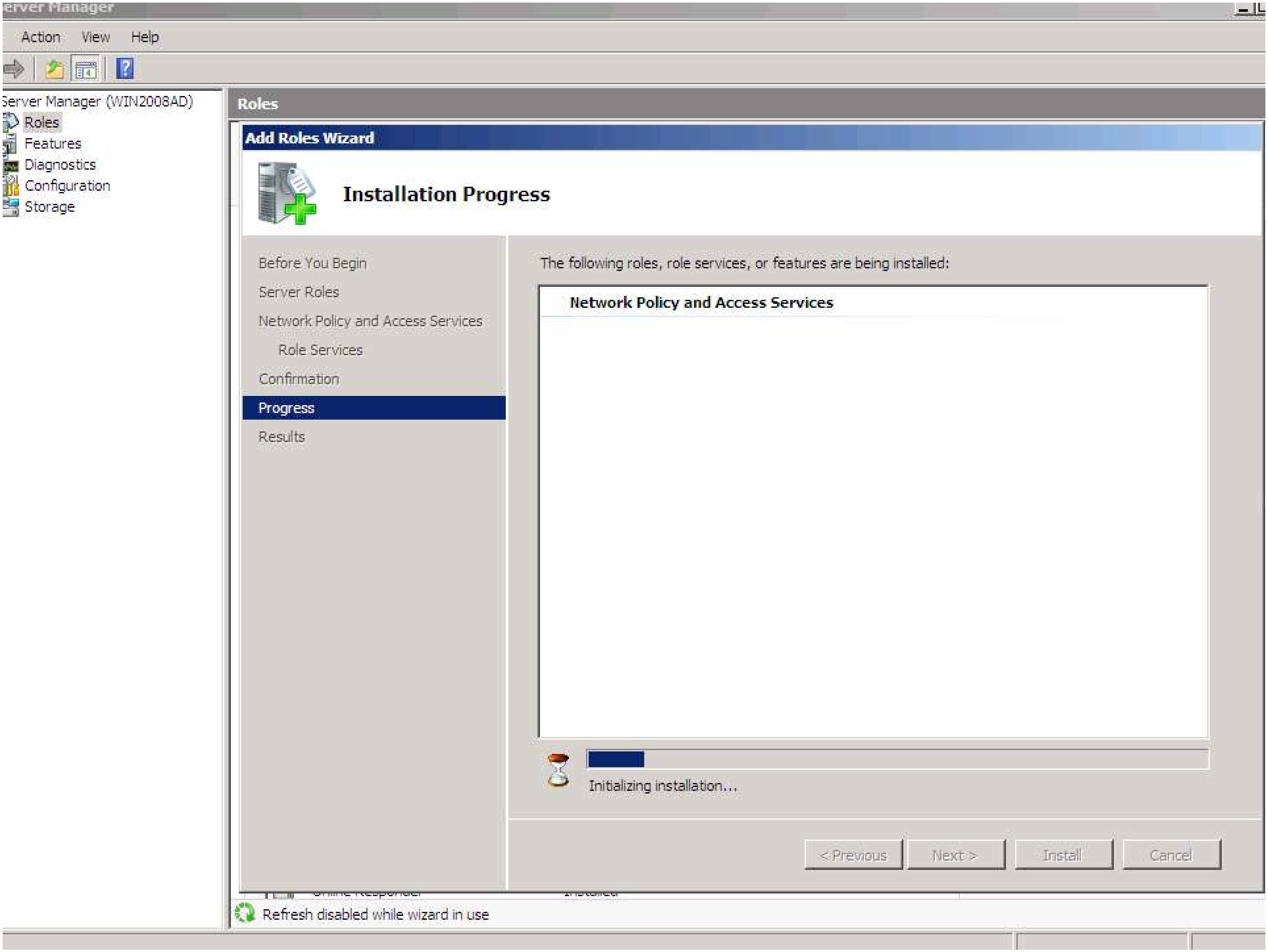
ⓘ This server might need to be restarted after the installation completes.

Network Policy and Access Services

Network Policy Server

Print, e-mail, or save this information

Refresh disabled while wizard in use



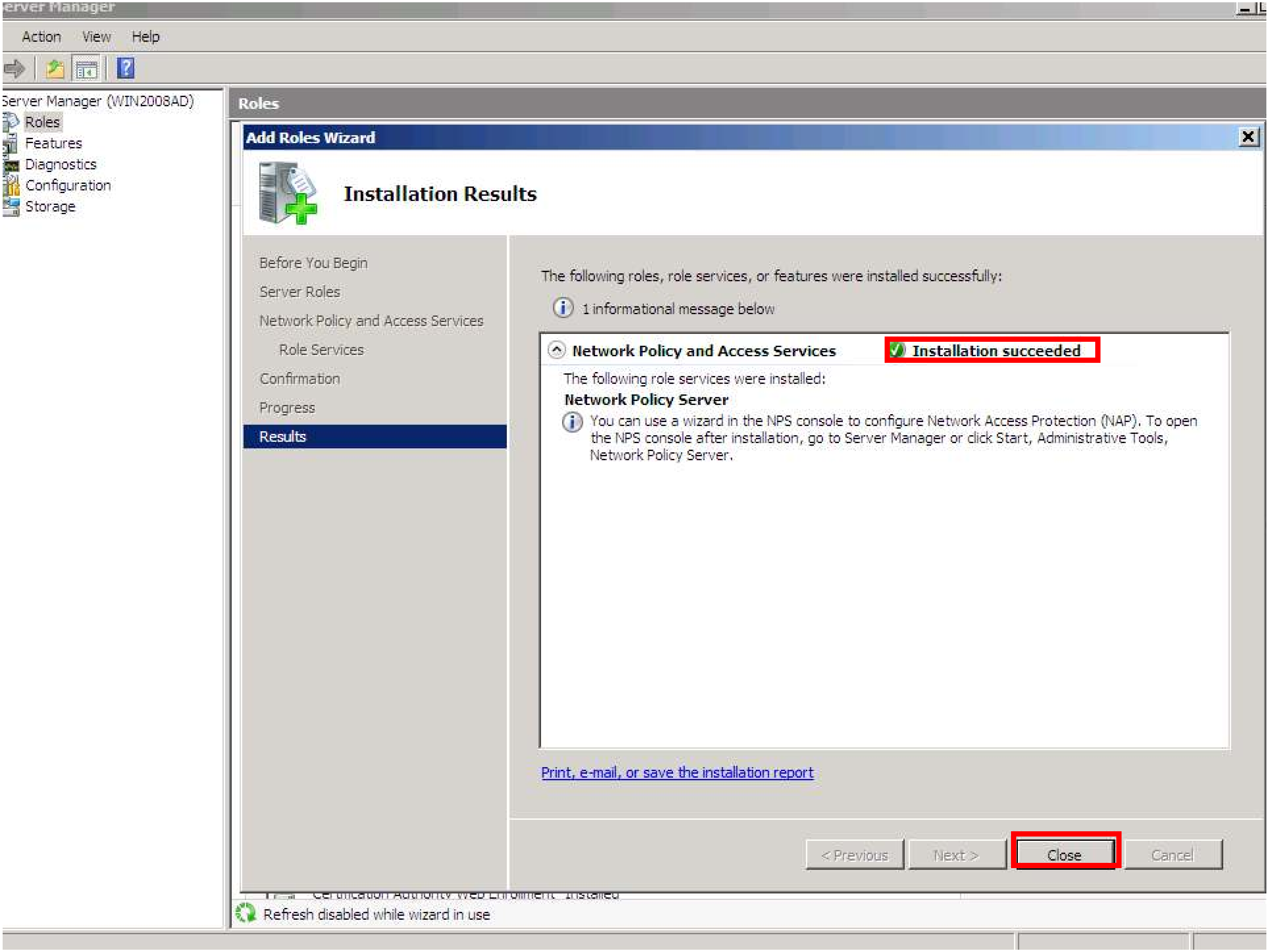
Installation Progress

The following roles, role services, or features are being installed:

Network Policy and Access Services

Initializing installation...

Refresh disabled while wizard in use



Installation Results

The following roles, role services, or features were installed successfully:

1 informational message below

Network Policy and Access Services ✓ **Installation succeeded**

The following role services were installed:

Network Policy Server

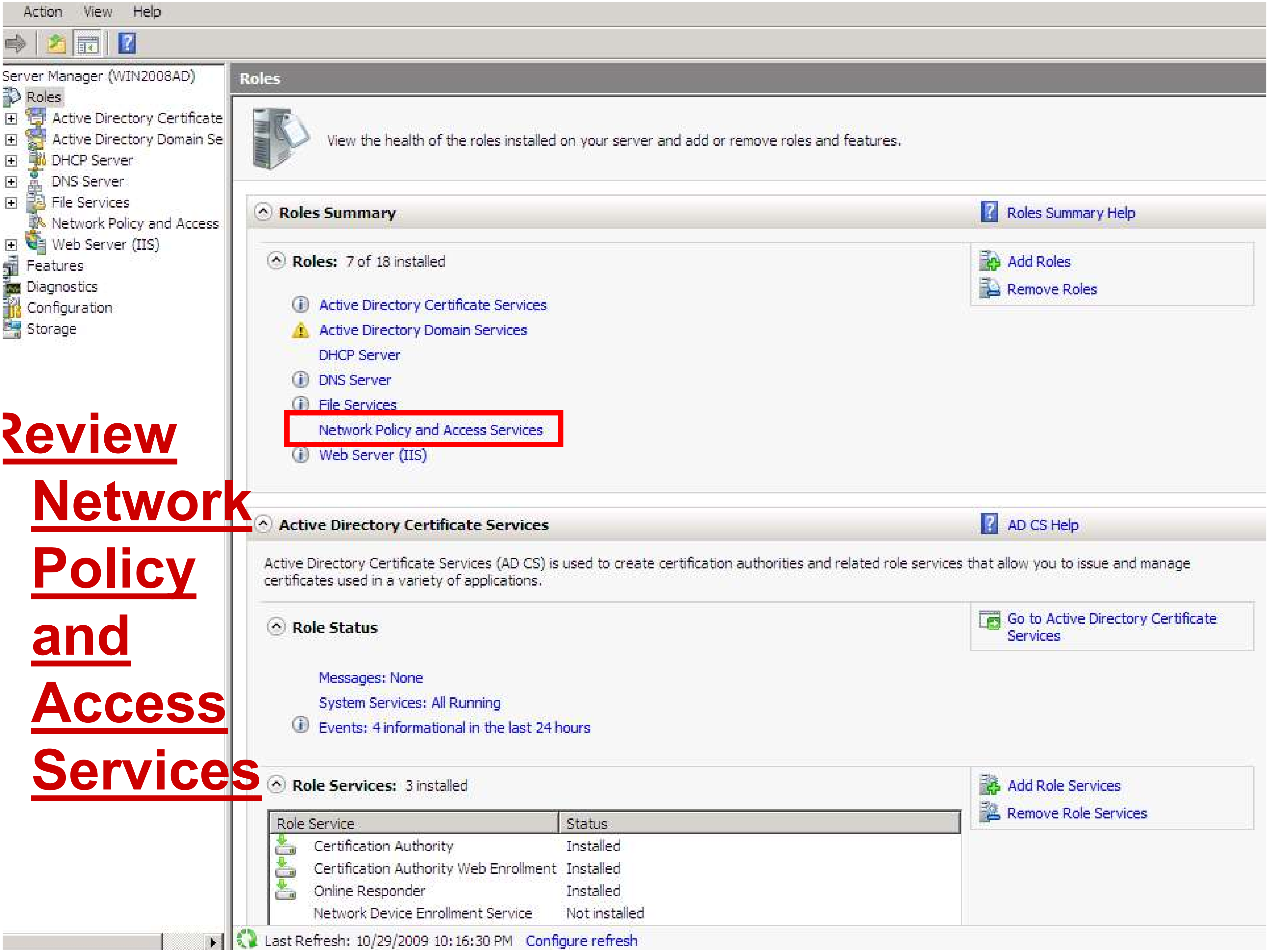
You can use a wizard in the NPS console to configure Network Access Protection (NAP). To open the NPS console after installation, go to Server Manager or click Start, Administrative Tools, Network Policy Server.

Print, e-mail, or save the installation report

Certification Authority Web Enrollment Installed

Refresh disabled while wizard in use

Review Network Policy and Access Services



Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 7 of 18 installed

- Active Directory Certificate Services
- Active Directory Domain Services
- DHCP Server
- DNS Server
- File Services
- Network Policy and Access Services
- Web Server (IIS)

Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Role Status

Messages: None

System Services: All Running

Events: 4 informational in the last 24 hours

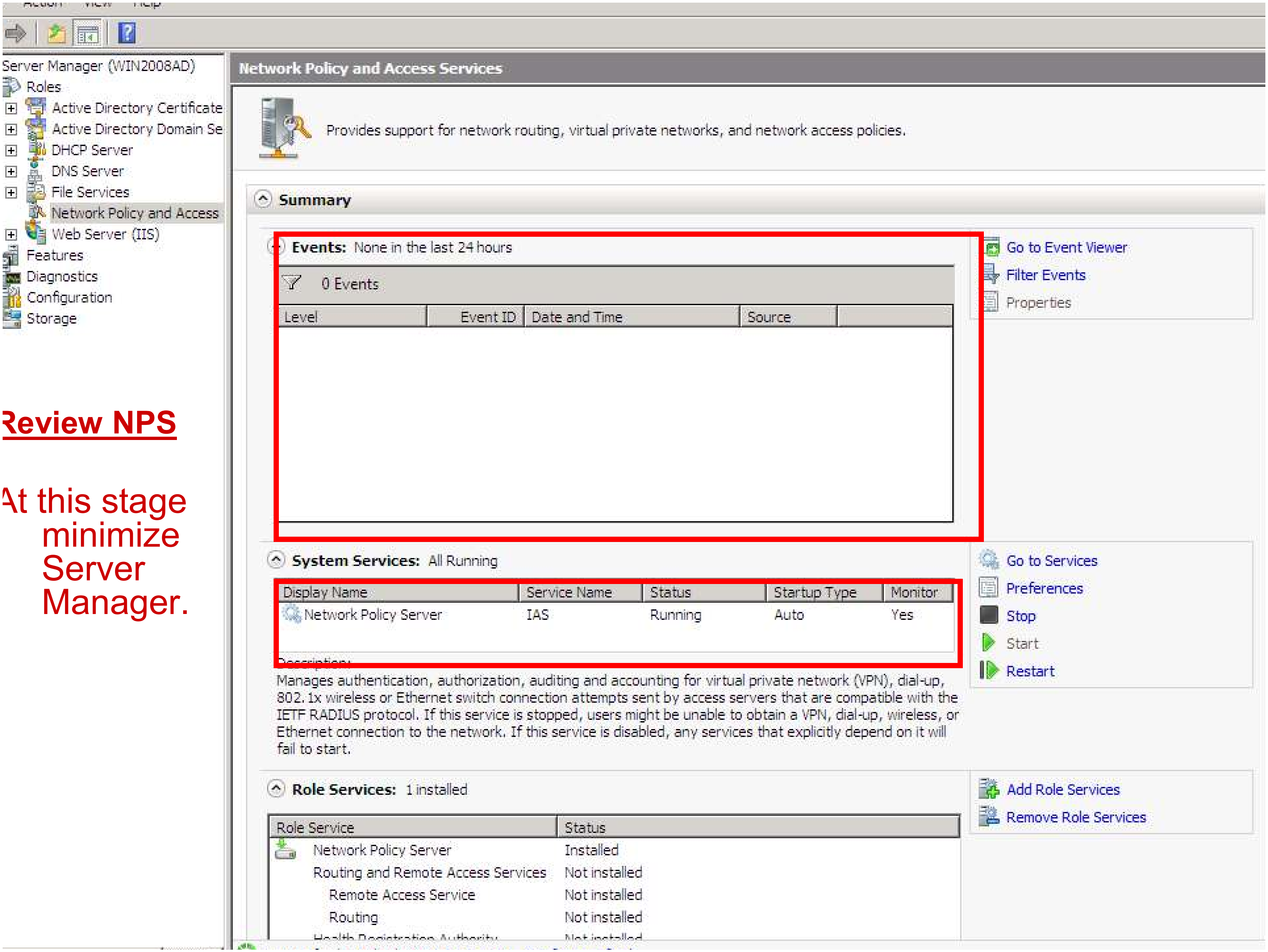
Role Services: 3 installed

Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Installed
Online Responder	Installed
Network Device Enrollment Service	Not installed

Last Refresh: 10/29/2009 10:16:30 PM Configure refresh

Review NPS

At this stage minimize Server Manager.



