

802.1x authentication with GNS3 windows 2012 and windows 7 client

pre-requirements

- VirtualBox 4.2.4 or later (www.virtualbox.org)
- GNS3 (www.gns3.org)
- windows 2012 installed to a virtual machine, and configured as DC
- a windows 7 client installed to a virtual machine, and member of the bomain

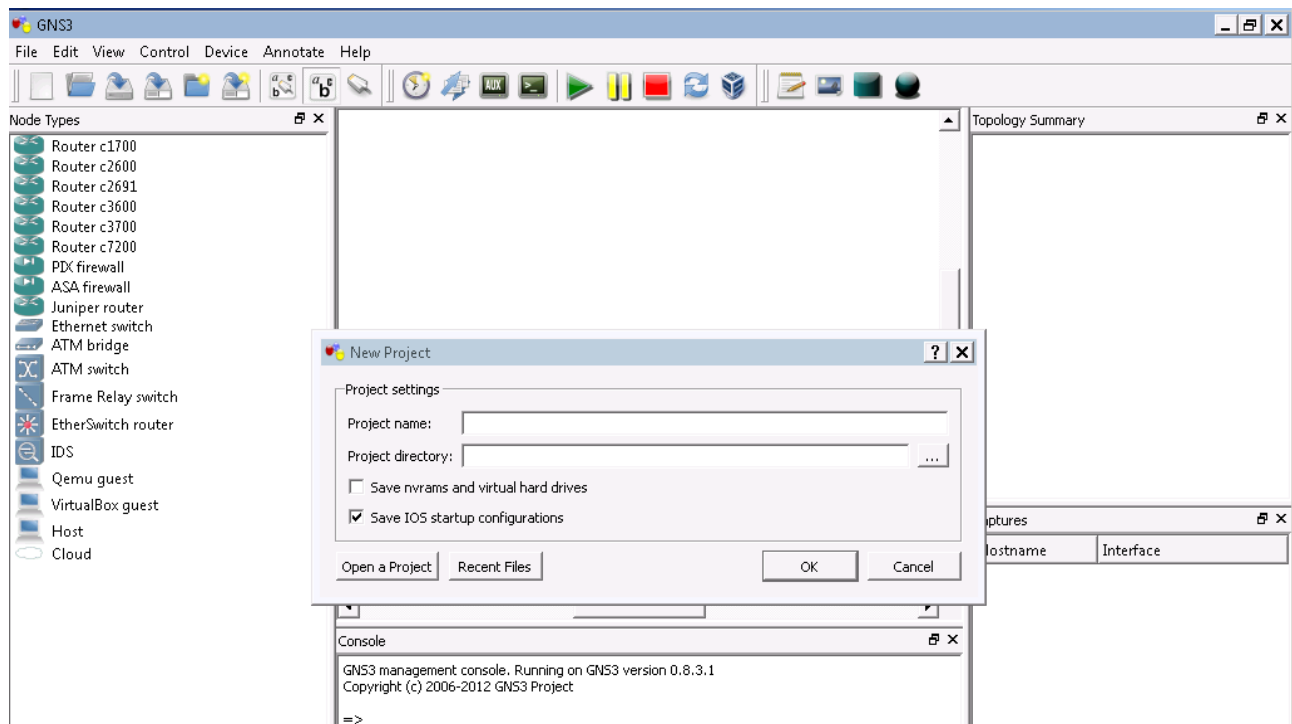
Table of Contents

pre-requirements.....	1
Environment setup.....	3
GNS3.....	3
Add the virtual machines.....	9
Connect the virtual machines to the virtual etherswitch router.....	11
Start the virtual devices.....	13
Install the Network Policy Server (RADIUS) to windows 2012.....	16
Install the Certificate Server to Windows 2012.....	22
Configure the certificate authority.....	36
Configure the RADIUS server.....	38
Set up the switch as RADIUS client.....	38
Set up the Connection Request Policy on the RADIUS Server.....	41
Set up the Network Policy on the RADIUS Server.....	48
Configure the EtherSwitch router for 802.1x.....	73
Test the 802.1x authentication on the client.....	77
NAP with DHCP enforce.....	85
Set up DHCP server on the windows 2012 machine.....	85
Set up the DHCP relay on the switch.....	92
Add the “Health roles” to the already installed NAP Service.....	93
Group policy settings for DHCP and 802.1x enforce.....	103
Set up the NAP capability on the DHCP.....	112
Set up the NAP on the NPS server.....	120
Create a Remediation Server Group.....	120
Set up windows security health.....	122
Create Health policy.....	124
Create Network Policy.....	127
Create the second Network policy for non compliant machines.....	136
NAP with 802.1x enforce.....	146
Turn off the NAP on the DHCP scope.....	146
Enable the EAP Quarantine enforcement client by group policy.....	148
Enable the NAP capability on the client computers network card.....	157
Set up the NPS server manually.....	160
Disable the previous DHCP Network policy rules.....	160
Modify the 802.1x authentication Network Policy, to check the health too.....	162
Create a new Network policy rule for the non compliant machines.....	167
Create Connection Policy on the NPS server.....	195
Set up the NPS by wizard.....	200

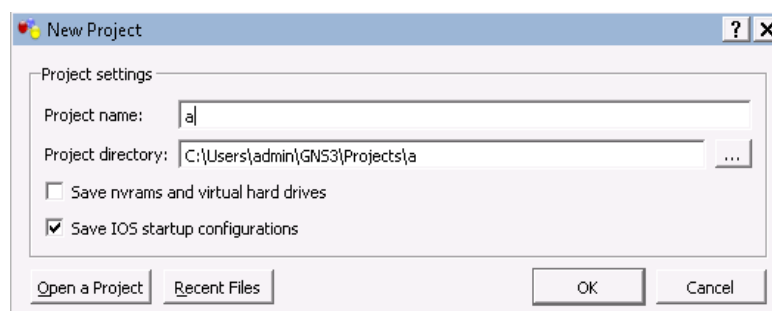
Environment setup

GNS3

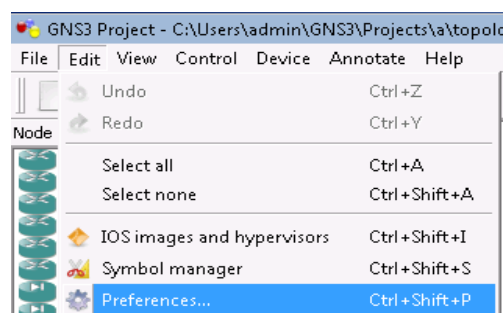
1. Start the GNS3. It will ask for a project name and directory.



2. Give it any name and directory

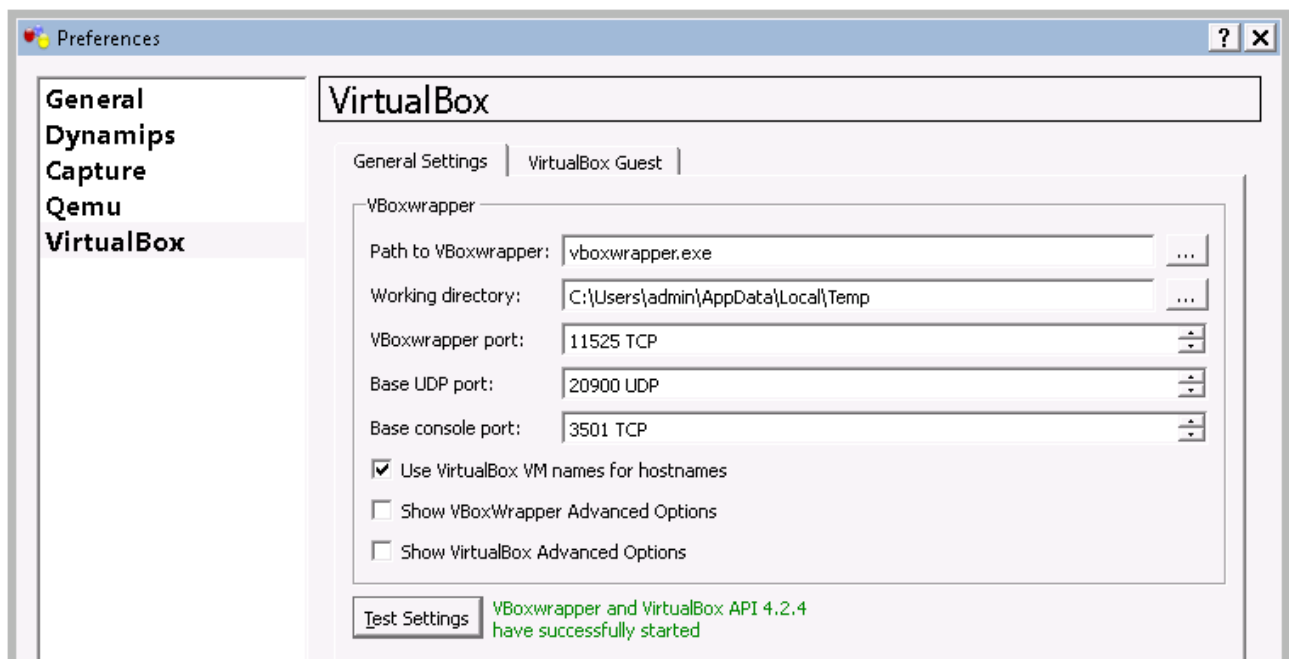


3. Select Edit / Preferences, to test and set up the virtualbox integration.

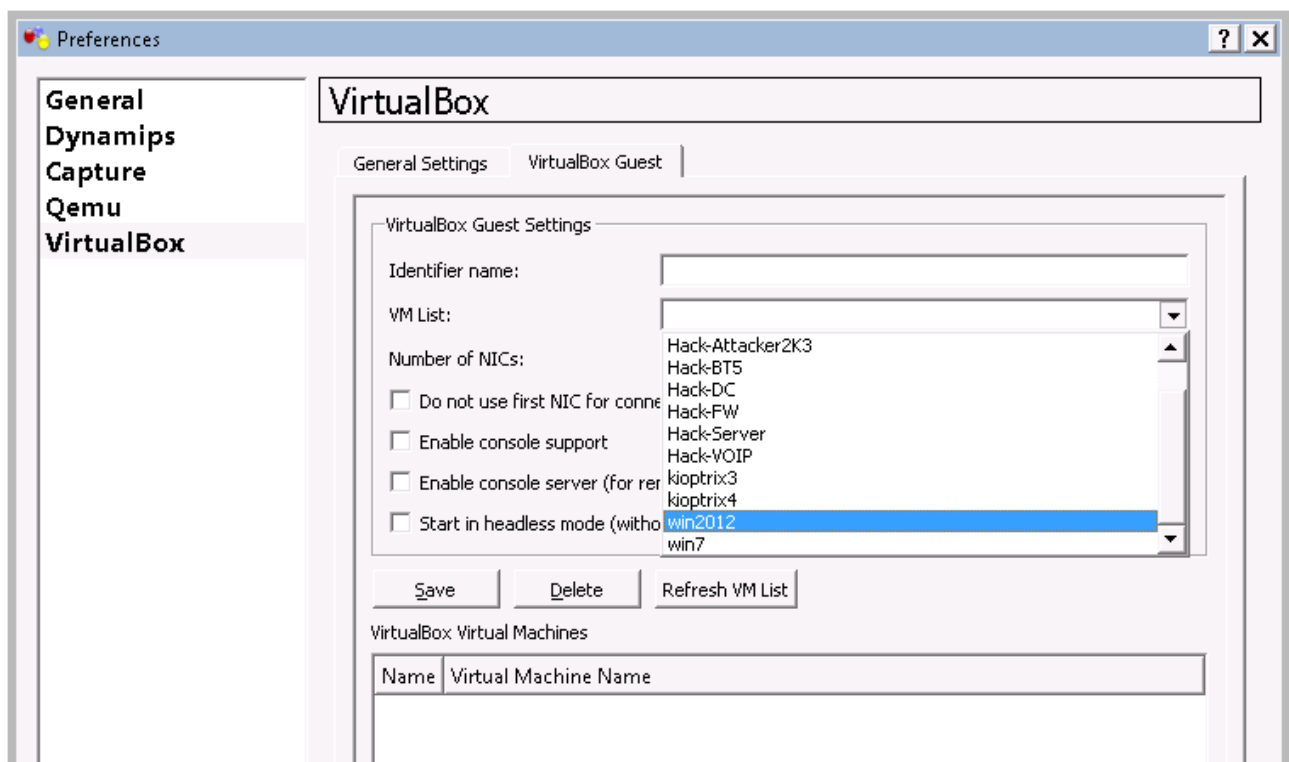


4. On the preferences window select Virtualbox, and on the „General Settings” tab click on the test

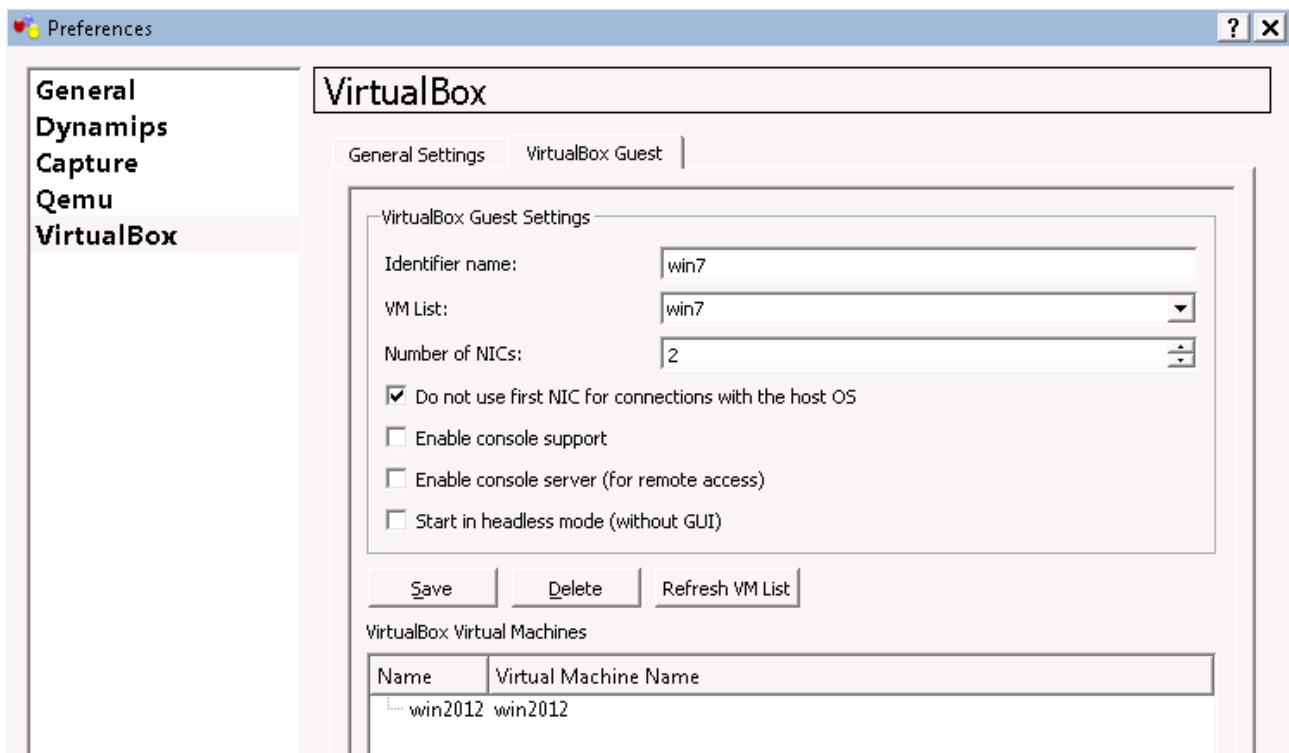
settings button. Hopefully the virtualbox API works fine. If not try to reinstall the GNS3 (I recommend to use the all in one installation package).



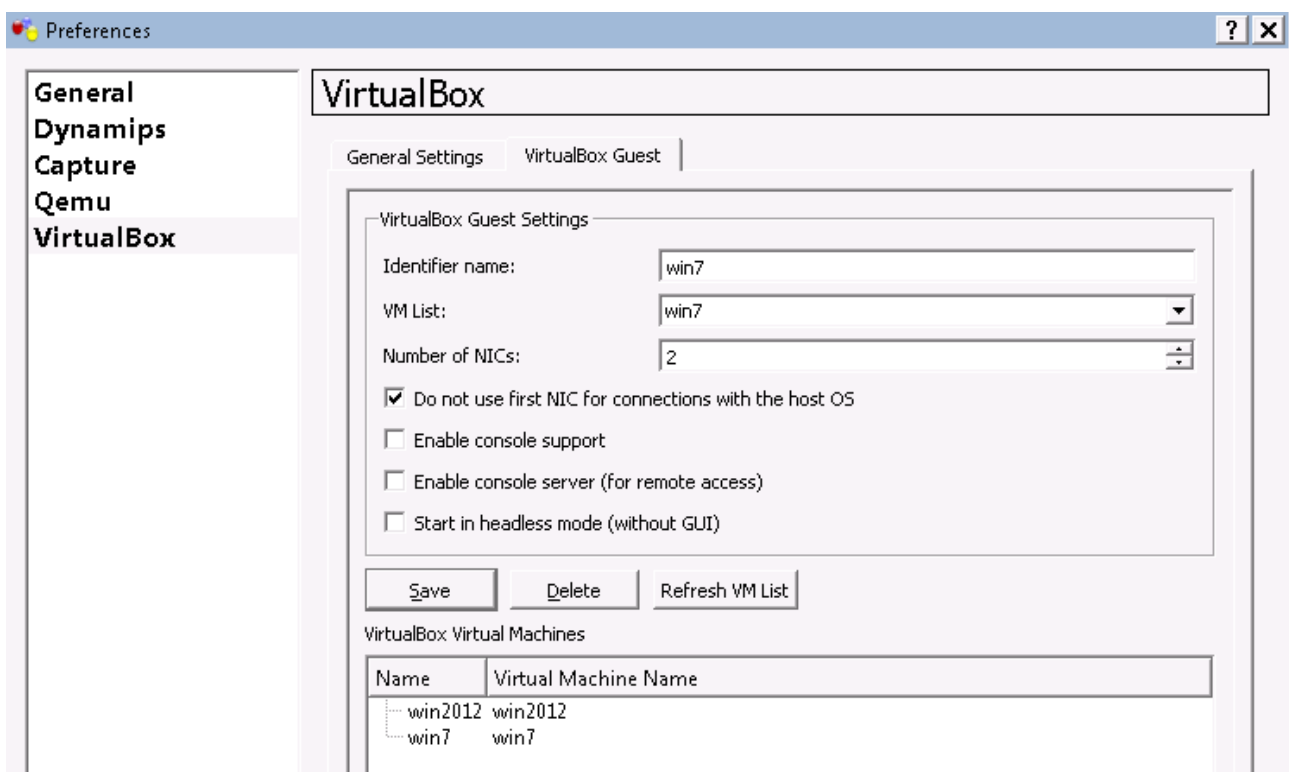
5. Open the „VM List” combobox, and select the virtual machine what you want to add. We will add two virtualmachines, then win2012 and the win7:



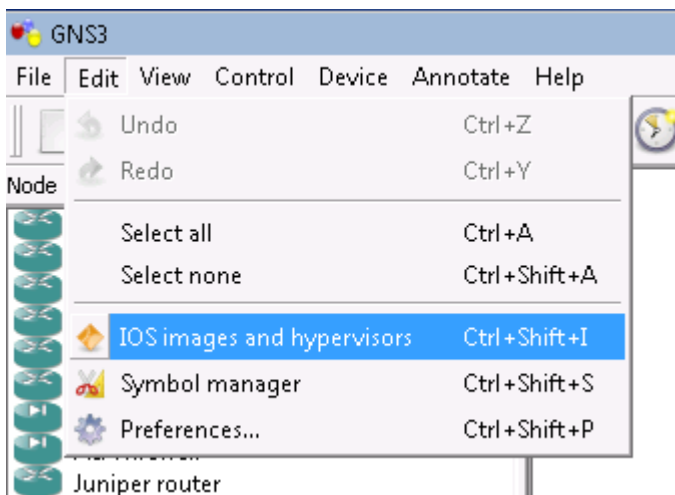
6. We want to simulate a network, and do not want to connect out of the virtual environment so check the „Do not use first NIC for connections with the host OS” box, then click to the „Save” button.