Server Manager (WIN2008AD)
- Roles
  - Active Directory Certificate
  - Active Directory Domain Se
  - DHCP Server
  - DNS Server
  - File Services
  - Network Policy and Access
  - Web Server (IIS)
- Features
- Diagnostics
- Configuration
- Storage

Network Policy and Access Services

Provides support for network routing, virtual private networks, and network access policies.

Summary

Events: None in the last 24 hours

0 Events

Level	Event ID	Date and Time	Source

System Services: All Running

Display Name	Service Name	Status	Startup Type	Monitor
Network Policy Server	IAS	Running	Auto	Yes

Description:
Manages authentication, authorization, auditing and accounting for virtual private network (VPN), dial-up, 802.1x wireless or Ethernet switch connection attempts sent by access servers that are compatible with the IETF RADIUS protocol. If this service is stopped, users might be unable to obtain a VPN, dial-up, wireless, or Ethernet connection to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

Role Services: 1 installed

Role Service	Status
Network Policy Server	Installed
Routing and Remote Access Services	Not installed
Remote Access Service	Not installed
Routing	Not installed
Health Registration Authority	Not installed

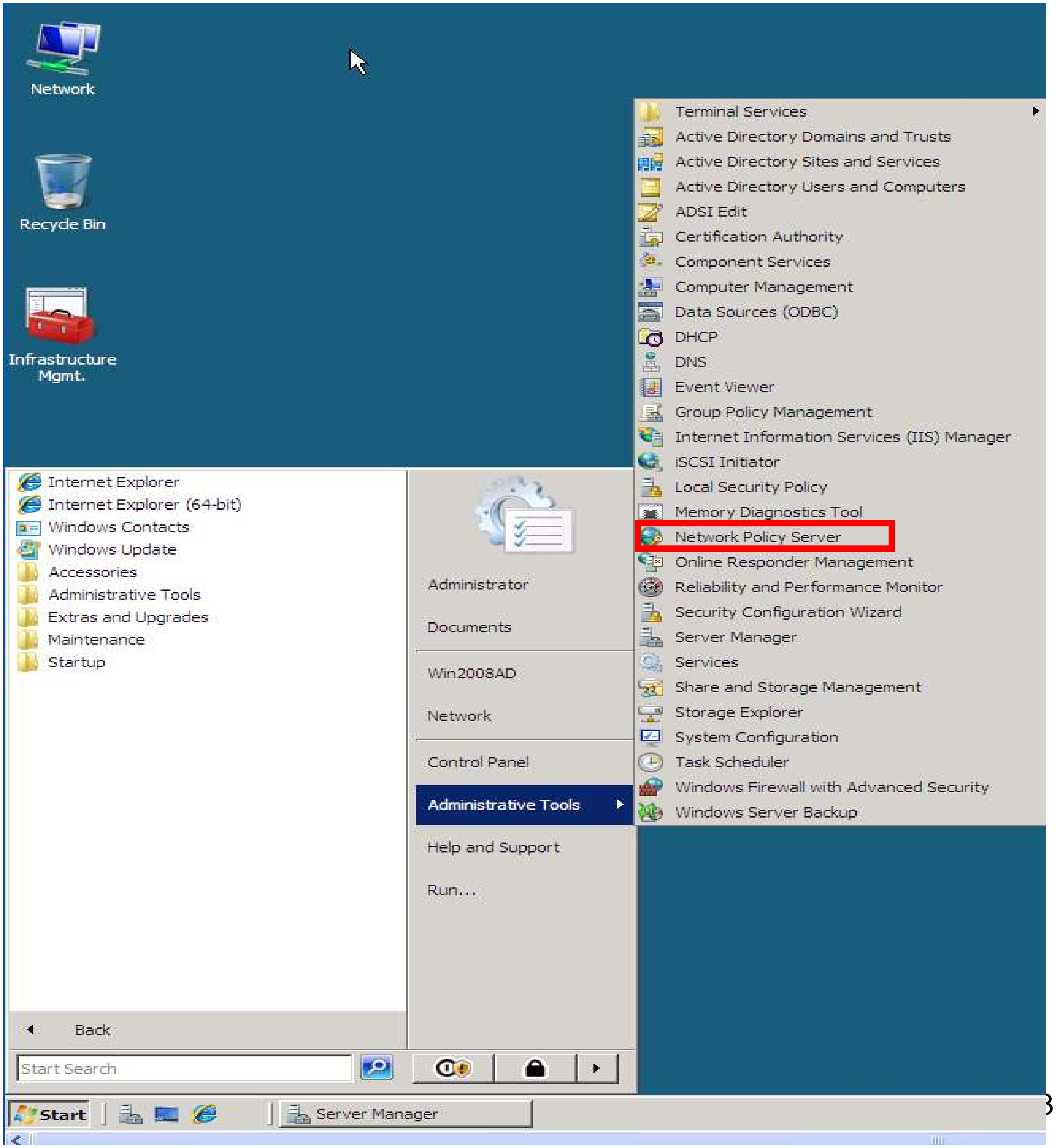
Configure NPS

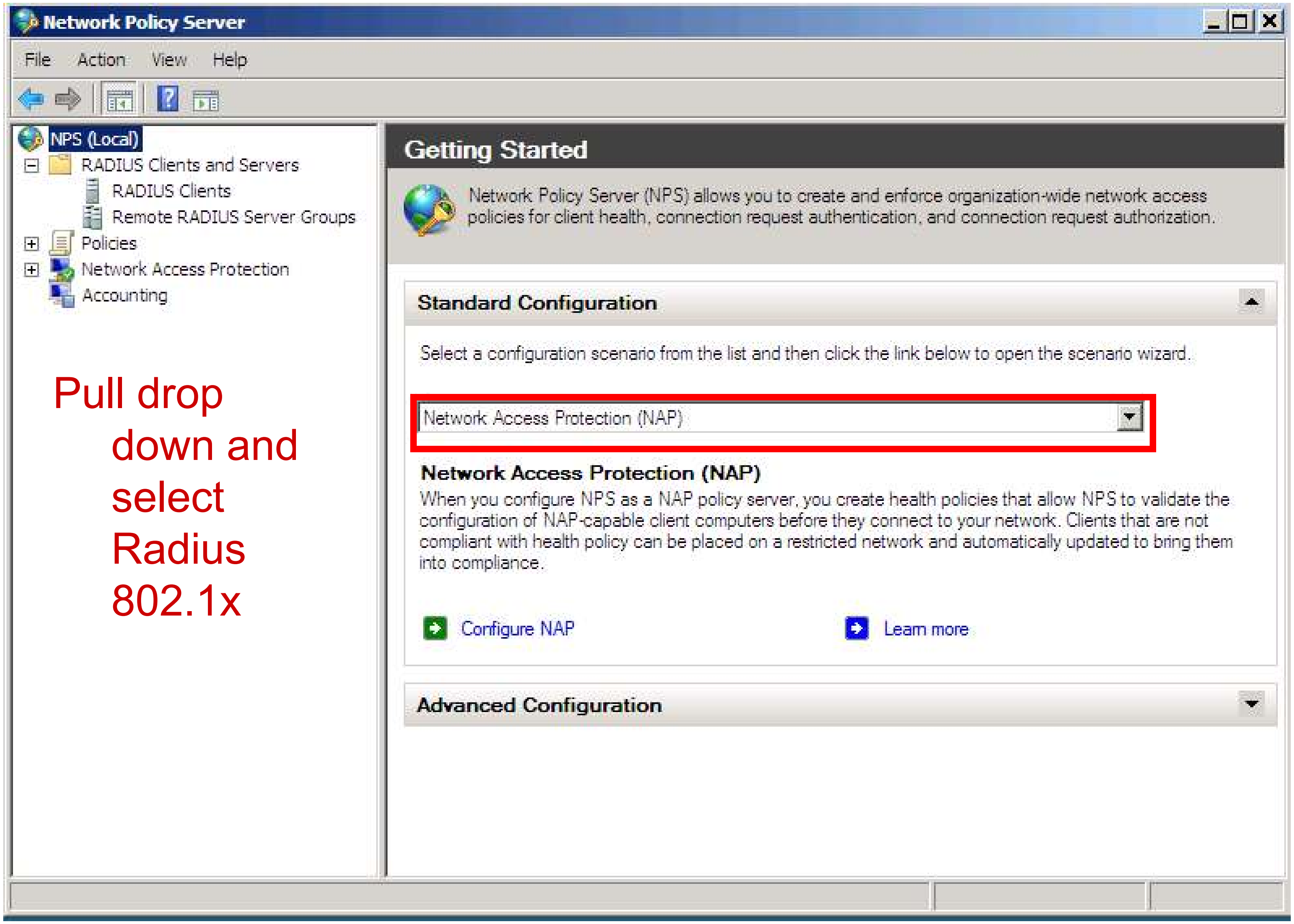
Click, Start, All Programs,

Administrative Tools,

Network Policy Server

to configure NPS





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.

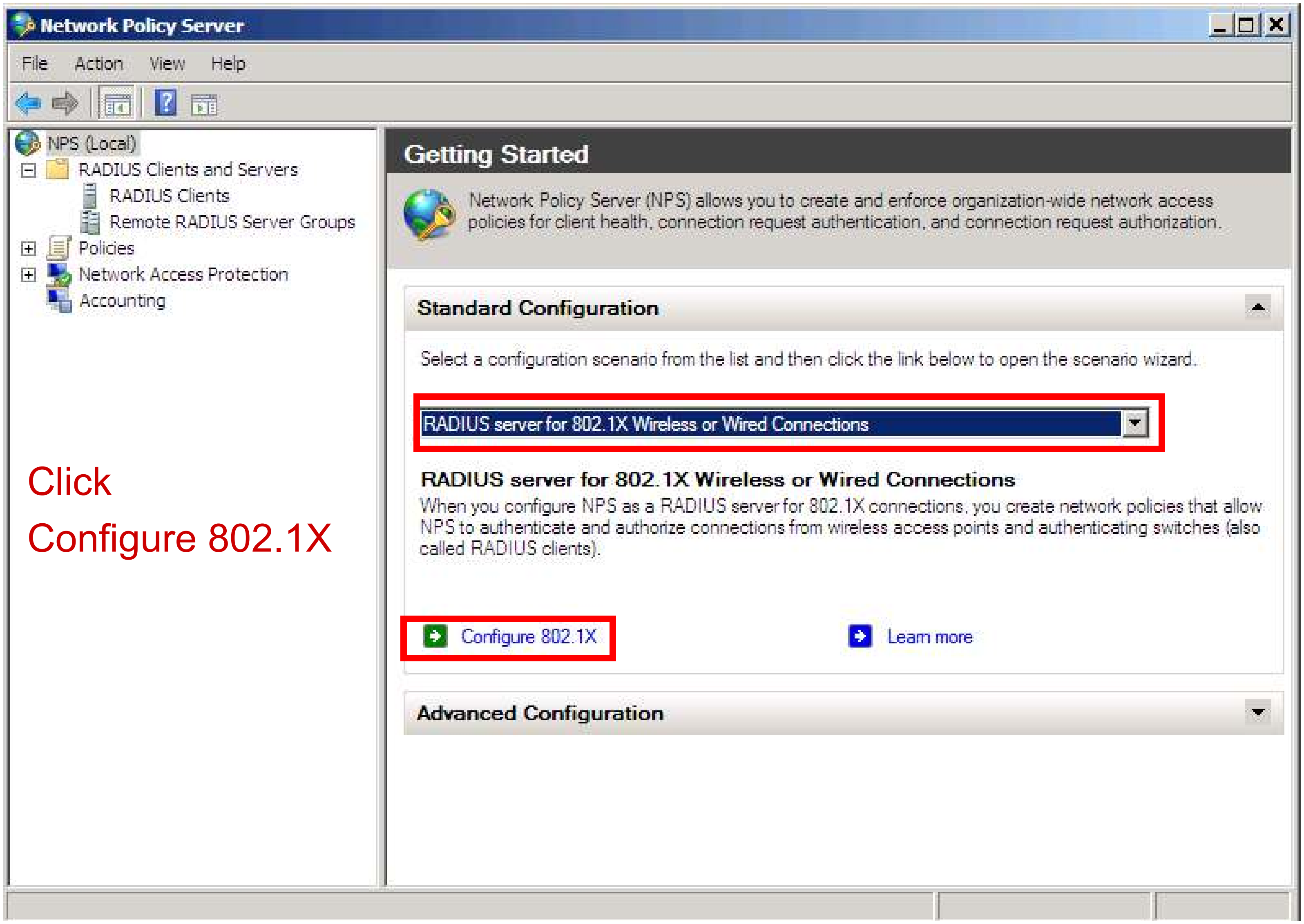
Network Access Protection (NAP)

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.

Advanced Configuration

Pull drop down and select Radius 802.1x



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.