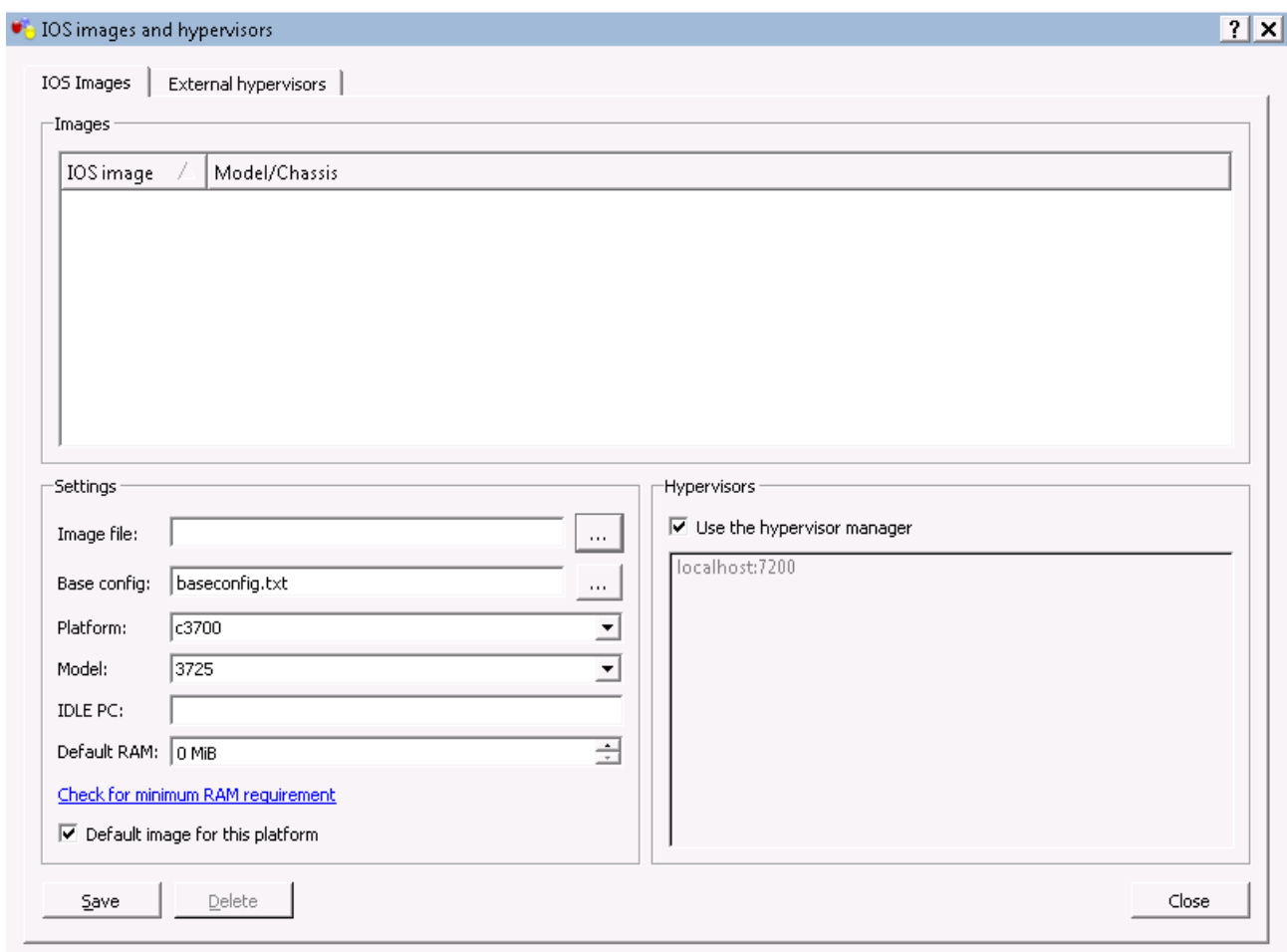
7. Similarly add the win7 machine:



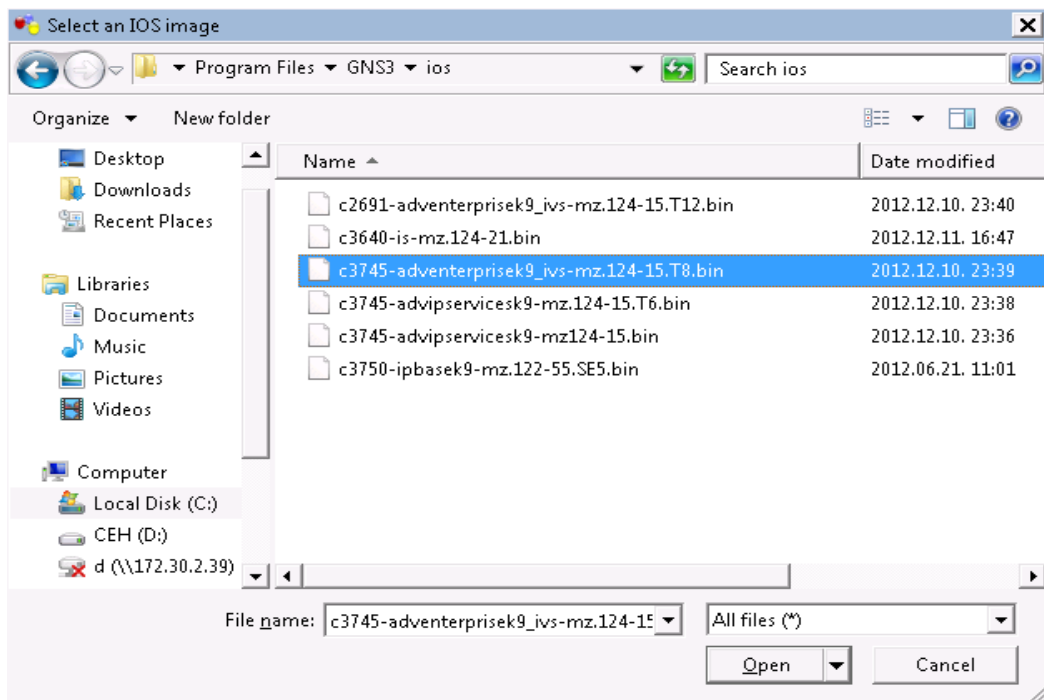
8. Now we have to add an IOS image to the GNS3. Borrow one from your company, then click to the Edit / „IOS images and hypervisors”



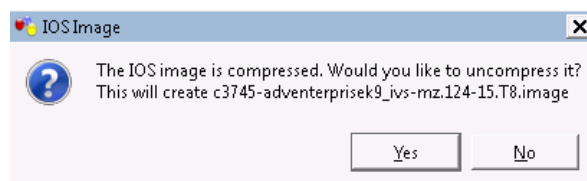
9. Click to the „...” icon next to the „Image File”



10. Select your borrowed image file, then click to the open button:



11. If the image should be decompressed, just click to the yes button.



12. click to the “Save” button. You will see a warning message: “Warning: IDLE PC will have to be configured”, we will deal it later. Finally click to the “Close” button.

IOS images and hypervisors

IOS Images

External hypervisors

Images

IOS image	Model/Chassis
127.0.0.1:C:\Program Files\GNS3\ios\c3745-adventerprisek9_jvs-mz.124-15.T8.image	3745

Settings

Image file:

s\c3745-adventerprisek9_jvs-mz.124-15.T8.image

...

Base config:

baseconfig.txt

...

Platform:

c3700

Model:

3745

IDLE PC:

Default RAM:

128 MIB

[Check for minimum RAM requirement](#)

☒ Default image for this platform

Hypervisors

☒ Use the hypervisor manager

localhost:7200

Save

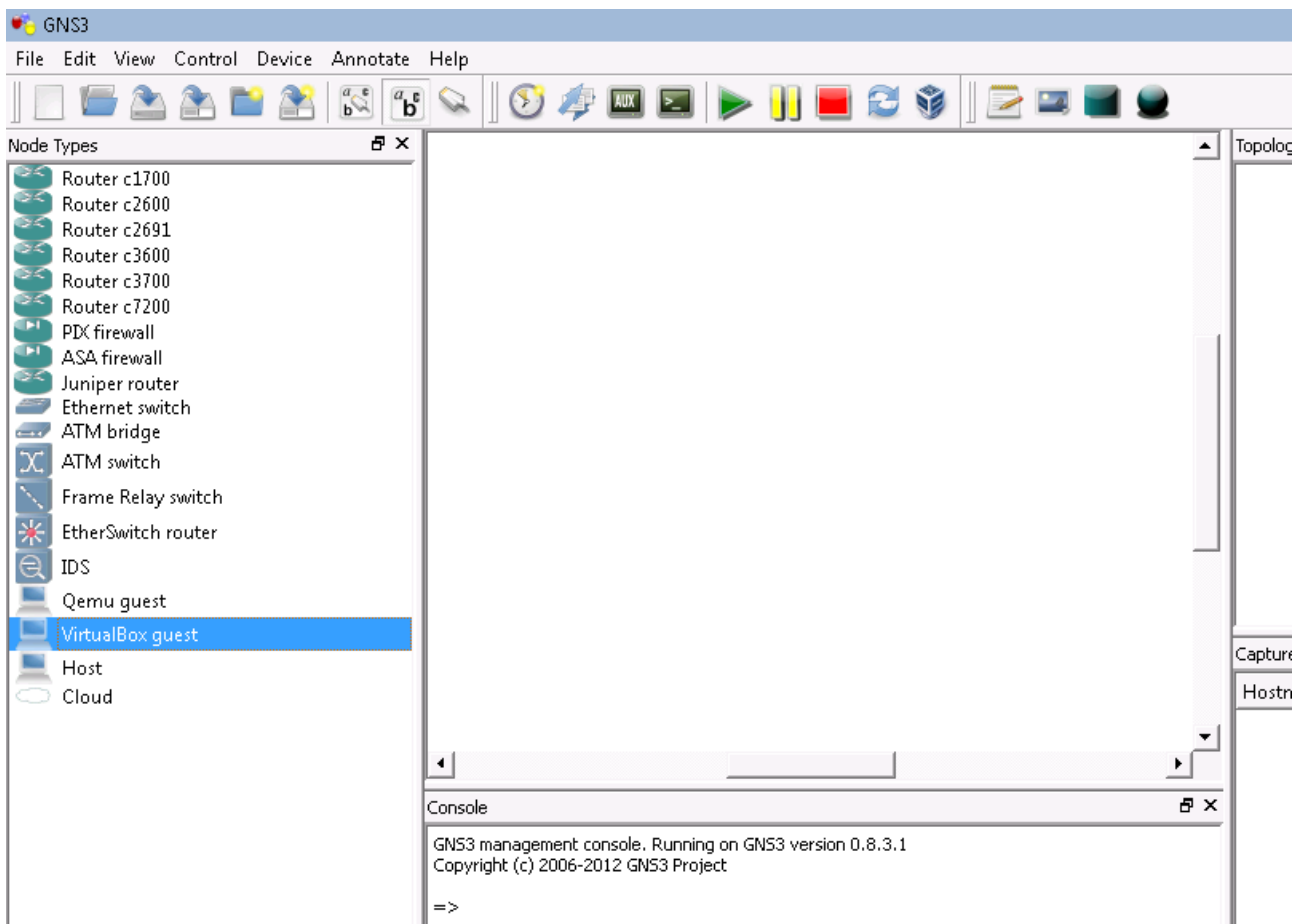
Delete

Warning: IDLE PC will have to be configured! [Find out why and how](#)