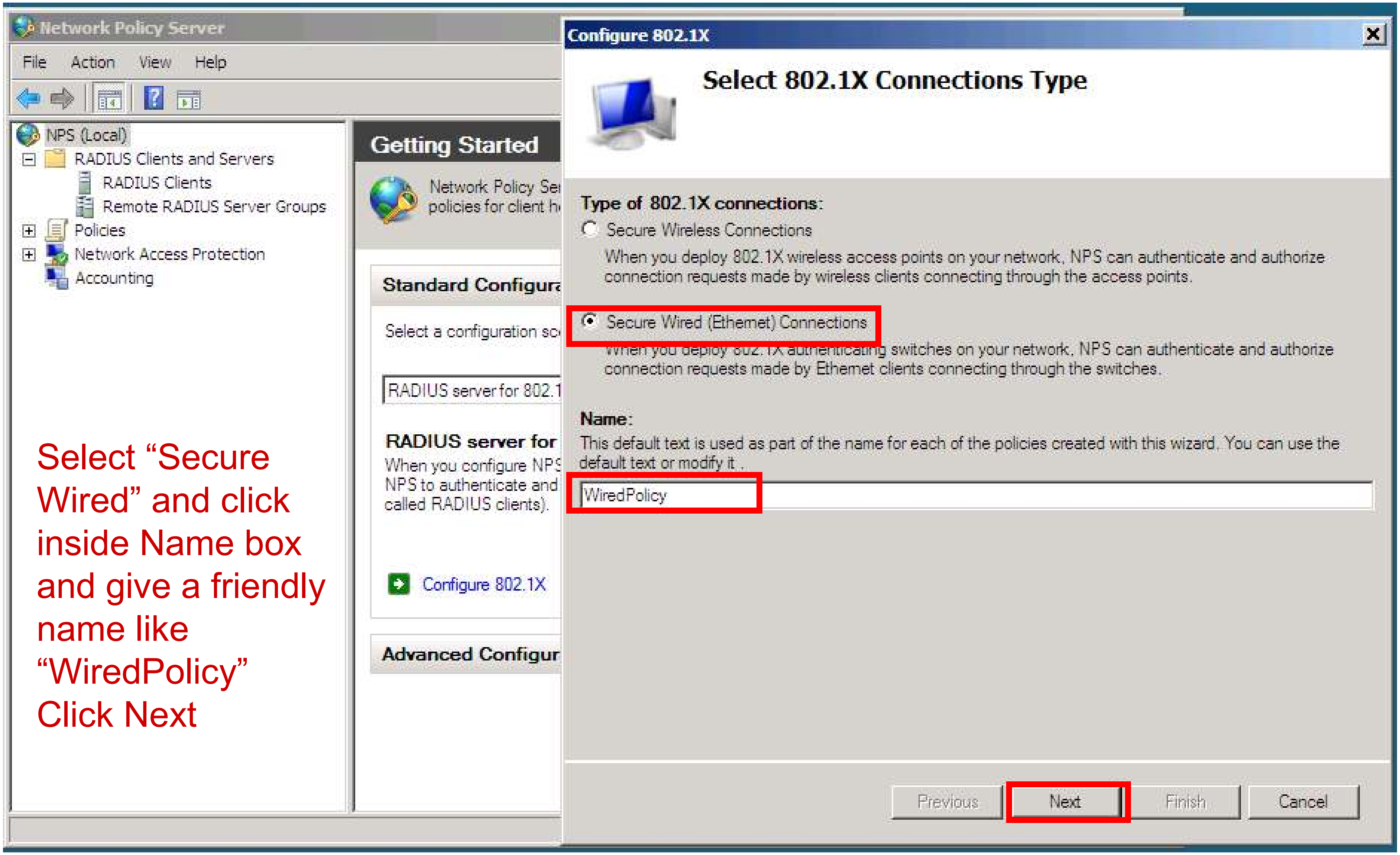
RADIUS server for 802.1X Wireless or Wired Connections

RADIUS server for 802.1X Wireless or Wired Connections

When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

Click

Configure 802.1X



Network Policy Se
policies for client h

Select a configuration sc

RADIUS server for 802.1

RADIUS server for
When you configure NPS
NPS to authenticate and
called RADIUS clients).

Configure 802.1X

Select 802.1X Connections Type

Type of 802.1X connections:

○ Secure Wireless Connections

When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

● Secure Wired (Ethernet) Connections

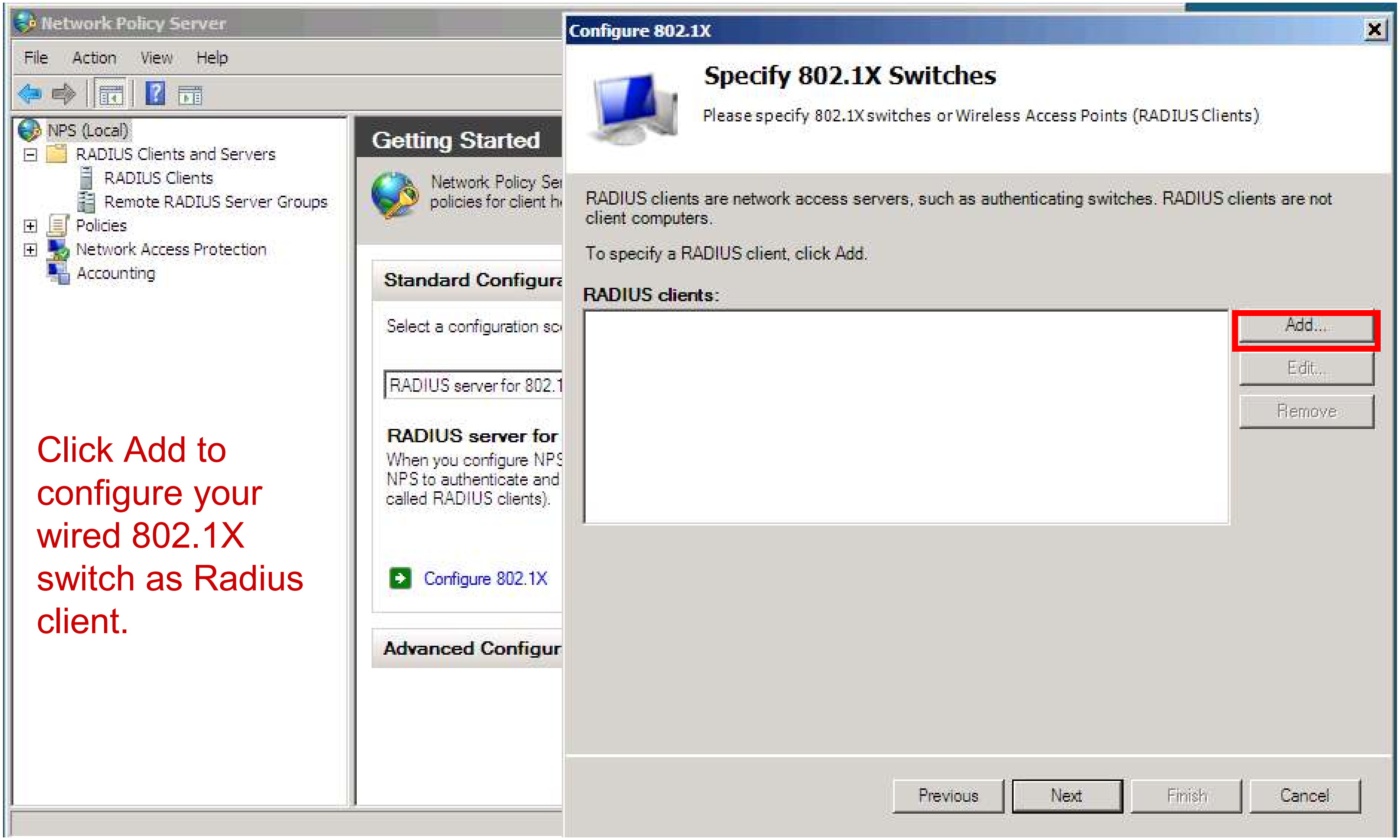
When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

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 .

WiredPolicy

Select "Secure Wired" and click inside Name box and give a friendly name like "WiredPolicy"
Click Next



Specify 802.1X Switches

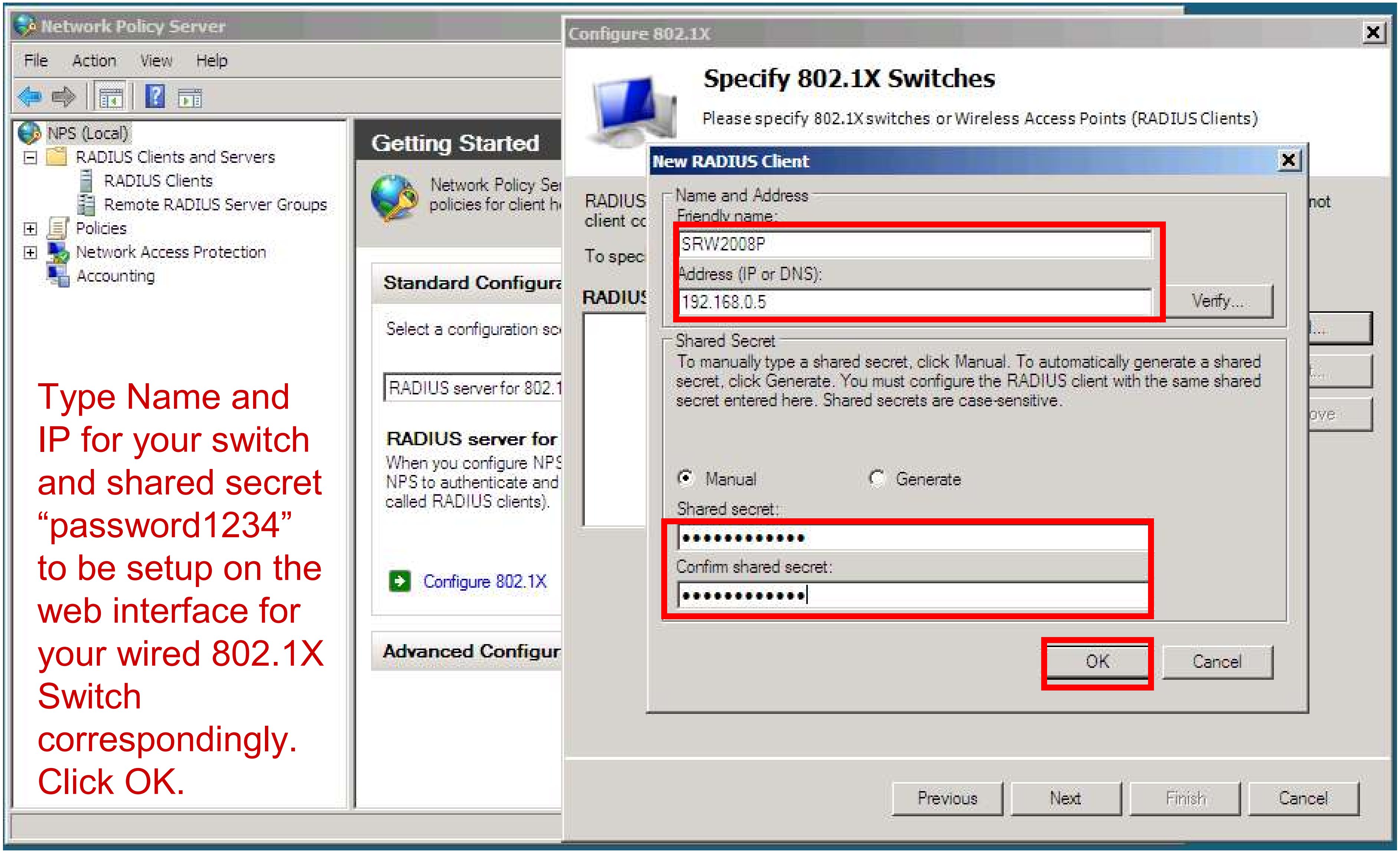
Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)

RADIUS clients are network access servers, such as authenticating switches. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

RADIUS clients:

Click Add to configure your wired 802.1X switch as Radius client.



Specify 802.1X Switches

Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)

New RADIUS Client

Name and Address

Friendly name: SRW2008P

Address (IP or DNS): 192.168.0.5

Shared Secret

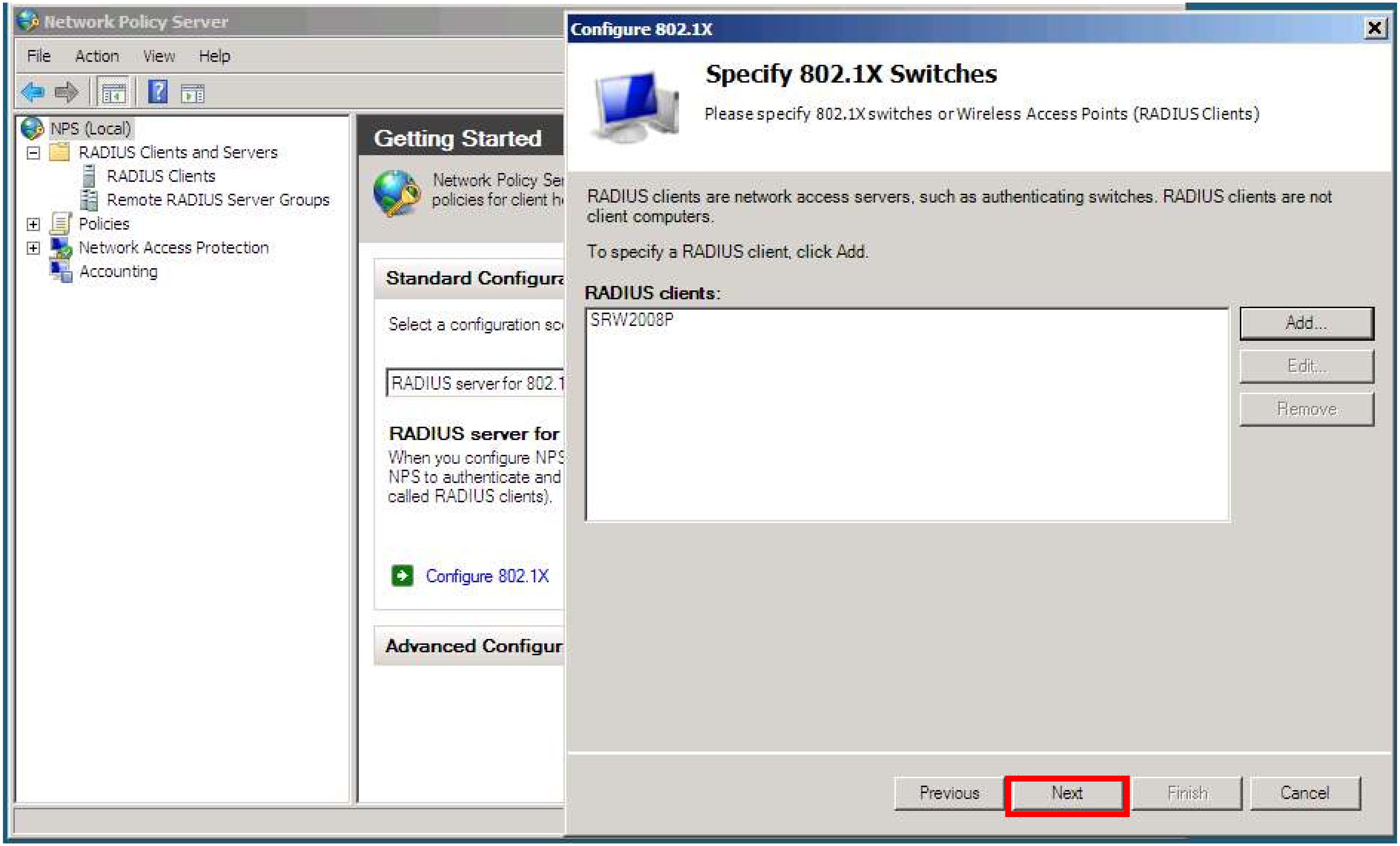
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••••••••••

Confirm shared secret: •••••••••••••

Type Name and IP for your switch and shared secret “password1234” to be setup on the web interface for your wired 802.1X Switch correspondingly. Click OK.



Specify 802.1X Switches

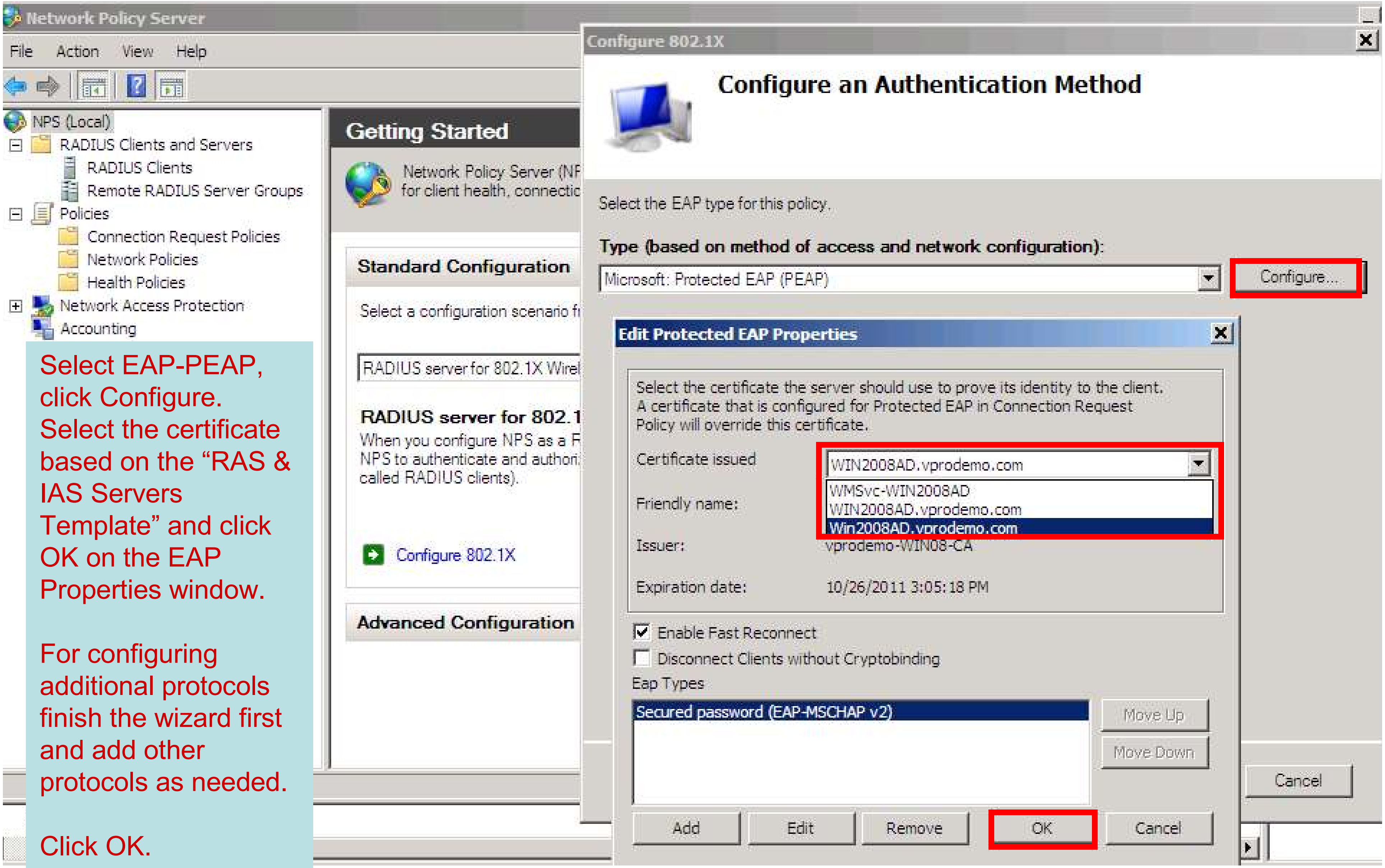
Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)

RADIUS clients are network access servers, such as authenticating switches. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

RADIUS clients:

SRW2008P



Network Policy Server (NP
for client health, connectio

Select a configuration scenario fr

RADIUS server for 802.1

When you configure NPS as a R
NPS to authenticate and authori
called RADIUS clients).

Configure an Authentication Method

Select the EAP type for this policy.

Type (based on method of access and network configuration): Microsoft: Protected EAP (PEAP)

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued: WIN2008AD.vprodemo.com

WMSvc-WIN2008AD
WIN2008AD.vprodemo.com
Win2008AD.vprodemo.com

Friendly name:

Issuer: vprodemo-WIN08-CA

Expiration date: 10/26/2011 3:05:18 PM

☑ Enable Fast Reconnect

☐ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

Select EAP-PEAP, click Configure. Select the certificate based on the “RAS & IAS Servers Template” and click OK on the EAP Properties window.

For configuring additional protocols finish the wizard first and add other protocols as needed.

Click OK.

Important Note on the NPS Certificates:

Use the following Technet articles to configure the NPS certificate based on the RAS and IAS Servers Template

NPS Server Certificate and CA installation:
http://technet.microsoft.com/en-us/library/cc771431%28WS.10%29.aspx
NPS Server Certificate: Configure the Template and Auto-enrollment
http://technet.microsoft.com/en-us/library/cc754198%28WS.10%29.aspx

If you require clients to “validate server certificate” then the root certificate for the CA that issues the NPS certificate should be present in the client’s Trusted root store.

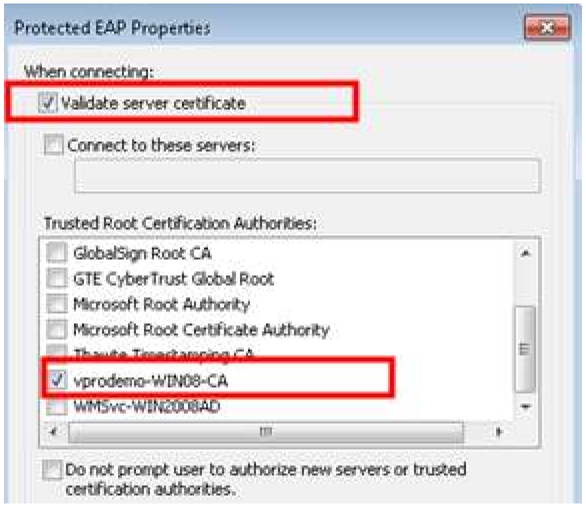
Important Note on the EAP-PEAP Protocol:

Although EAP-PEAP protocols uses windows username / password for authentication, it still requires a certificate to be installed on the NPS server. If certificate is not installed on the NPS, it uses the self-signed web services management certificate in IIS7 (WMSvc-XXXX).

With EAP-PEAP a secure tunnel is first established between Radius and the client and the username/password exchange happens inside that secure tunnel.

Tip: We noticed that when the authentication fails because of incorrect certificate, NPS logs this event as Invalid user name/password for EAP-PEAP authentication and do not report the actual error which should state “Secure tunnel could not be established for the EAP-PEAP authentication”.

Tip: First test with “validating server certificate” unchecked to troubleshoot any certificate configuration issues for EAP-PEAP protocol. Once successful, turn on “Validate server certificate” option if required in your environment.



Protected EAP Properties

When connecting:

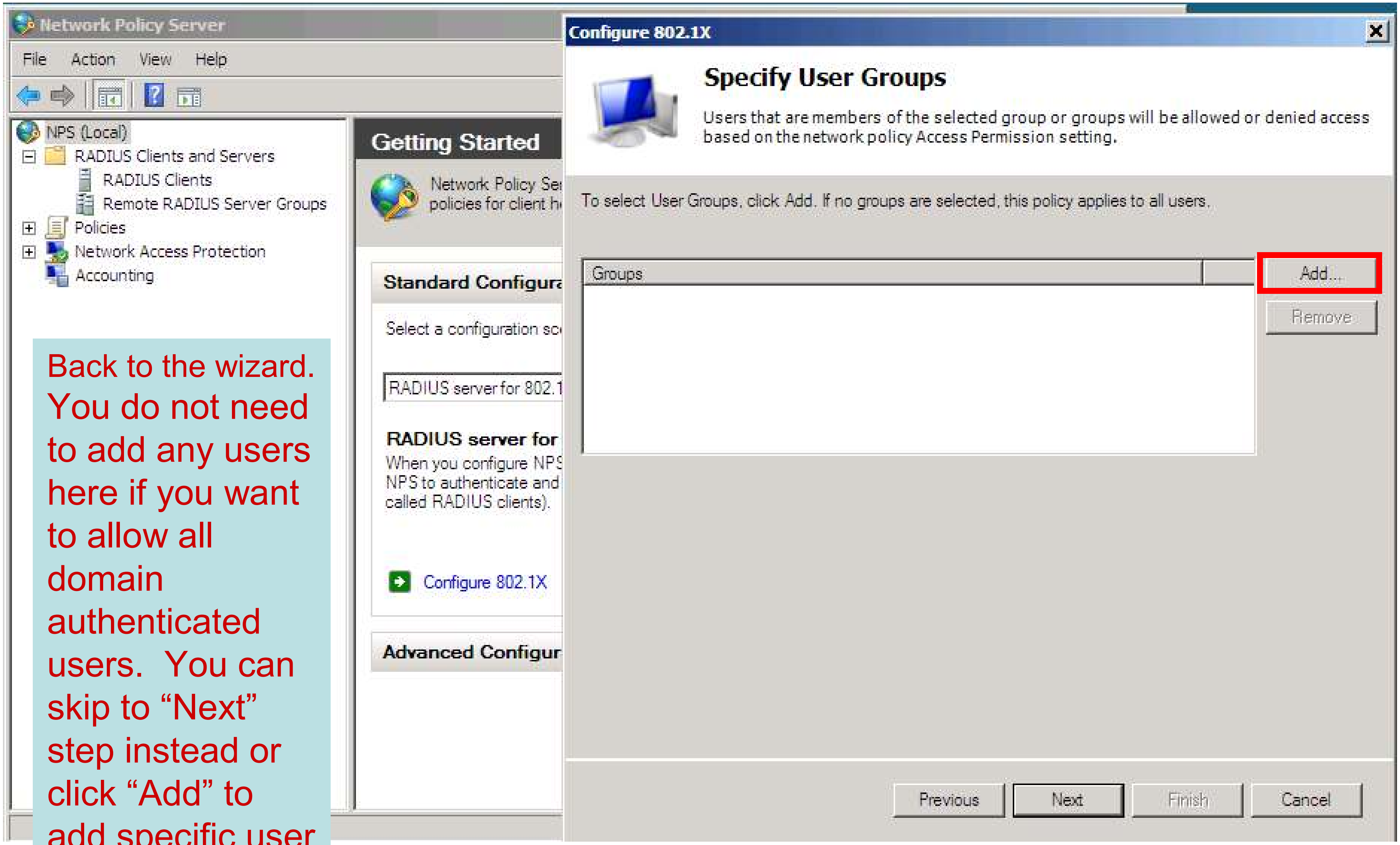
☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ GlobalSign Root CA
□ GTE CyberTrust Global Root
□ Microsoft Root Authority
□ Microsoft Root Certificate Authority
□ Thawte Timestamping CA
☑ vprodemo-WIN08-CA
□ WMSvc-WIN2008AD

□ Do not prompt user to authorize new servers or trusted certification authorities.



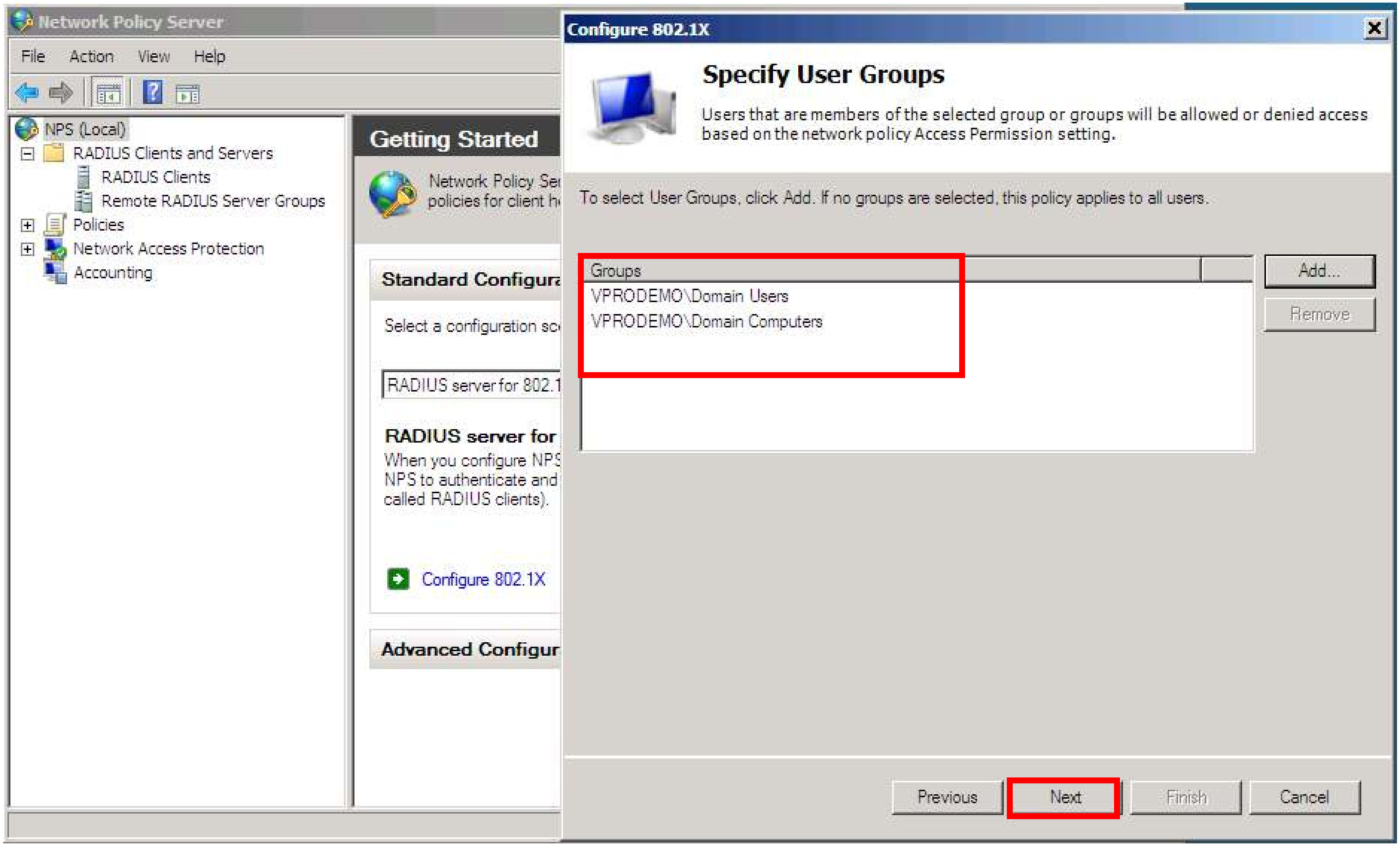
Configure 802.1X

Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Back to the wizard. You do not need to add any users here if you want to allow all domain authenticated users. You can skip to "Next" step instead or click "Add" to add specific user groups that you would like