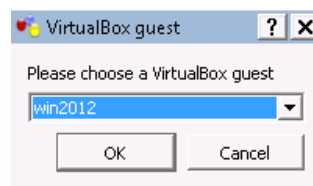
Close

Add the virtual machines

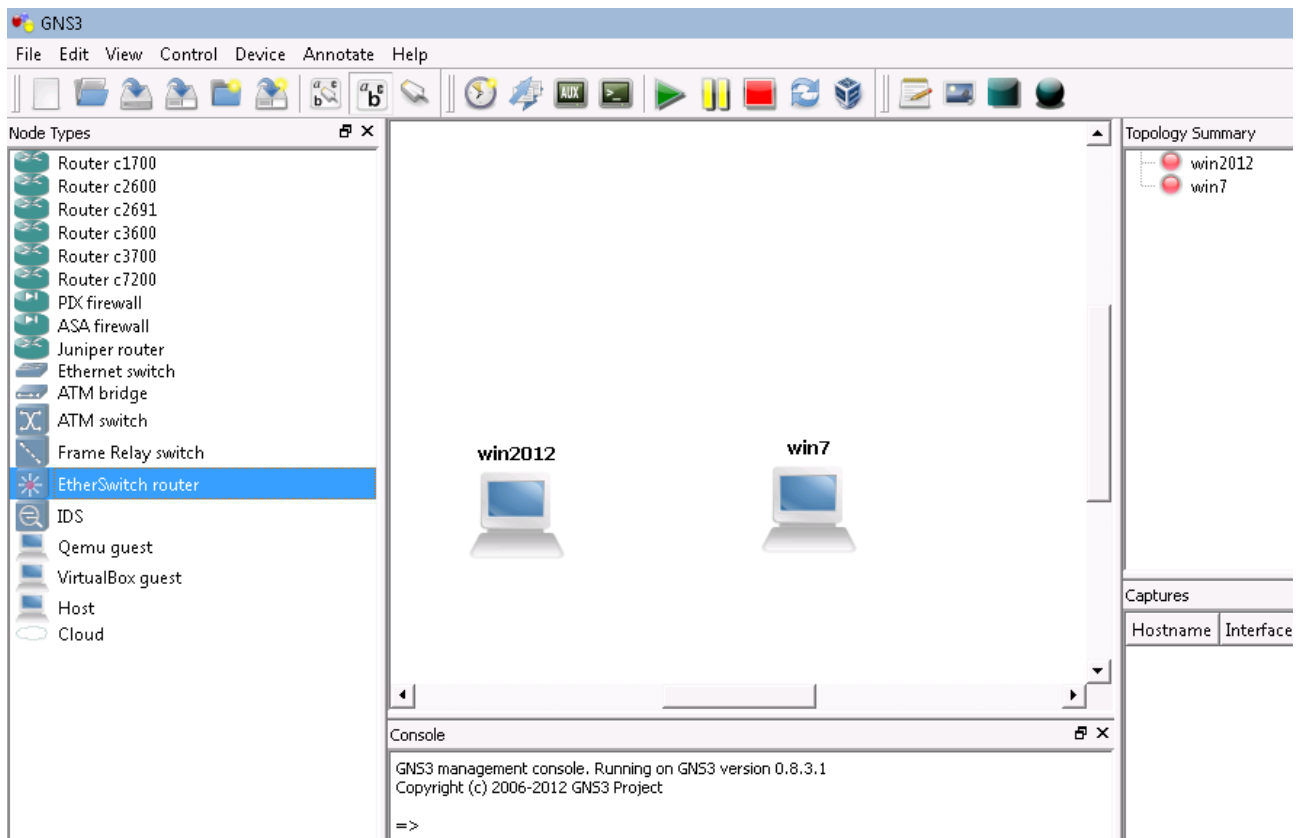
13. Select the “VirtualBox guest” icon on the left, and drag and drop it to the large empty area on the middle.



14. A window appears to select which virtual machine you want to add. First I add the windows 2012 server:

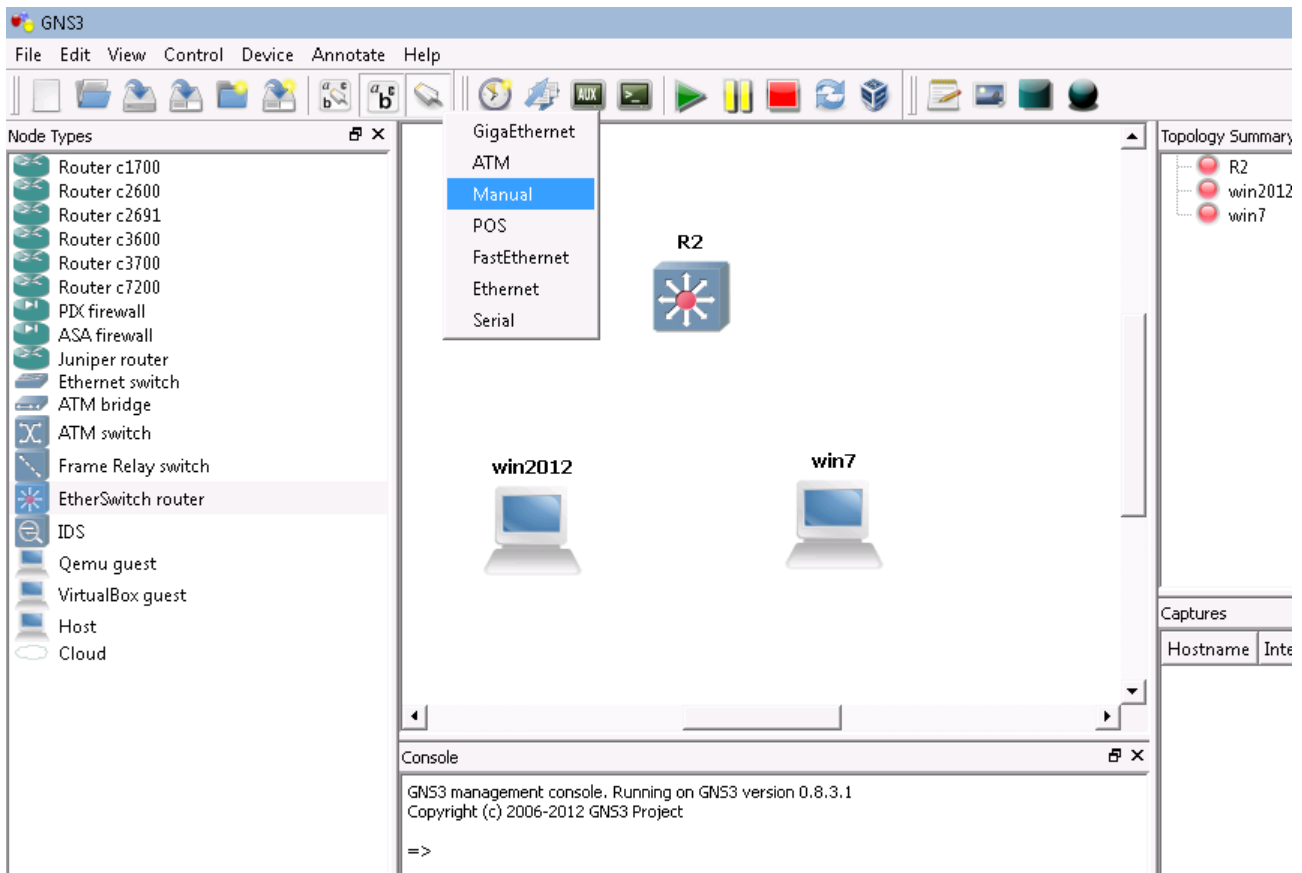


15. Similarly drag and drop a second “VirtualBox guest” to the middle area. Now the previous selection window may not appear, because there is only one other “VirtualBox guest” remained.

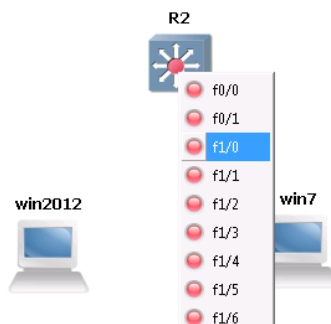


Connect the virtual machines to the virtual etherswitch router

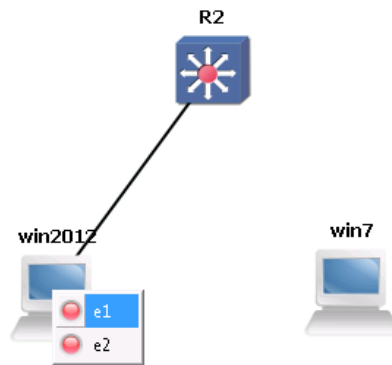
16 The drag and drop an “EtherSwitch router” to the middle area. Now we must connect the “VirtualBox” guests to the switch. Select the connect icon, and from the popup menu the “Manual” connection (if you select a simple Gigabit or Fastethernet you can not choose the exact port):



17 We connect the first NIC of the win2012 VirtualBox guest to the FastEthernet 1/0 port of the “EtherSwitch router” and the first NIC of the win7 VirtualBox guest to the FastEthernet 1/1 port of the “EtherSwitch router”. To do these connections right click to the “EtherSwitch router”, and select the “FastEthernet 1/0” (f1/0) port:

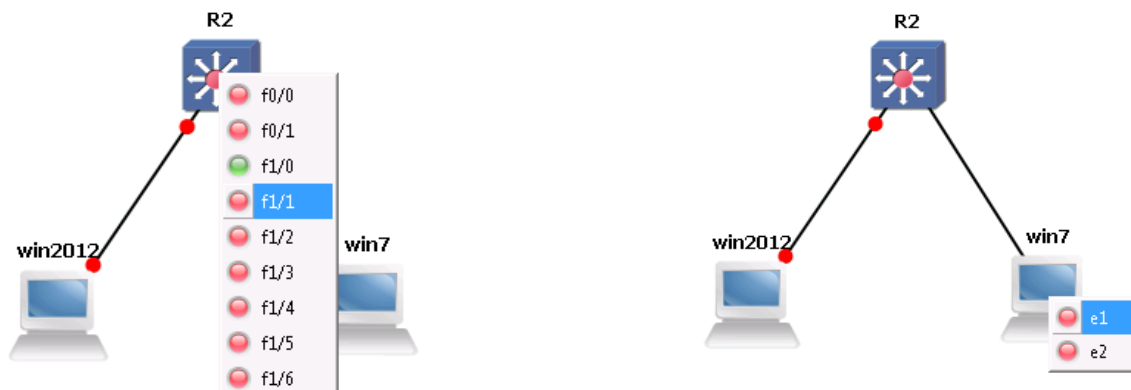


18 Right click to the win2012 VirtualBox guest, and from the popup menu select the “e1” interface

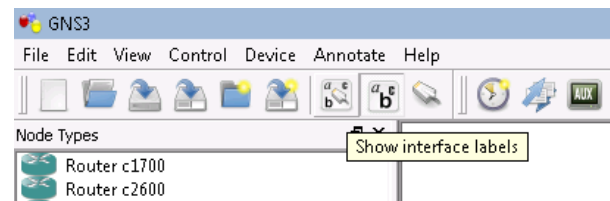
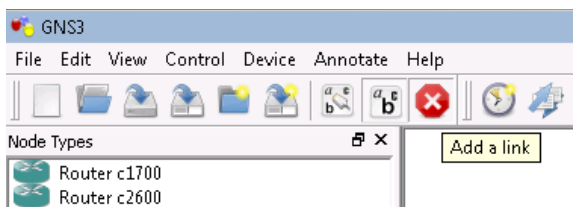


19 to create the other connection
right click again to the

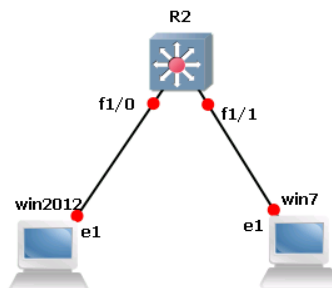
“EtherSwitch router” and select the “FastEthernet 1/1” (f1/1) interface. Then right click to the win7
“VirtualBox guest”, and select the e1 interface of it:



20 to finish the connection click again the add link button on the task bar.

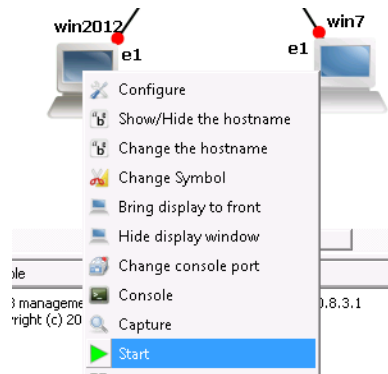


21 here is the final network draw with the interfaces:



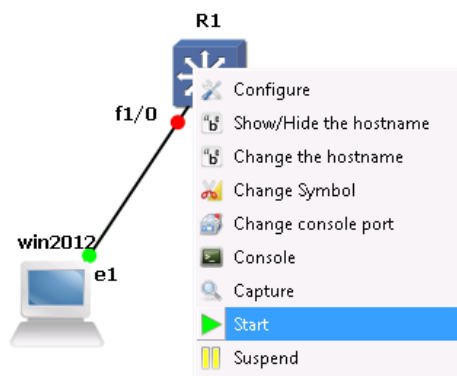
Start the virtual devices

22 Start the windows 2012 server by right click on it and select the start command from the popup menu:

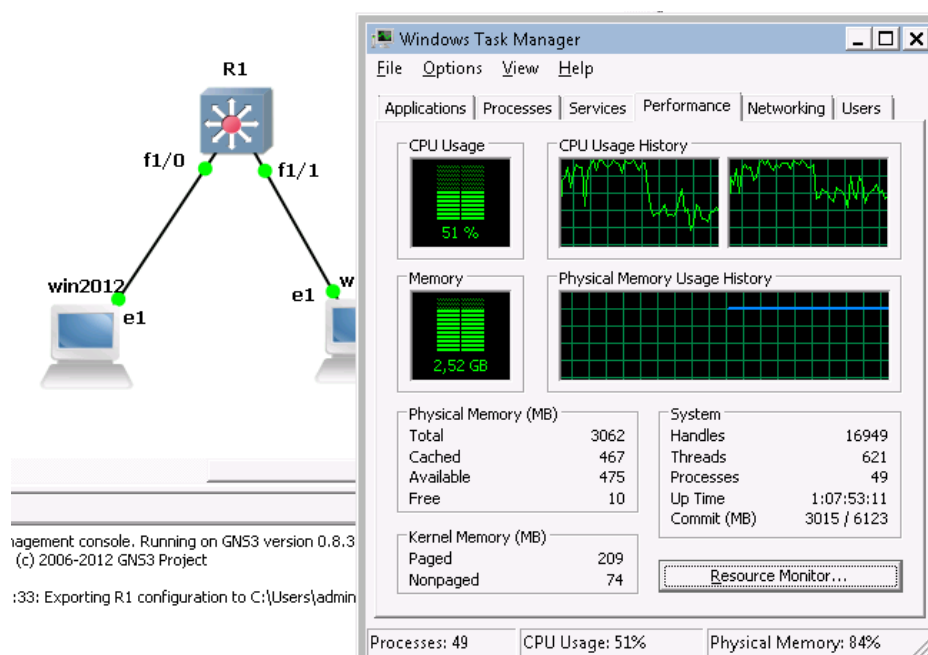


23. when it booted up similarly start the win7 machine.

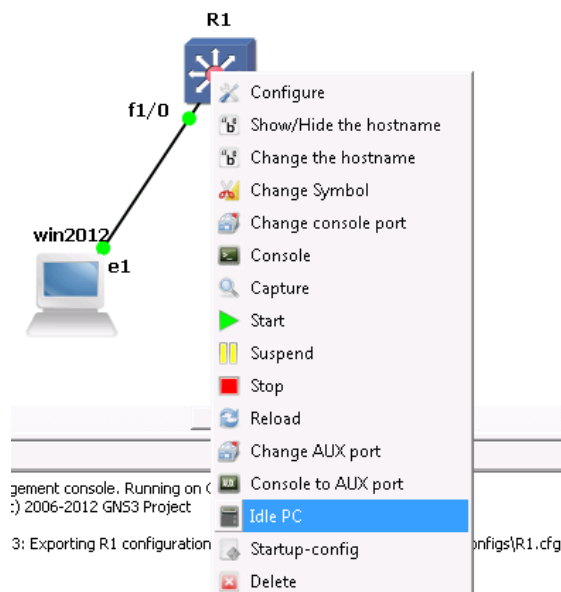
24. Then finally start the “EtherSwitch router”



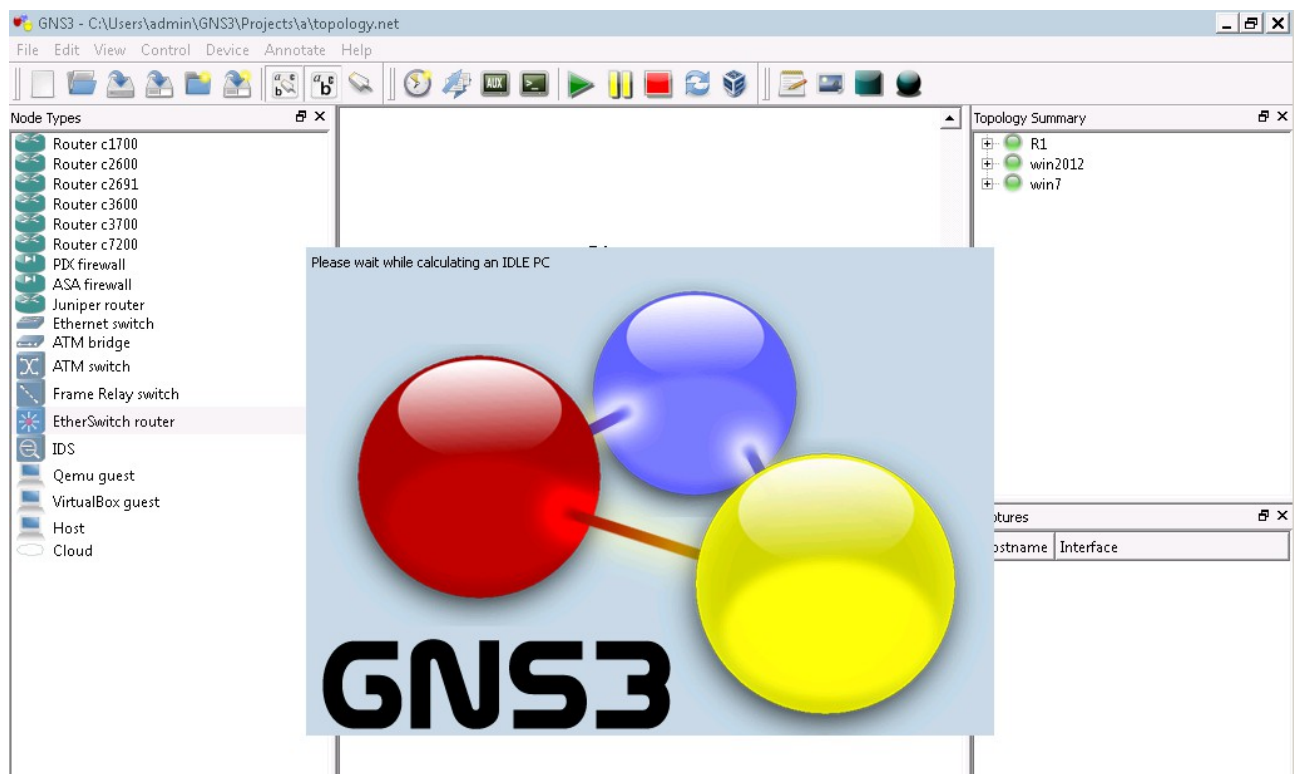
25 After starting the “EtherSwitch router” you will recognize it will up all the CPU resources of the computer. To help on it we should use the “IDLE PC”.