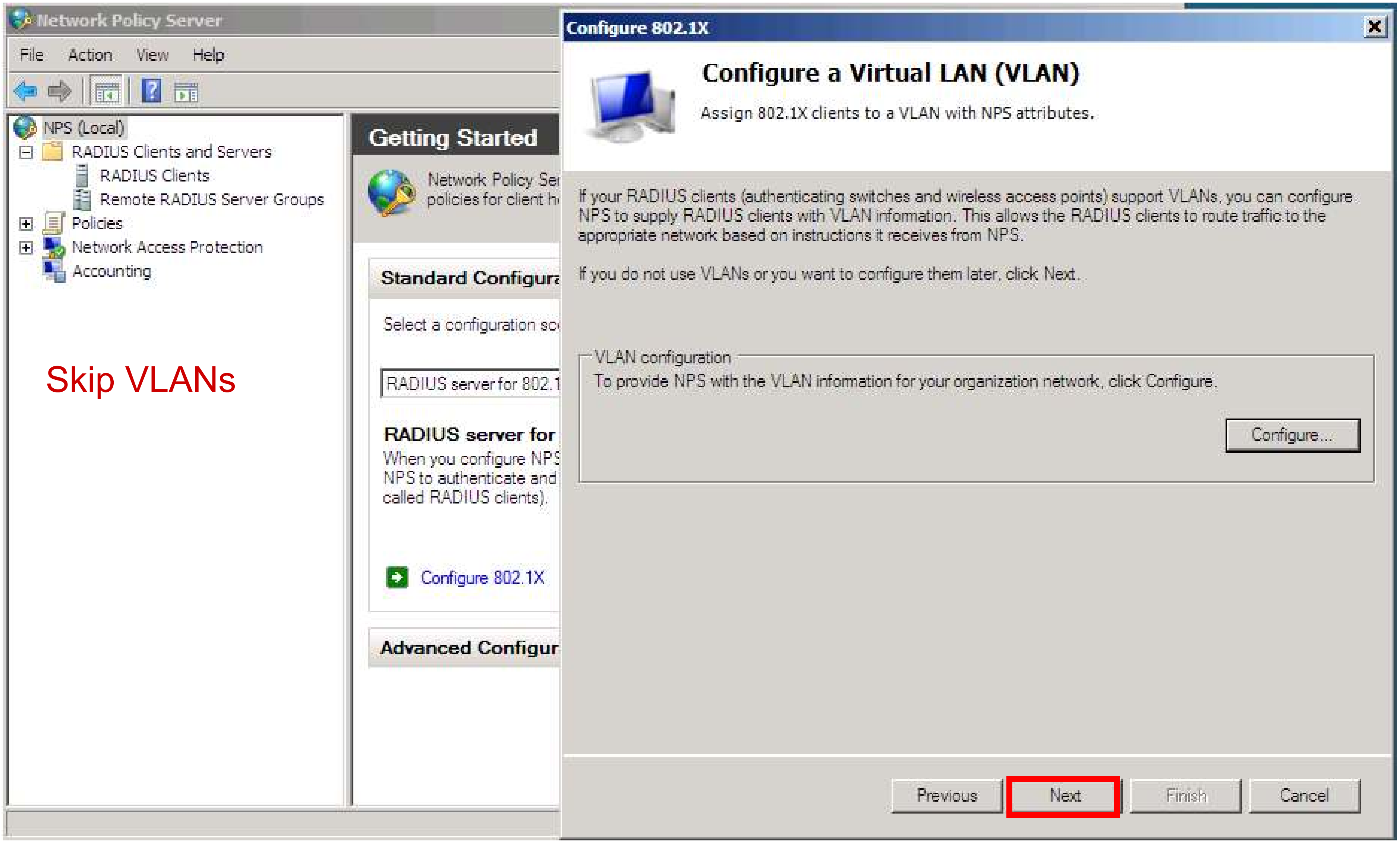


Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Groups
VPRODEMO\Domain Users
VPRODEMO\Domain Computers



Skip VLANs

Configure a Virtual LAN (VLAN)

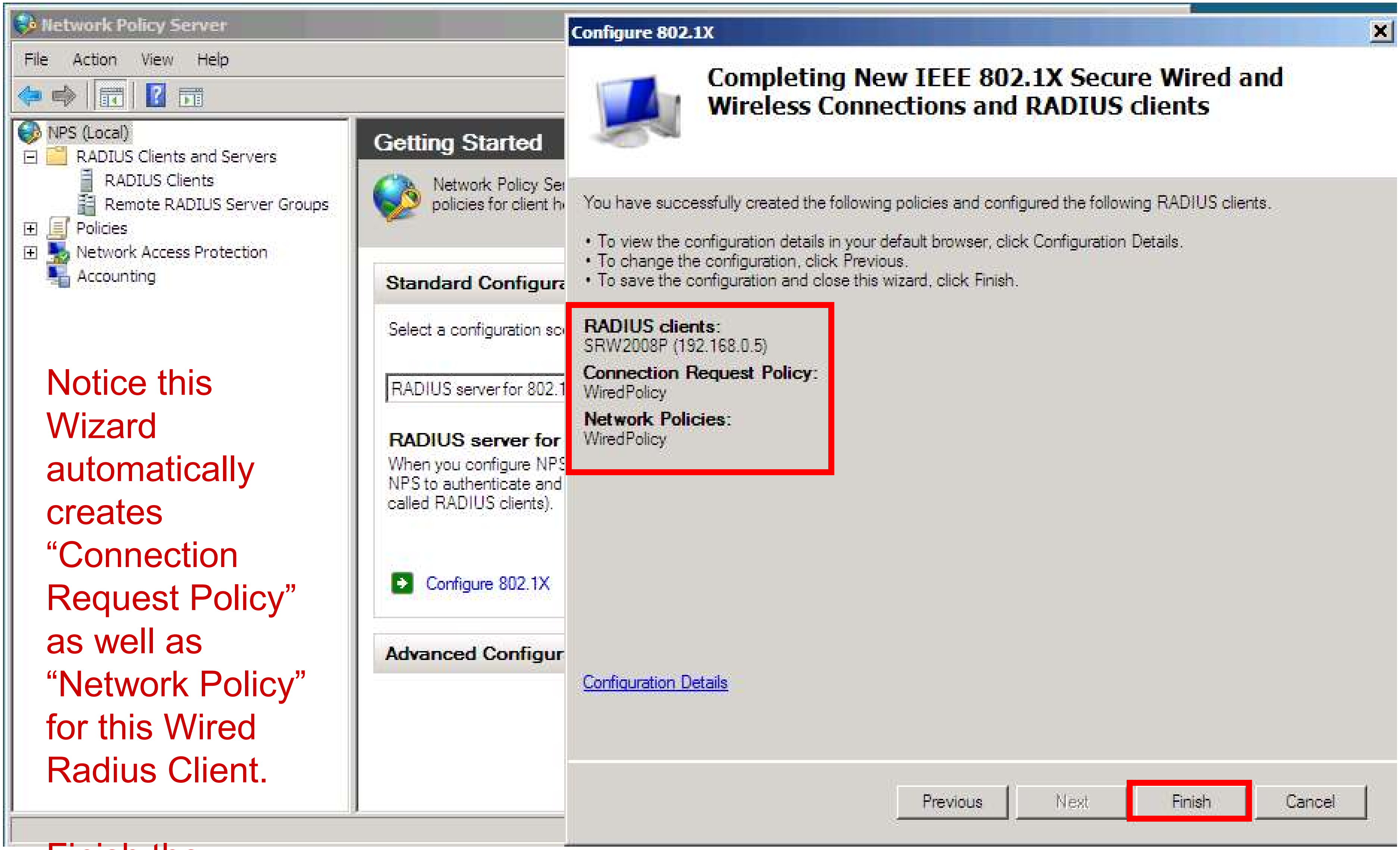
Assign 802.1X clients to a VLAN with NPS attributes.

If your RADIUS clients (authenticating switches and wireless access points) support VLANs, you can configure NPS to supply RADIUS clients with VLAN information. This allows the RADIUS clients to route traffic to the appropriate network based on instructions it receives from NPS.

If you do not use VLANs or you want to configure them later, click Next.

VLAN configuration

To provide NPS with the VLAN information for your organization network, click Configure.



Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients

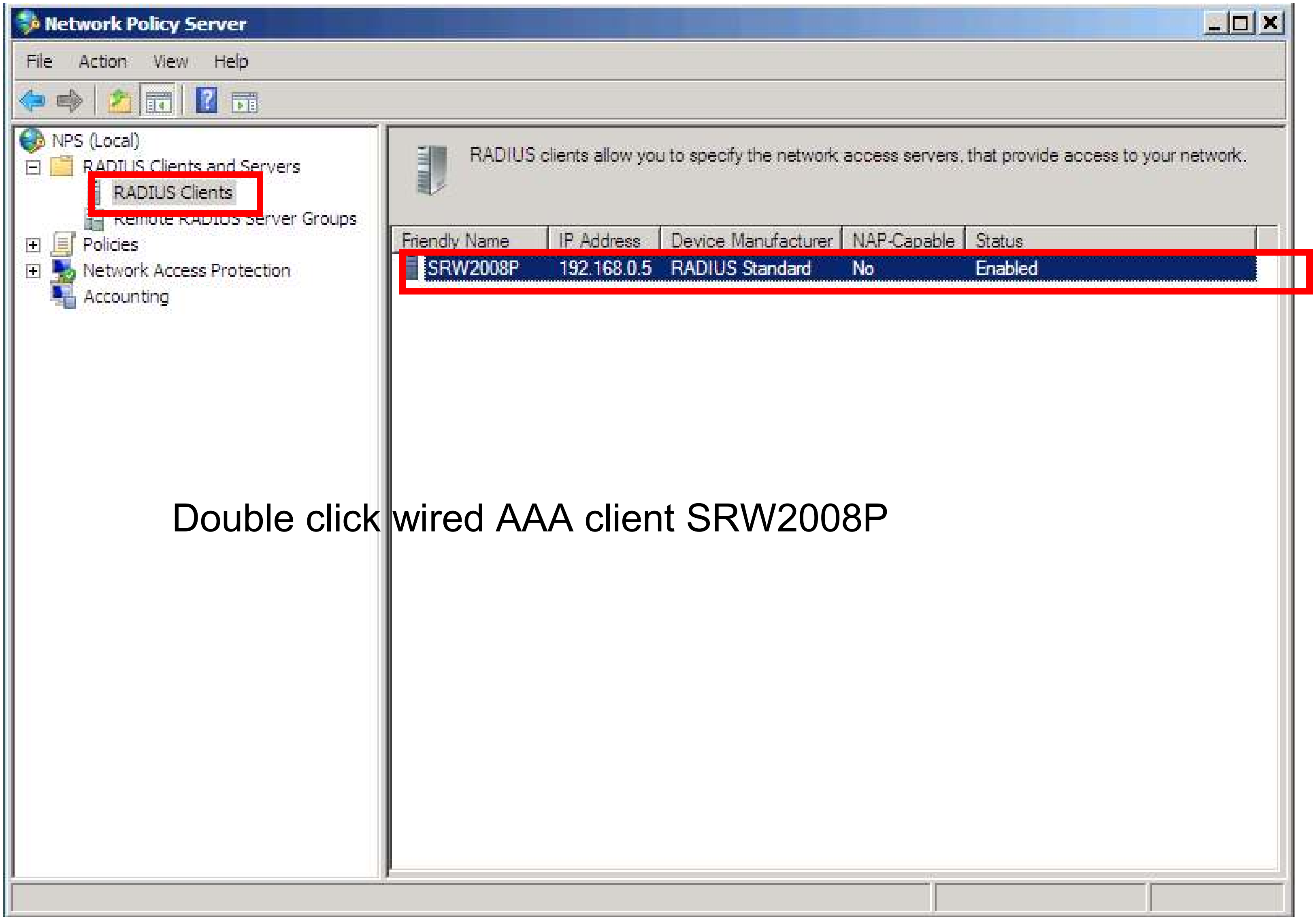
You have successfully created the following policies and configured the following RADIUS clients.

- 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:
SRW2008P (192.168.0.5)
Connection Request Policy:
WiredPolicy
Network Policies:
WiredPolicy

Notice this Wizard automatically creates “Connection Request Policy” as well as “Network Policy” for this Wired Radius Client.

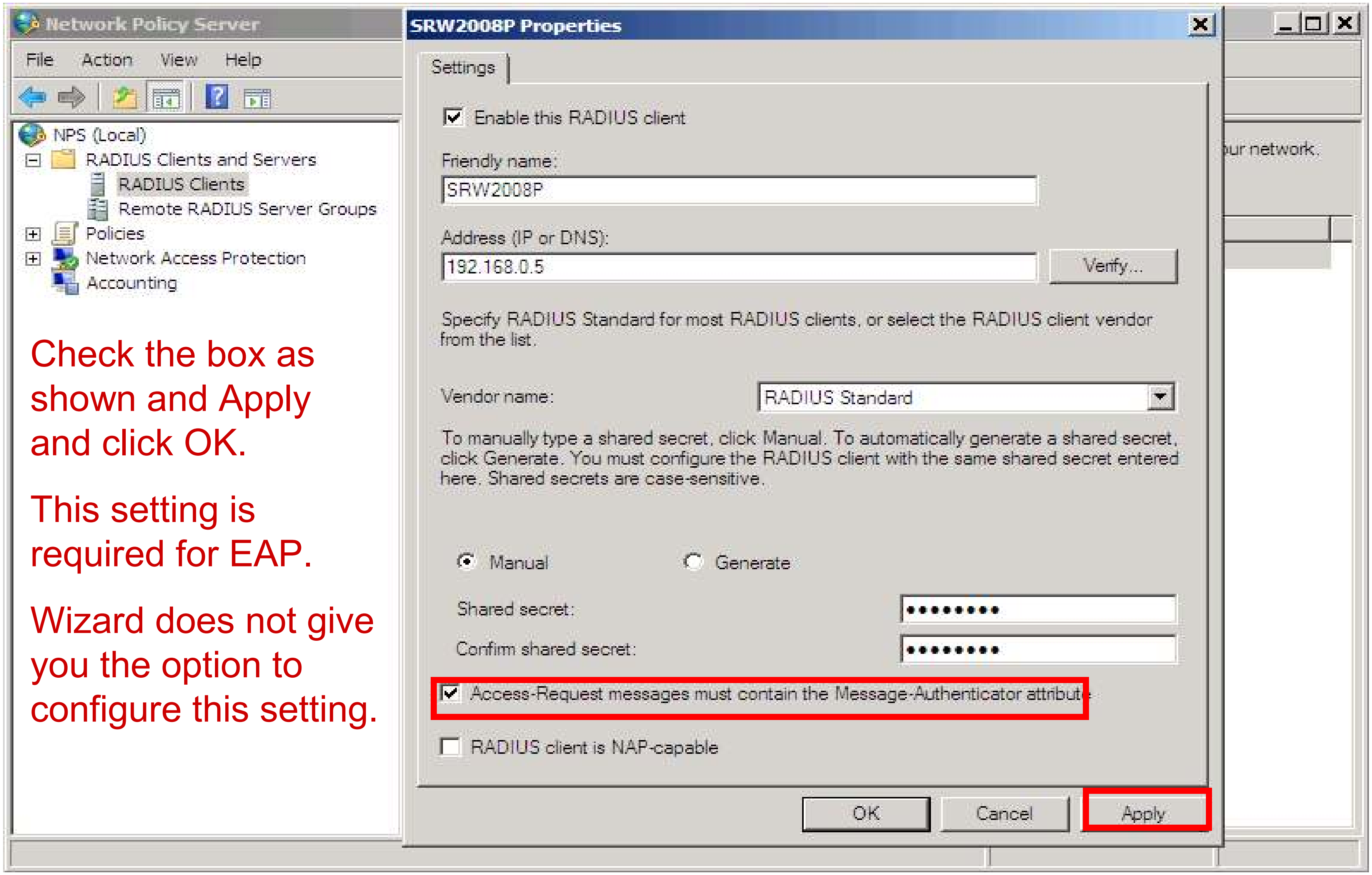
Finish the wizard.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
SRW2008P	192.168.0.5	RADIUS Standard	No	Enabled