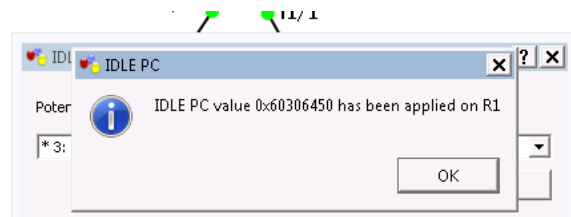
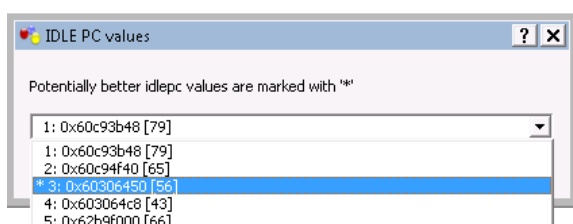
26 Right click to the “EtherSwitch router”, and from the popup menu select the “Idle PC” command



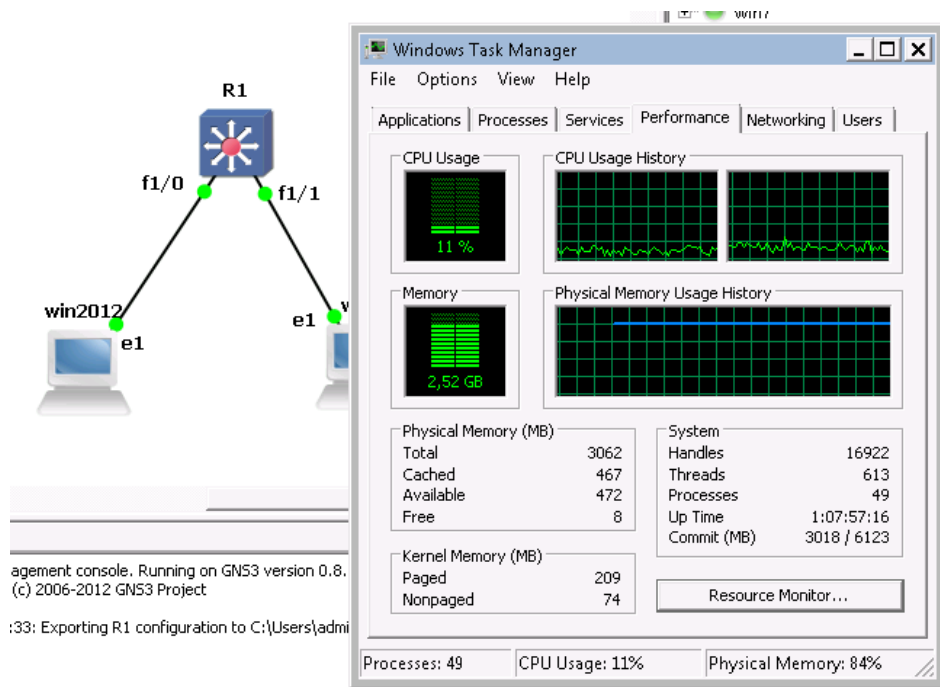
27 then it calculates for a while



28 Select a value with star in front of it, then click to the OK button. If an information widow appears click to the OK button on that as well:



29 The CPU stress of your computer should significantly decrease. If not repeat the process.



30 Test the connection between the win7 client and the win 2012 server by ping

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\administrator>ping 192.168.168.110

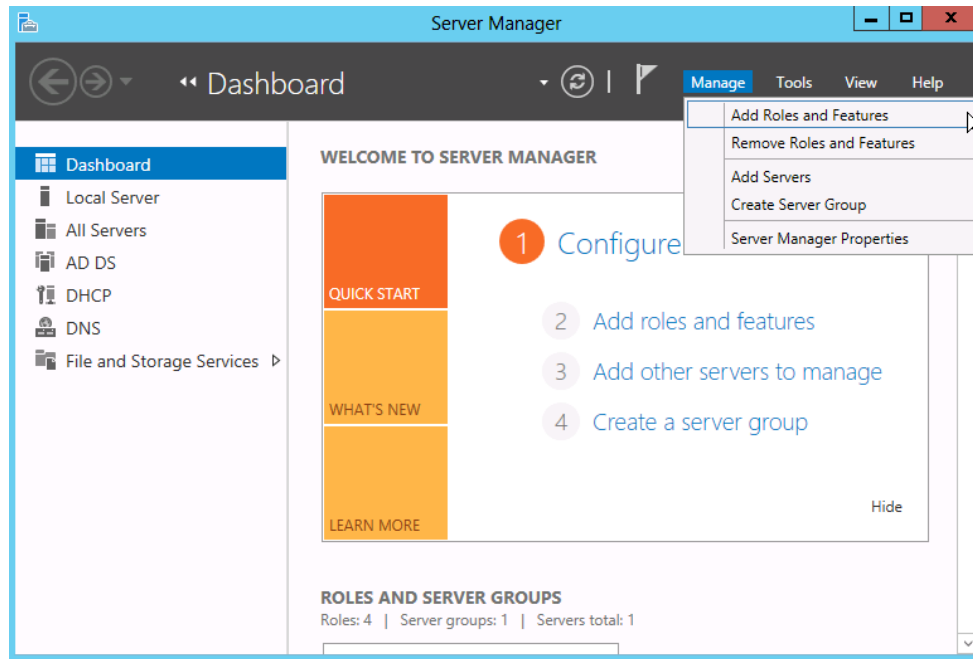
Pinging 192.168.168.110 with 32 bytes of data:
Reply from 192.168.168.110: bytes=32 time=1ms TTL=128
Reply from 192.168.168.110: bytes=32 time=5ms TTL=128
Reply from 192.168.168.110: bytes=32 time=7ms TTL=128
Reply from 192.168.168.110: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.168.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 3ms