Double click wired AAA client SRW2008P



☑ Enable this RADIUS client

Friendly name: SRW2008P

Address (IP or DNS): 192.168.0.5

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••••••

Confirm shared secret: •••••••••

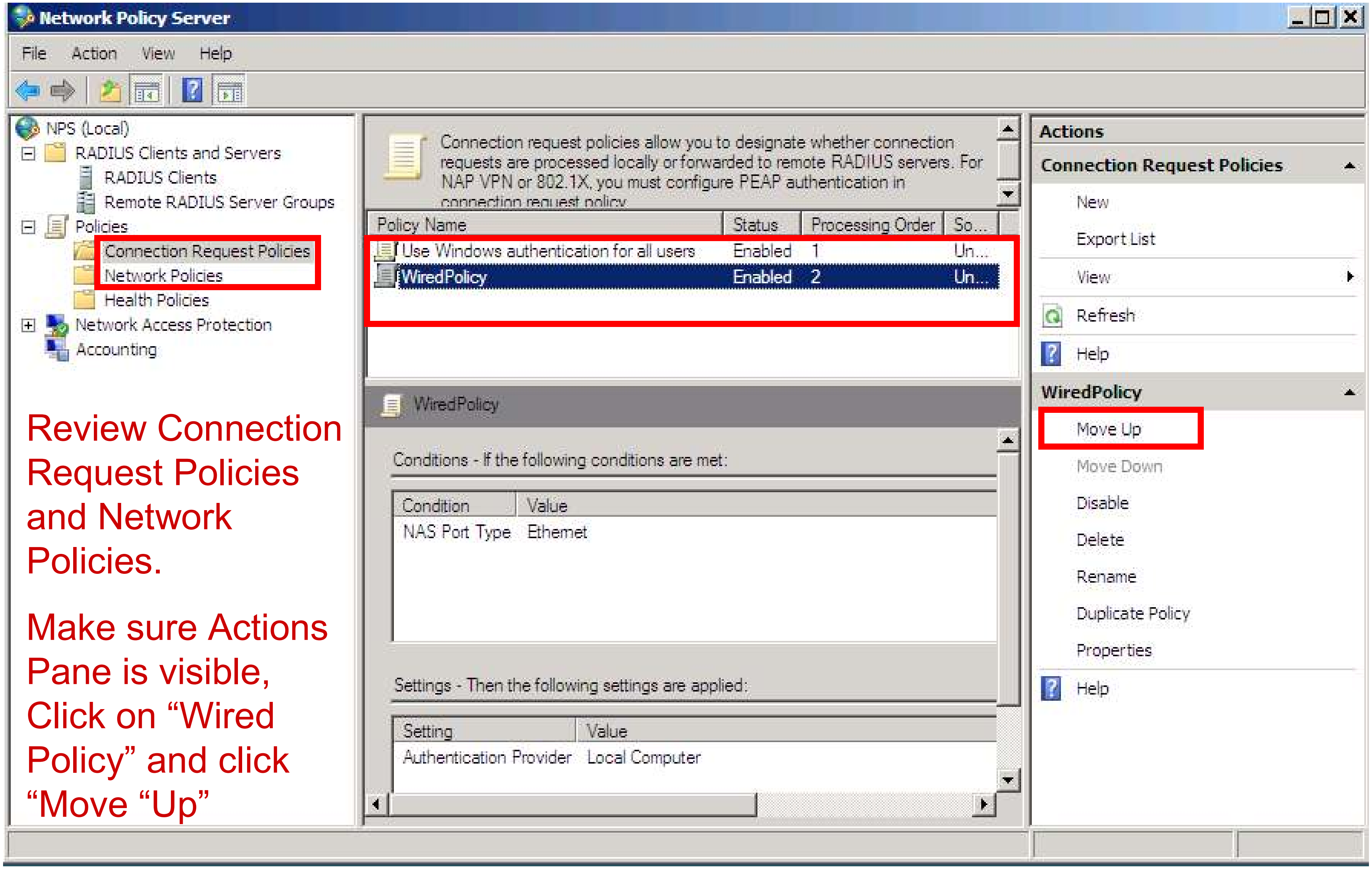
☑ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

Check the box as shown and Apply and click OK.

This setting is required for EAP.

Wizard does not give you the option to configure this setting.



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy

Policy Name	Status	Processing Order	So...
Use Windows authentication for all users	Enabled	1	Un...
WiredPolicy	Enabled	2	Un...

Conditions - If the following conditions are met:

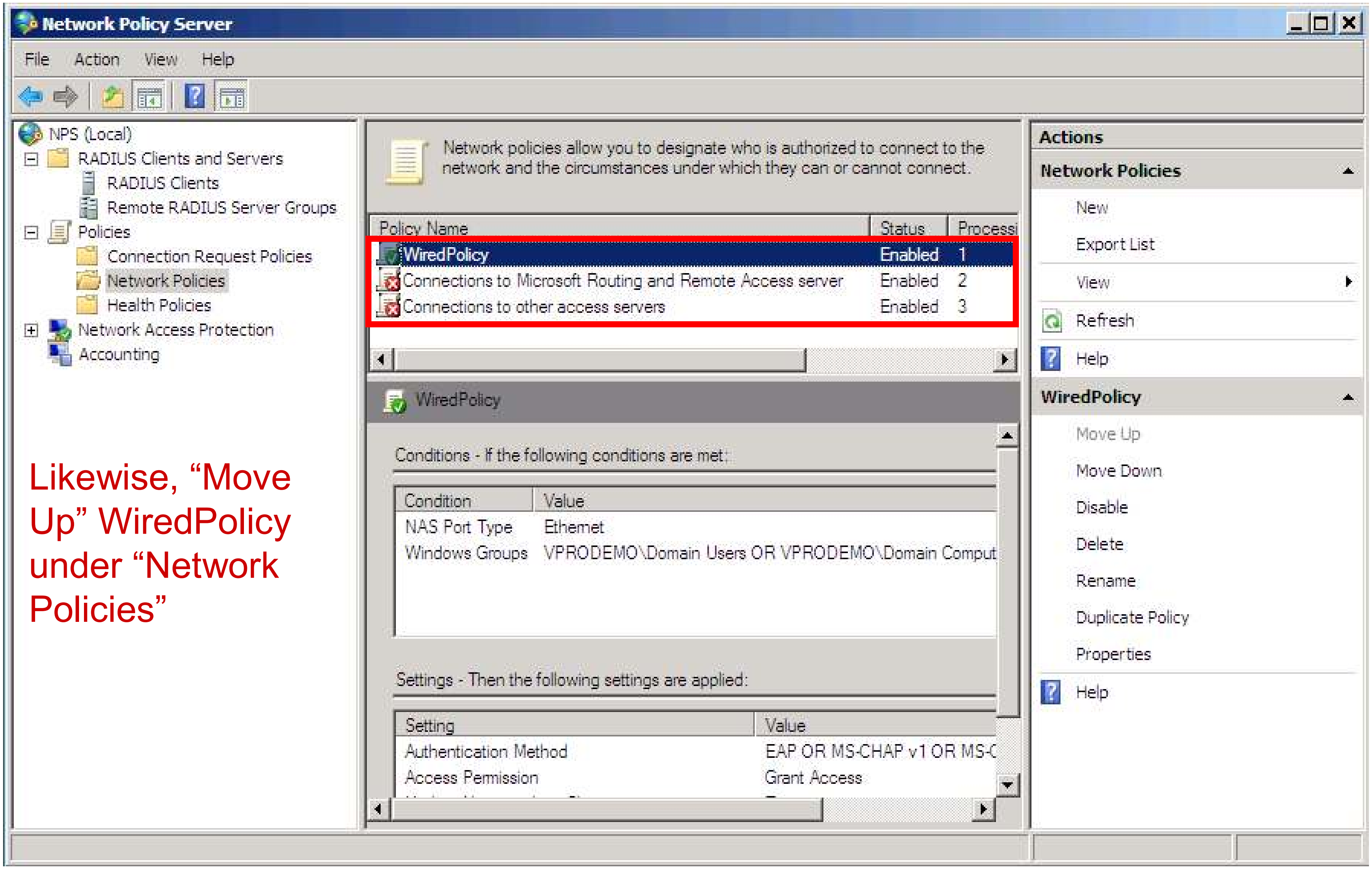
Condition	Value
NAS Port Type	Ethernet

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer

Review Connection Request Policies and Network Policies.

Make sure Actions Pane is visible, Click on “Wired Policy” and click “Move “Up”



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processi
WiredPolicy	Enabled	1
Connections to Microsoft Routing and Remote Access server	Enabled	2
Connections to other access servers	Enabled	3

WiredPolicy

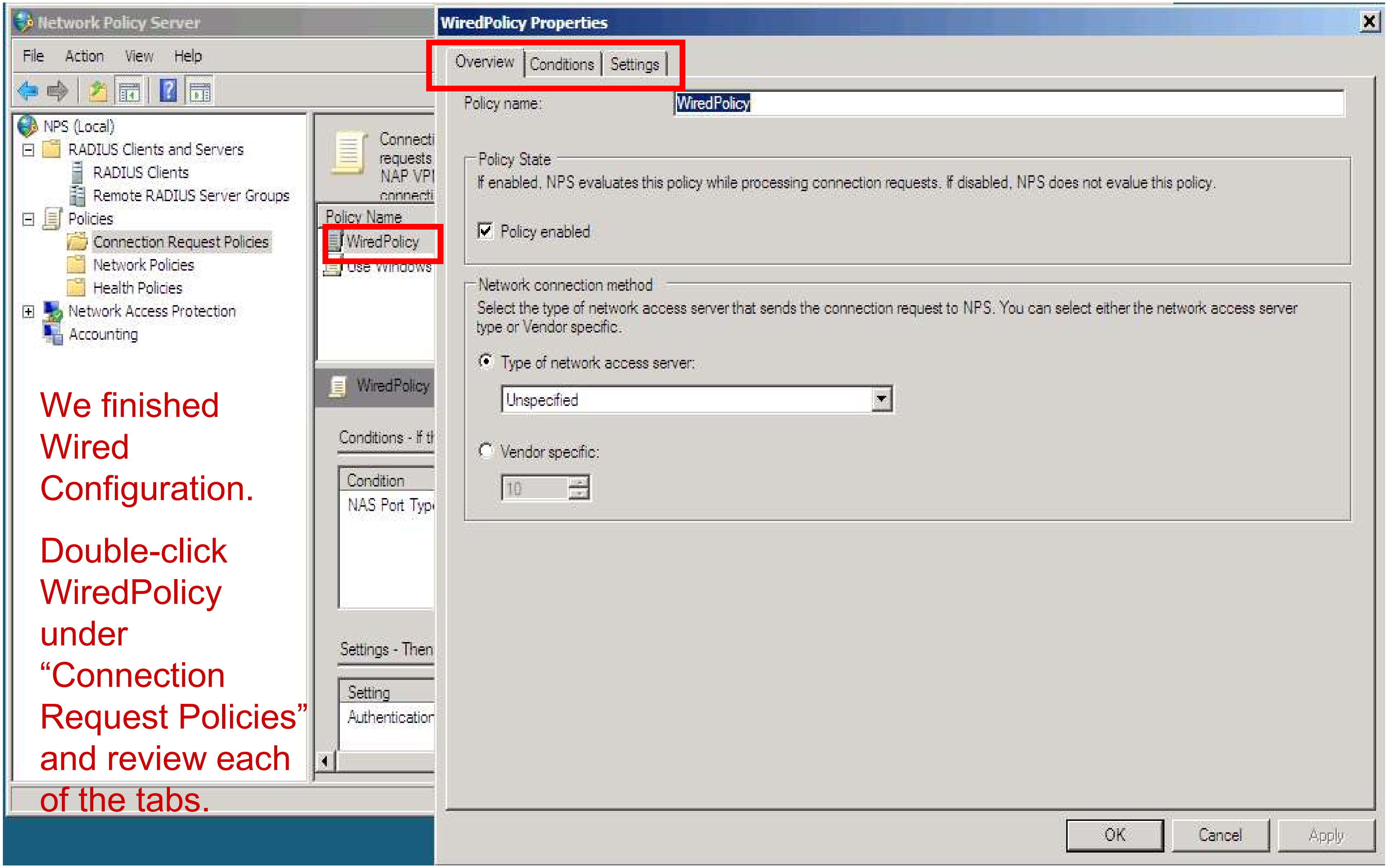
Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Ethernet
Windows Groups	VPRODEMO\Domain Users OR VPRODEMO\Domain Comput

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-C
Access Permission	Grant Access

Likewise, “Move Up” WiredPolicy under “Network Policies”



WiredPolicy Properties

Policy name: WiredPolicy

Policy State

If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.

☑ Policy enabled

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server:

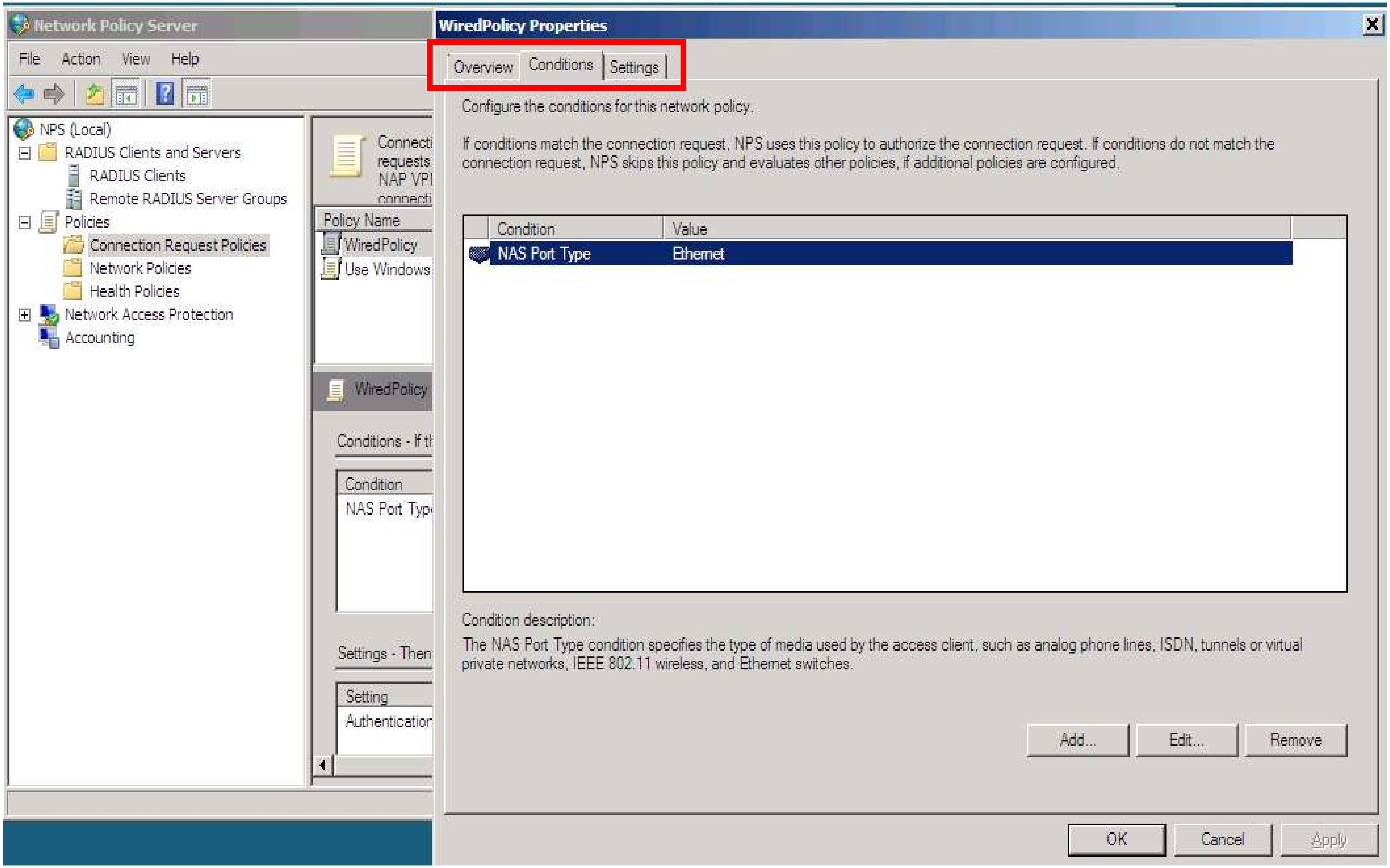
Unspecified

○ Vendor specific:

10

We finished Wired Configuration.

Double-click WiredPolicy under "Connection Request Policies" and review each of the tabs.



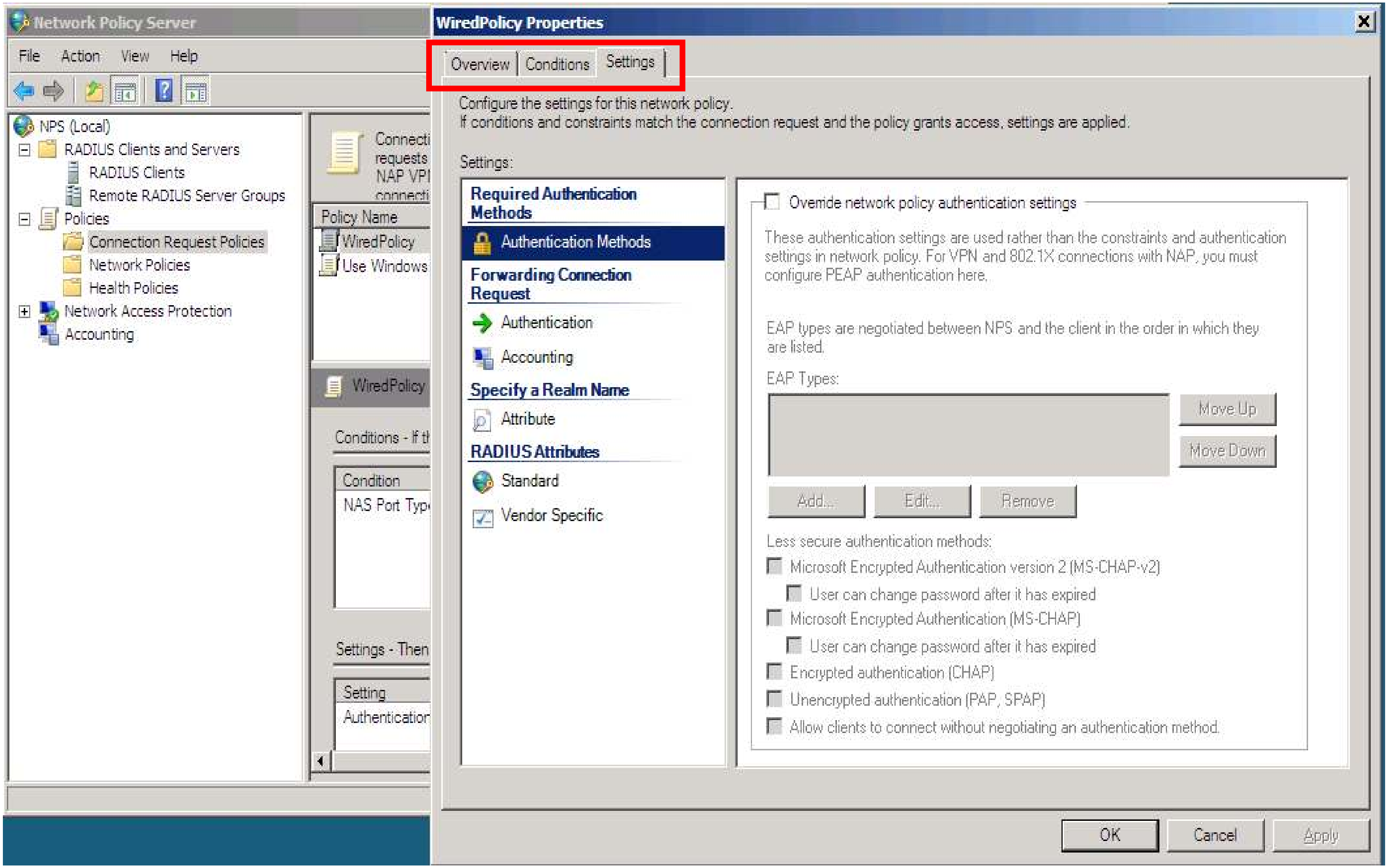
Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Ethernet

Condition description:

The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

□ Override network policy authentication settings

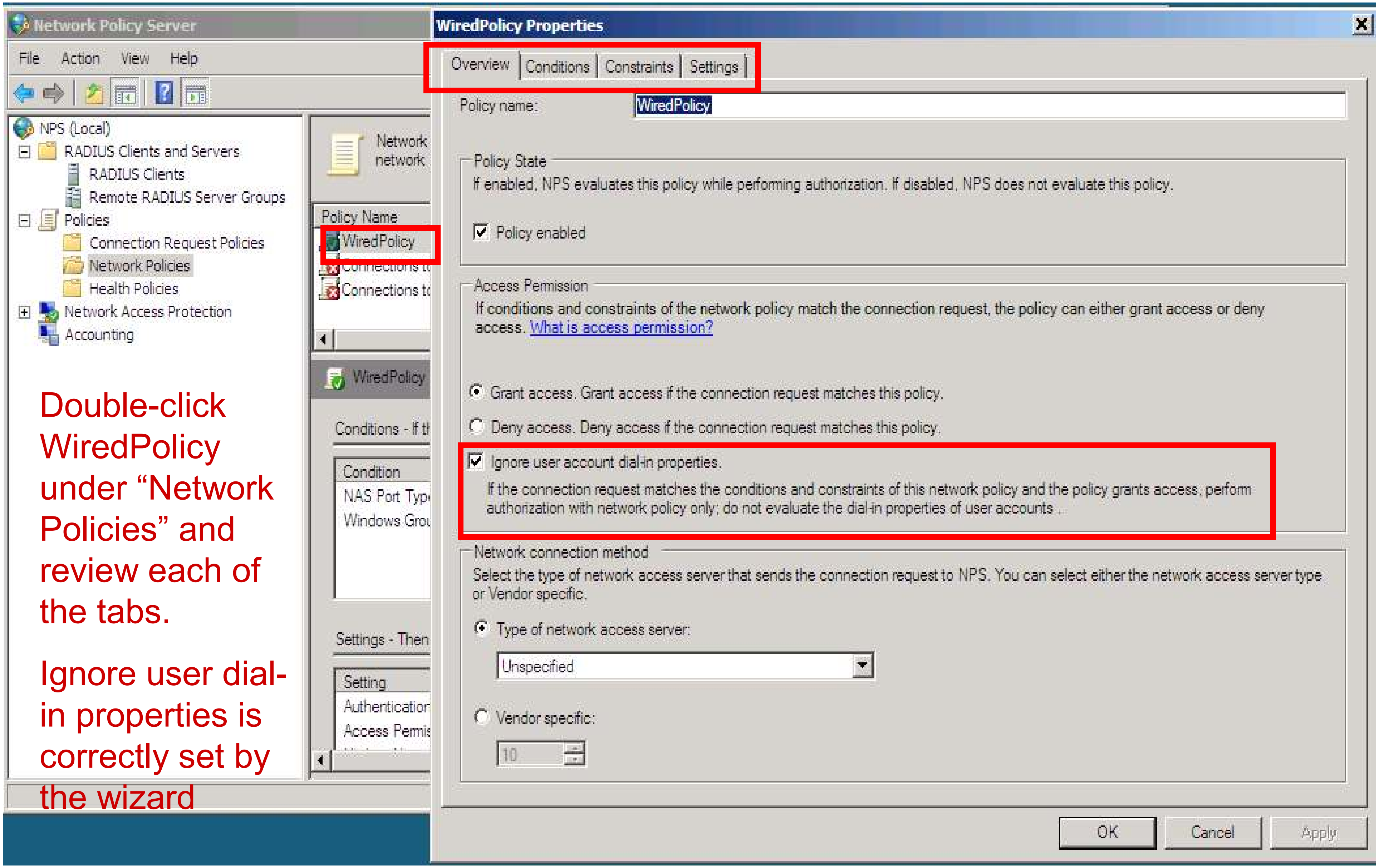
These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

- □ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - □ User can change password after it has expired
- □ Microsoft Encrypted Authentication (MS-CHAP)
  - □ User can change password after it has expired
- □ Encrypted authentication (CHAP)
- □ Unencrypted authentication (PAP, SPAP)
- □ Allow clients to connect without negotiating an authentication method.



WiredPolicy Properties

Policy name: WiredPolicy

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

☑ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server:

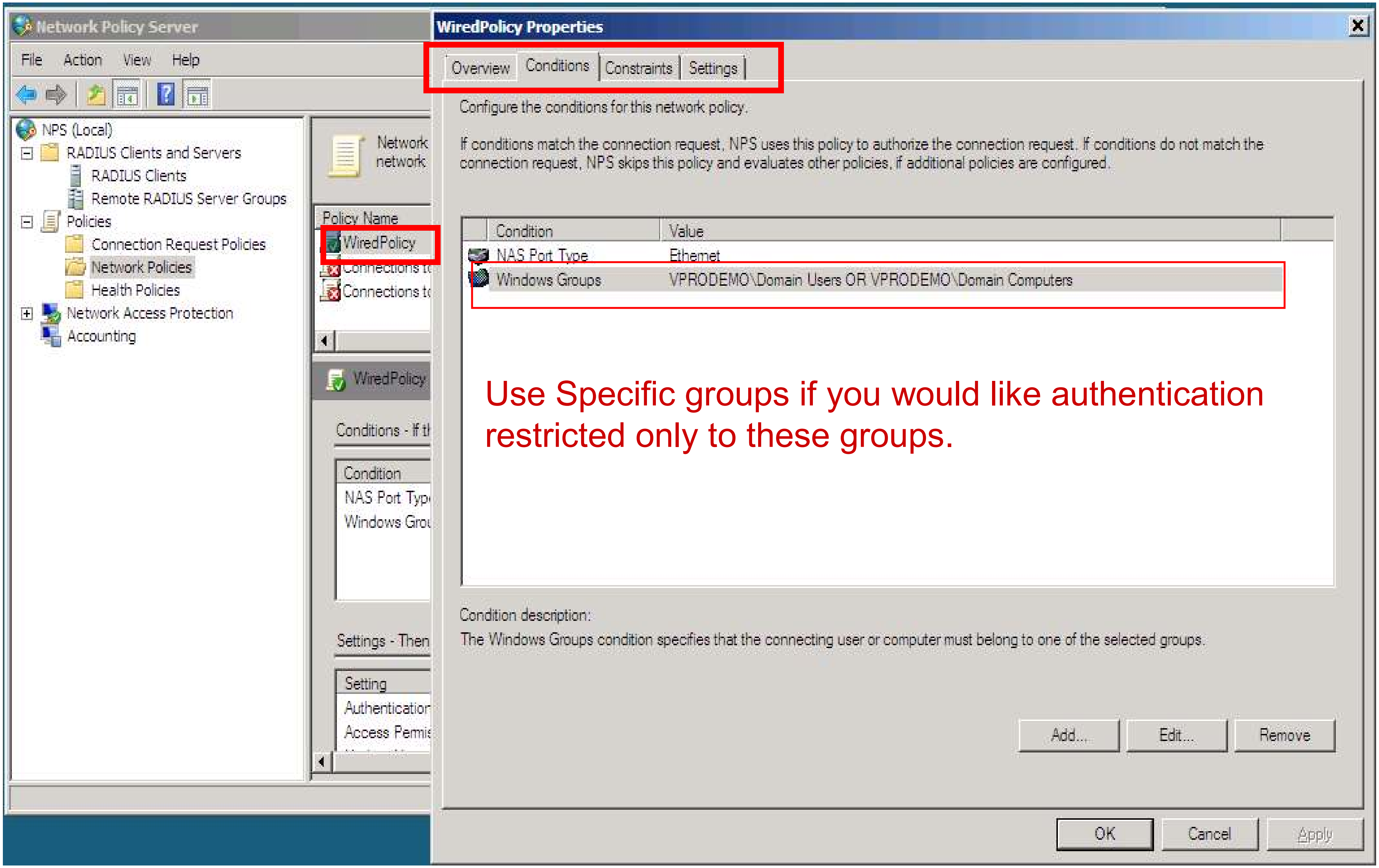
Unspecified

○ Vendor specific:

10

Double-click WiredPolicy under "Network Policies" and review each of the tabs.

Ignore user dial-in properties is correctly set by the wizard



Configure the conditions for this network policy.