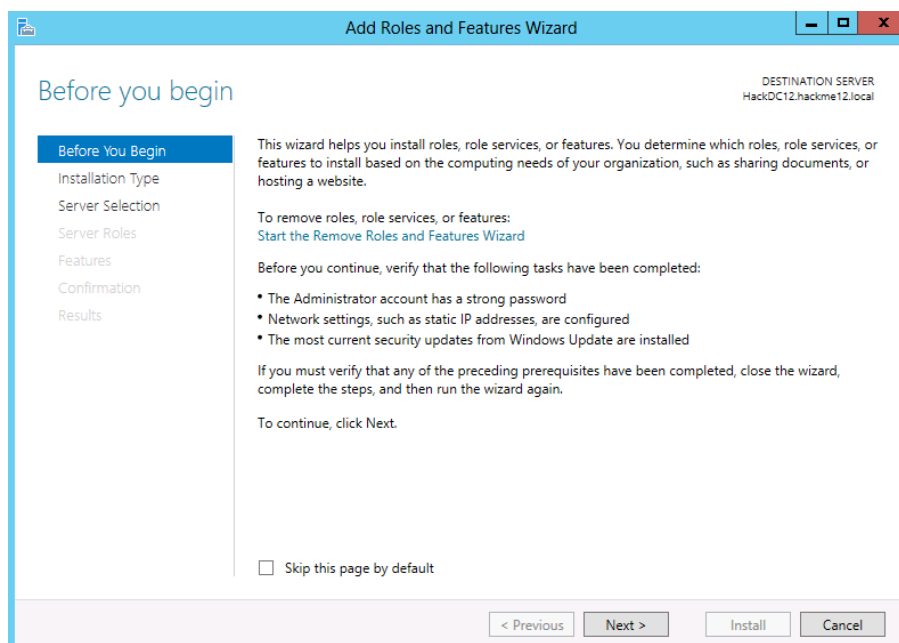
C:\Users\administrator>
```

Install the Network Policy Server (RADIUS) to windows 2012

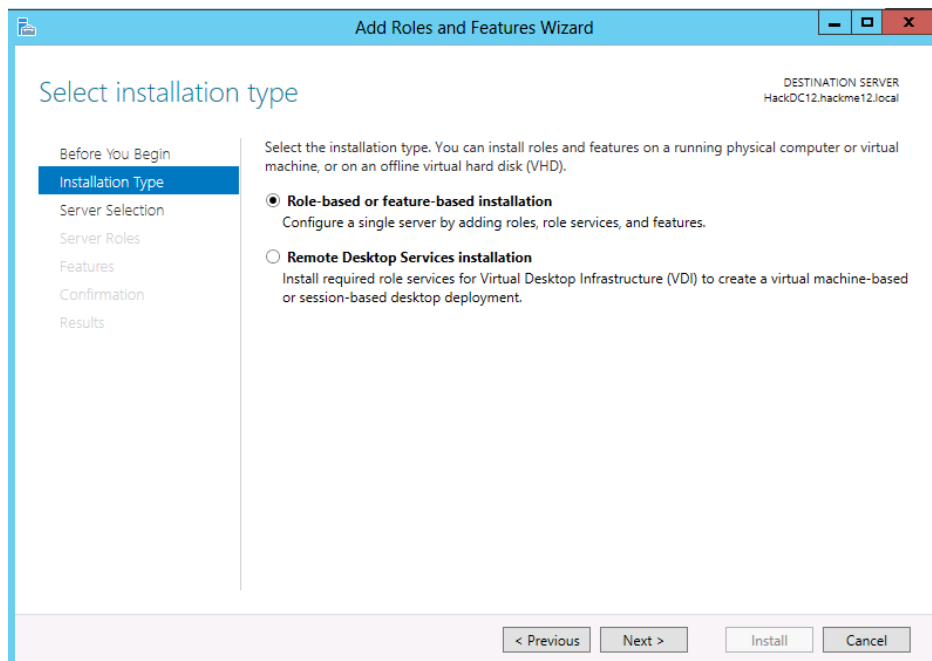
31 Start the server manager, if it does not start automatically, then select Manage / “Add Roles and Features”



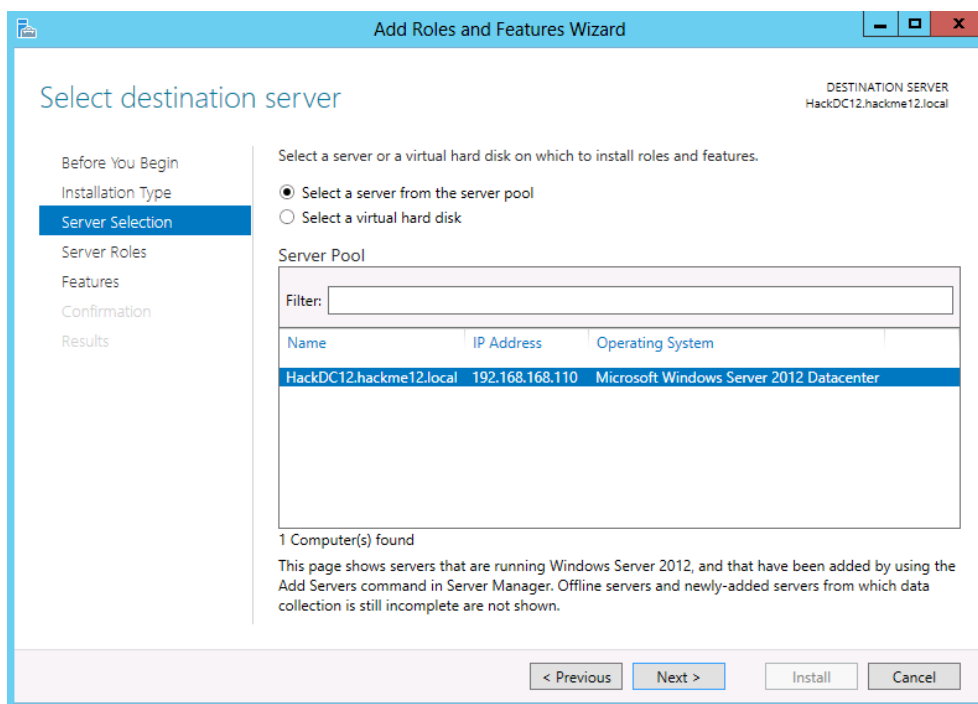
32 Click next on the welcome screen of the wizard:



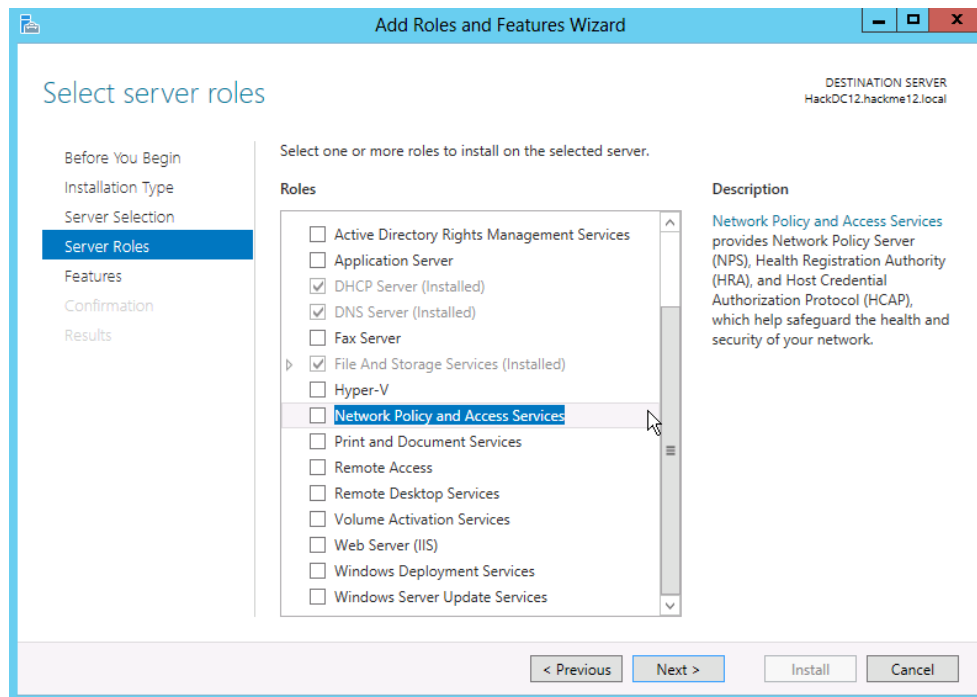
33 Select the Role-based or feature-based installation



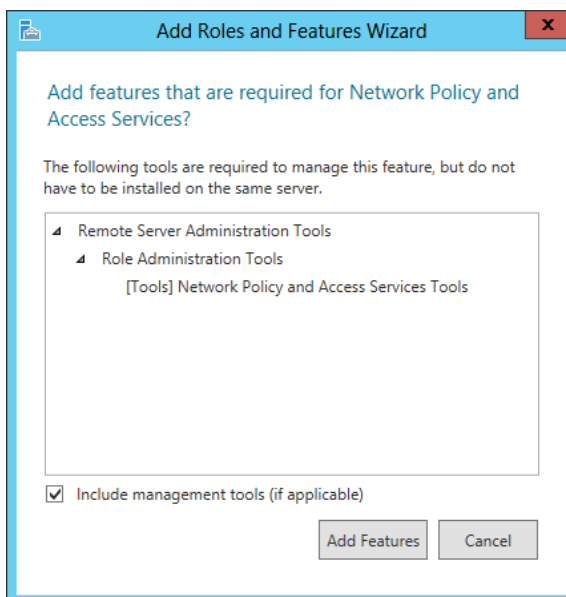
34 Select the local server



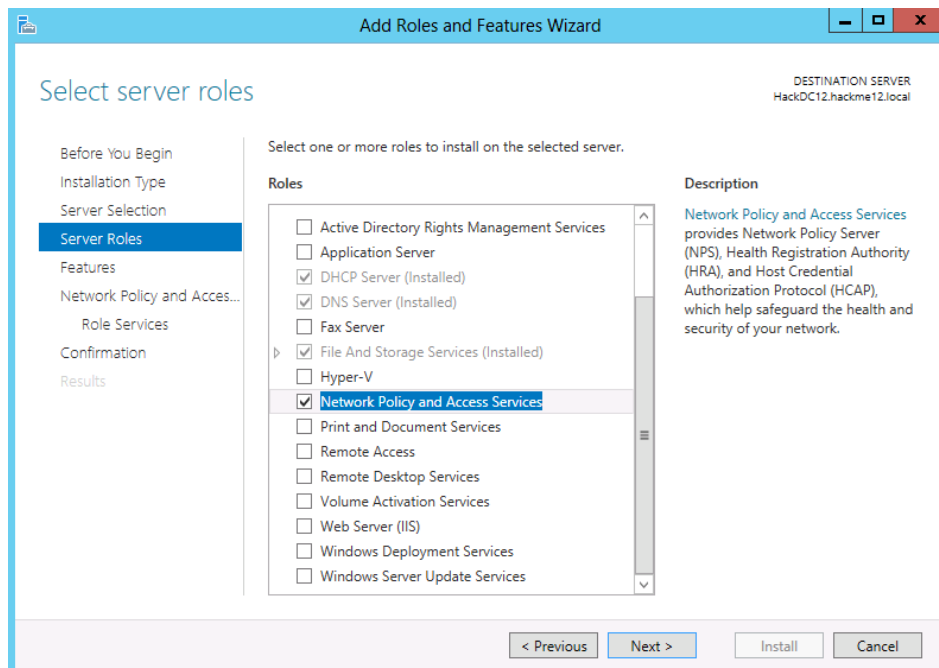
35 Select the “Network Policy and Access Services” to install.



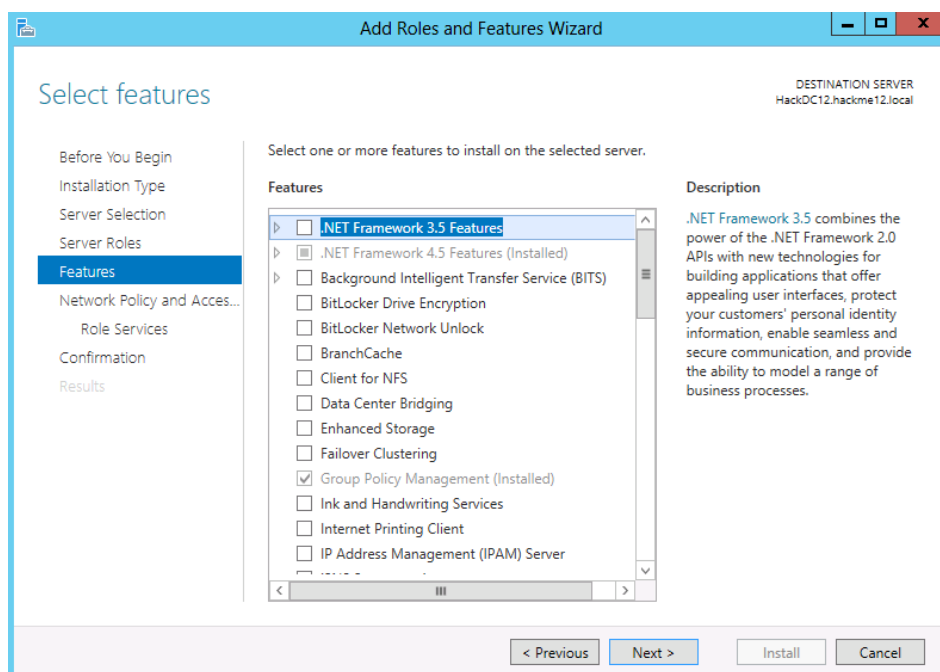
36 the computer informs you, it will requires some additional features to install. Click to the “Add Features” button, to accept the dependents.