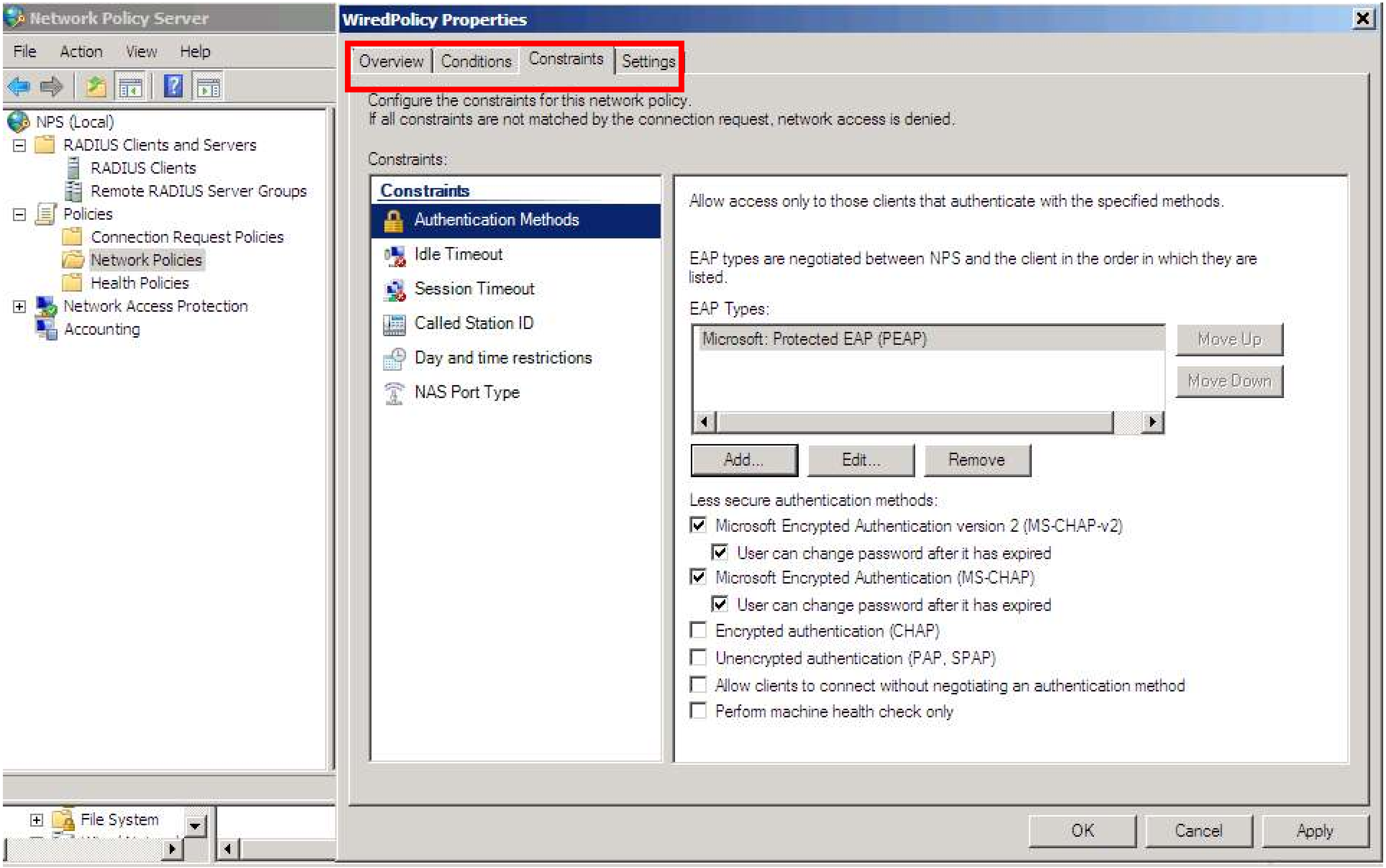
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Ethernet
Windows Groups	VPRODEMO\Domain Users OR VPRODEMO\Domain Computers

Condition description:

The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Use Specific groups if you would like authentication restricted only to these groups.



WiredPolicy Properties

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Authentication Methods
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☑ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

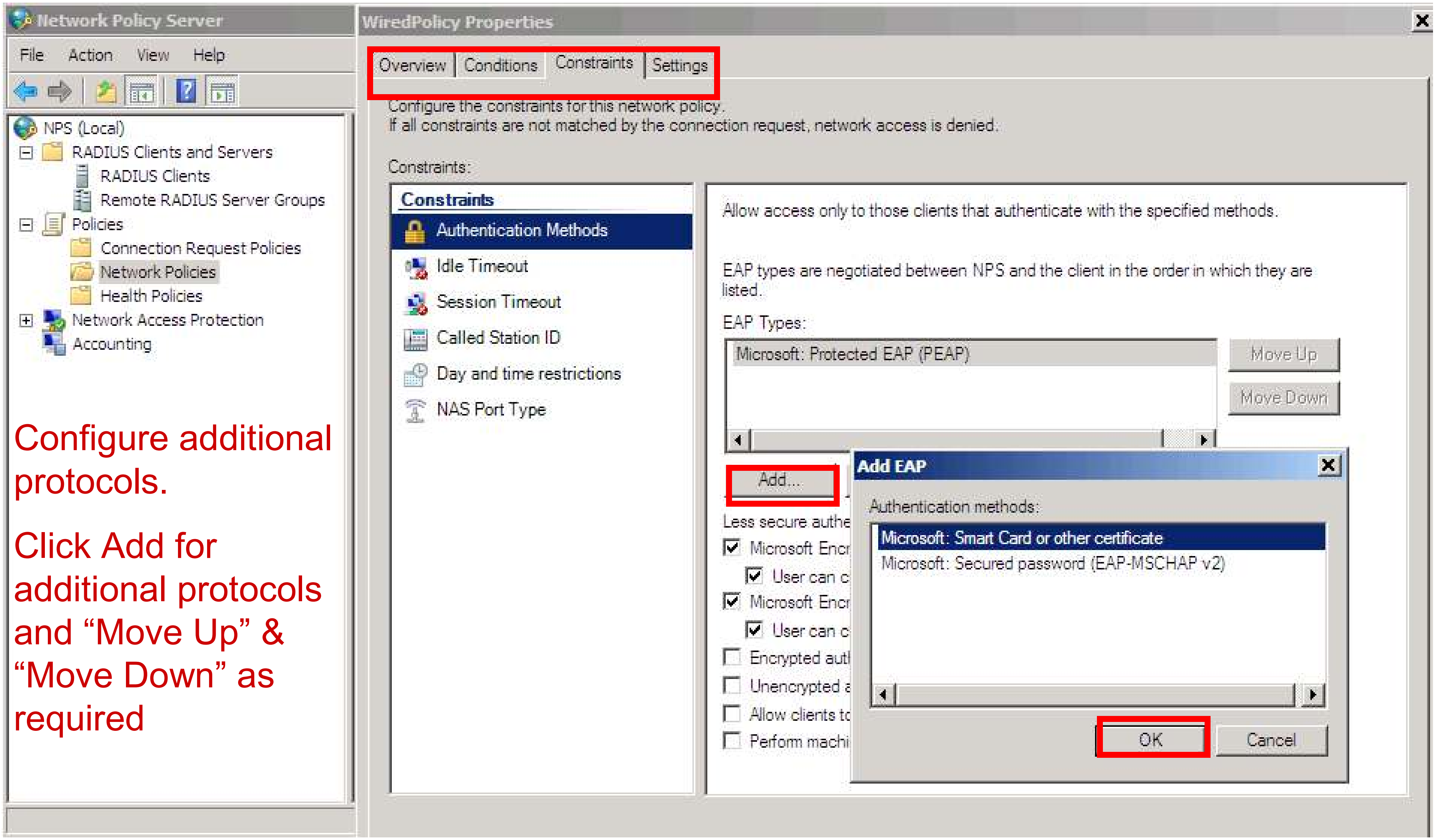
☑ User can change password after it has expired

☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method

☐ Perform machine health check only



Network Policy Server

File Action View Help

NPS (Local)
- RADIUS Clients and Servers
  - RADIUS Clients
  - Remote RADIUS Server Groups
- Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
- Accounting

WiredPolicy Properties

Overview | Conditions | Constraints | Settings

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints
- Authentication Methods
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP)

Less secure authe

☑ Microsoft Encr

☑ User can c

☑ Microsoft Encr

☑ User can c

☐ Encrypted aut

☐ Unencrypted a

☐ Allow clients to

☐ Perform machi

Add EAP

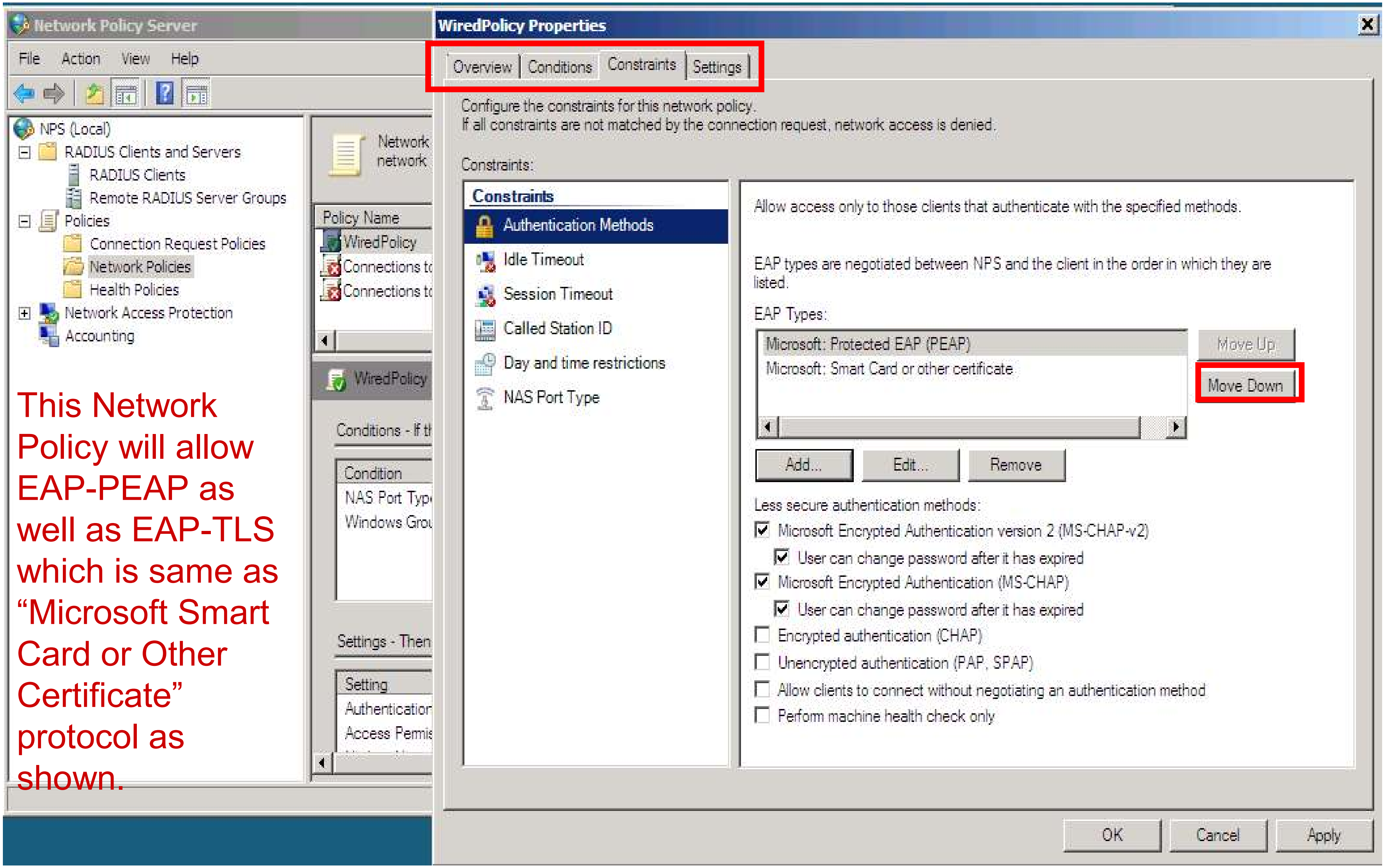
Authentication methods:

Microsoft: Smart Card or other certificate

Microsoft: Secured password (EAP-MSCHAP v2)

Configure additional protocols.

Click Add for additional protocols and “Move Up” & “Move Down” as required



Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

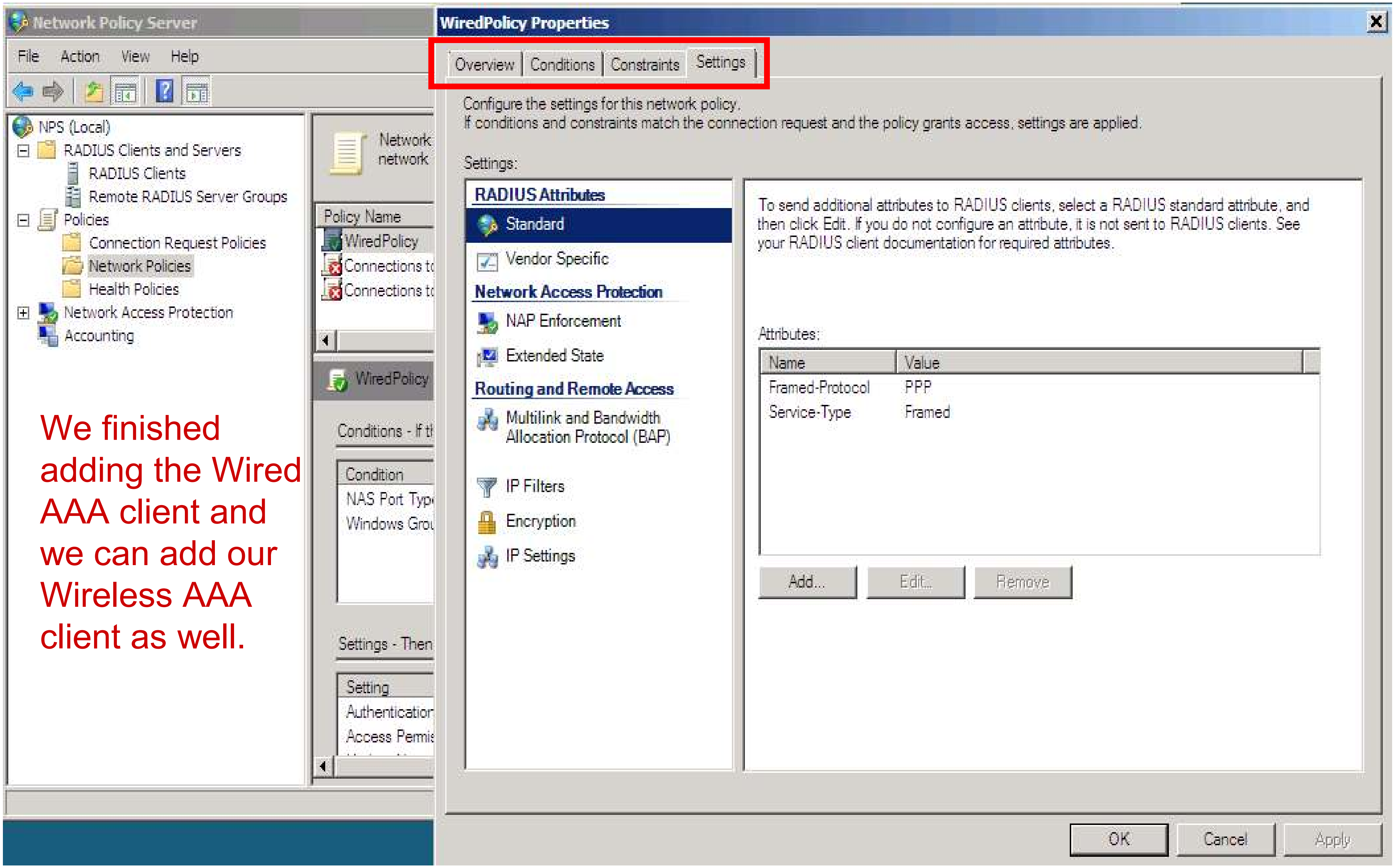
EAP Types:

Microsoft: Protected EAP (PEAP)
Microsoft: Smart Card or other certificate

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  ☑ User can change password after it has expired
☑ Microsoft Encrypted Authentication (MS-CHAP)
  ☑ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method
☐ Perform machine health check only

This Network Policy will allow EAP-PEAP as well as EAP-TLS which is same as “Microsoft Smart Card or Other Certificate” protocol as shown.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

We finished adding the Wired AAA client and we can add our Wireless AAA client as well.