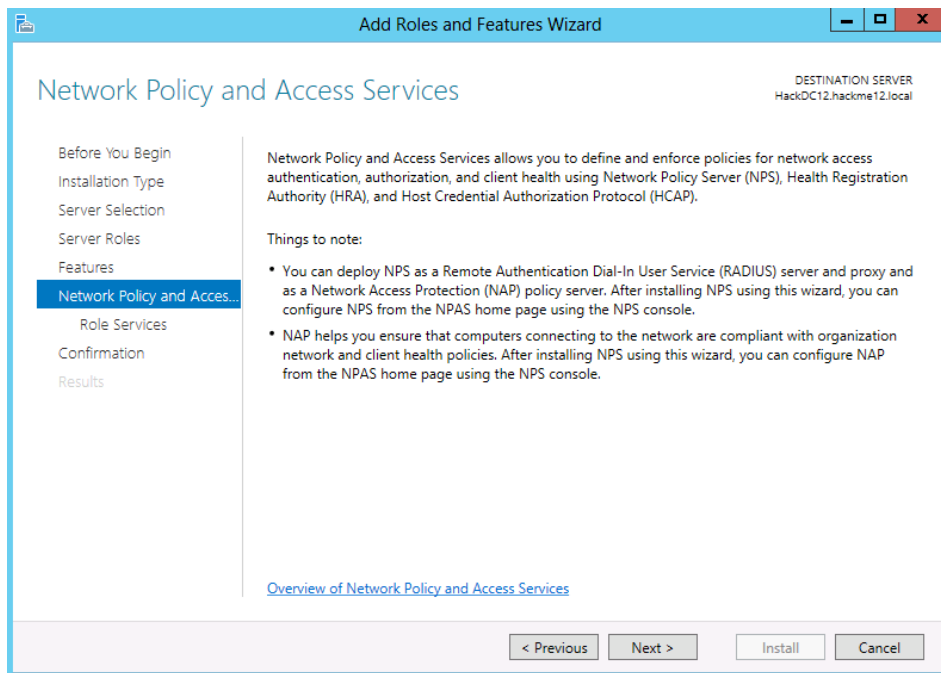
37 click to next to continue the wizard



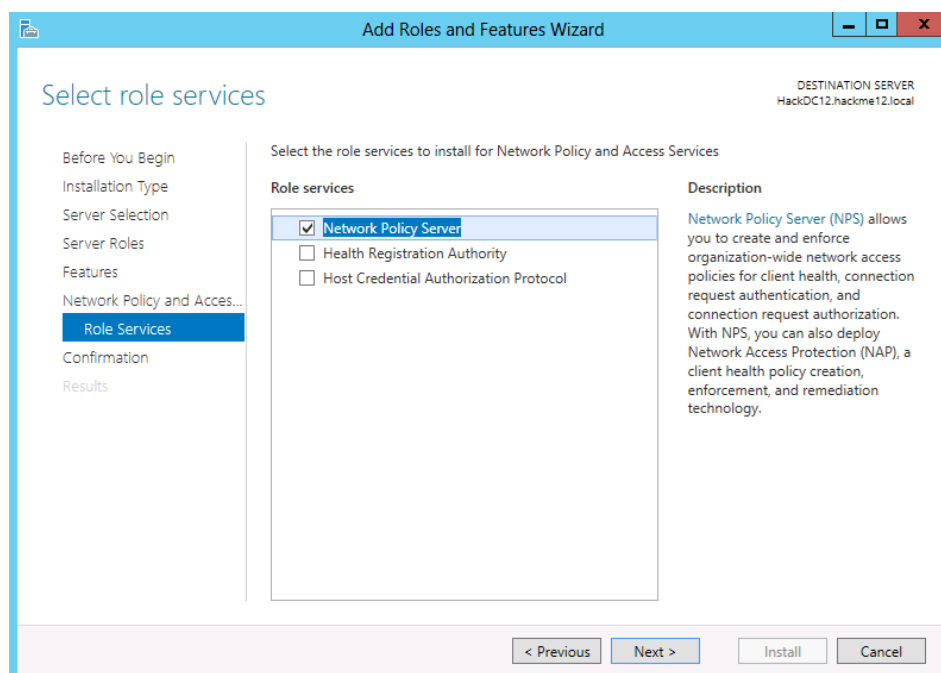
38 The required features are already selected, so click next on the “Select Feature” page



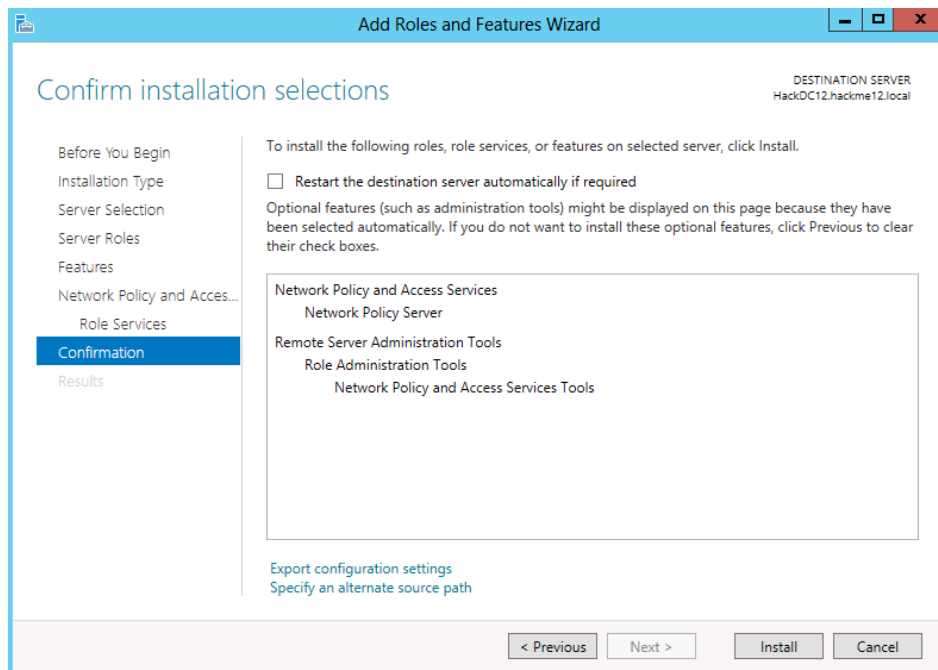
39 Click next on the “Network Policy and Access Services” screen



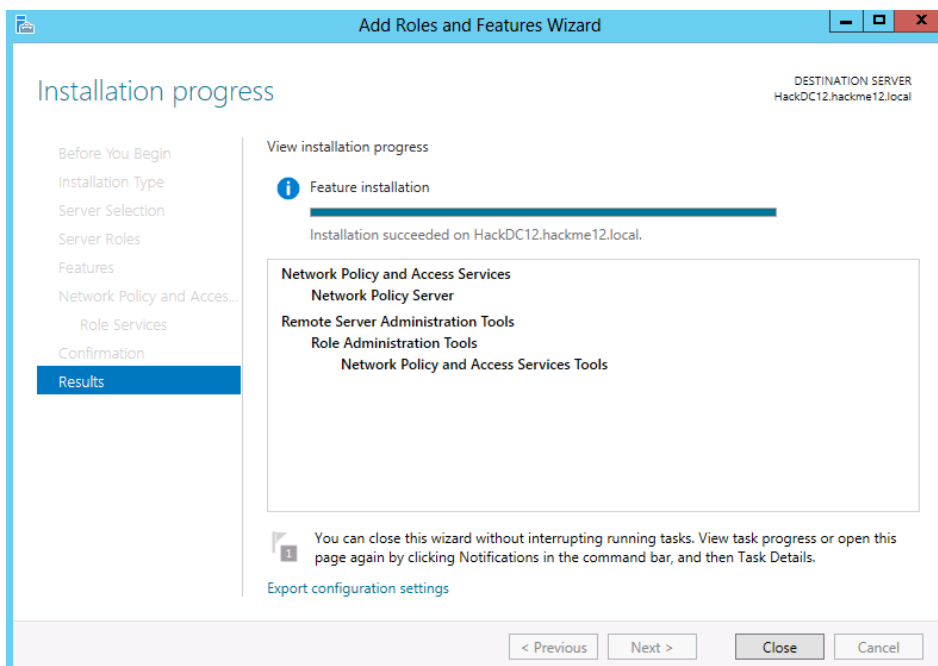
40 Select the “Network Policy Server” role service to install. We do not need the “Health Registration Authority” and the “Host Credential Authorization Protocol” yet, we will install them later, when we configure the health policy with 802.1x.



41 On the confirmation window click to the “Install” button.

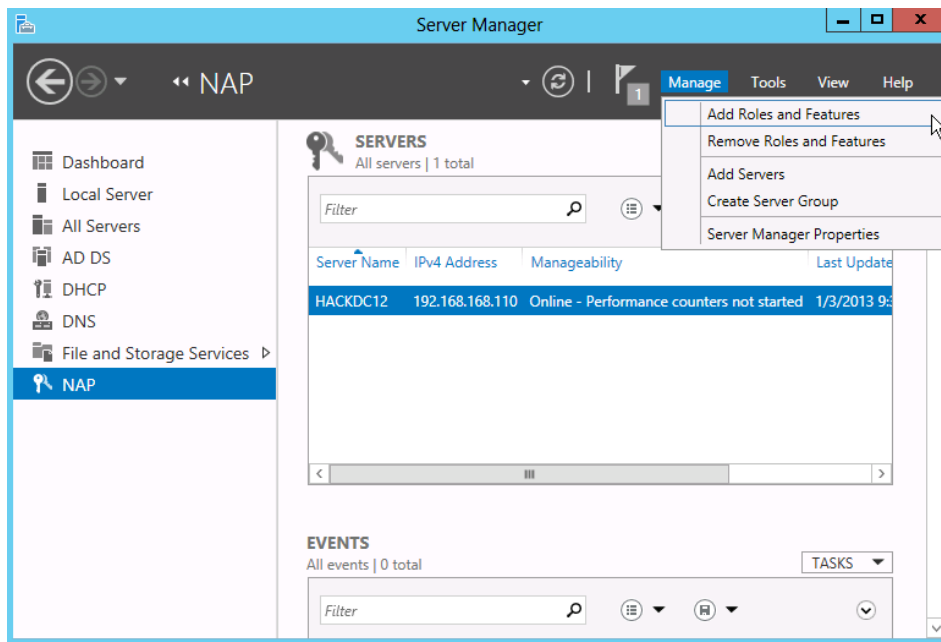


42 then wait until the installation finish

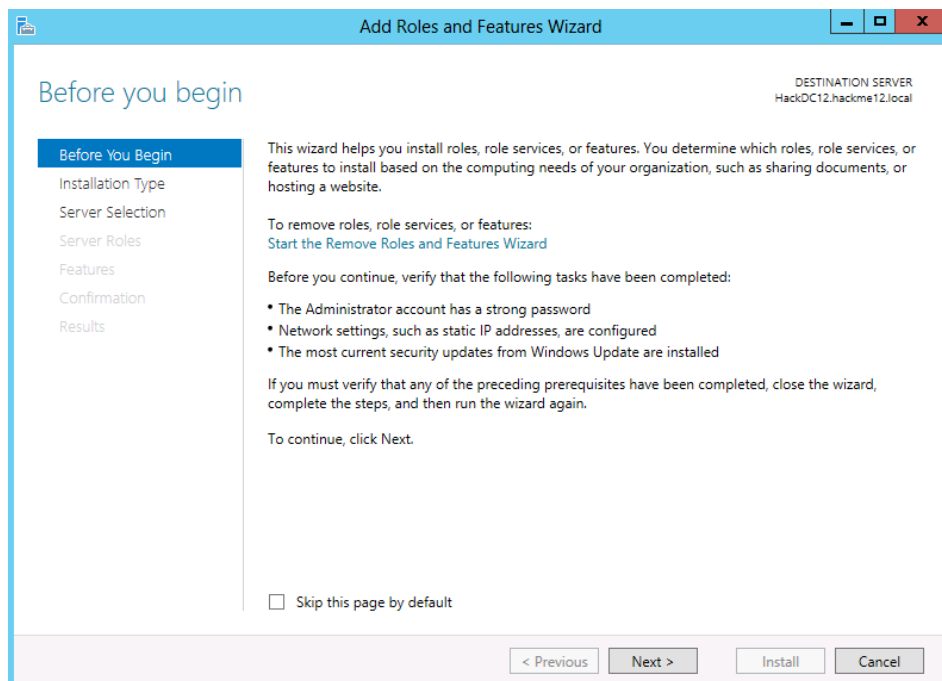


Install the Certificate Server to Windows 2012

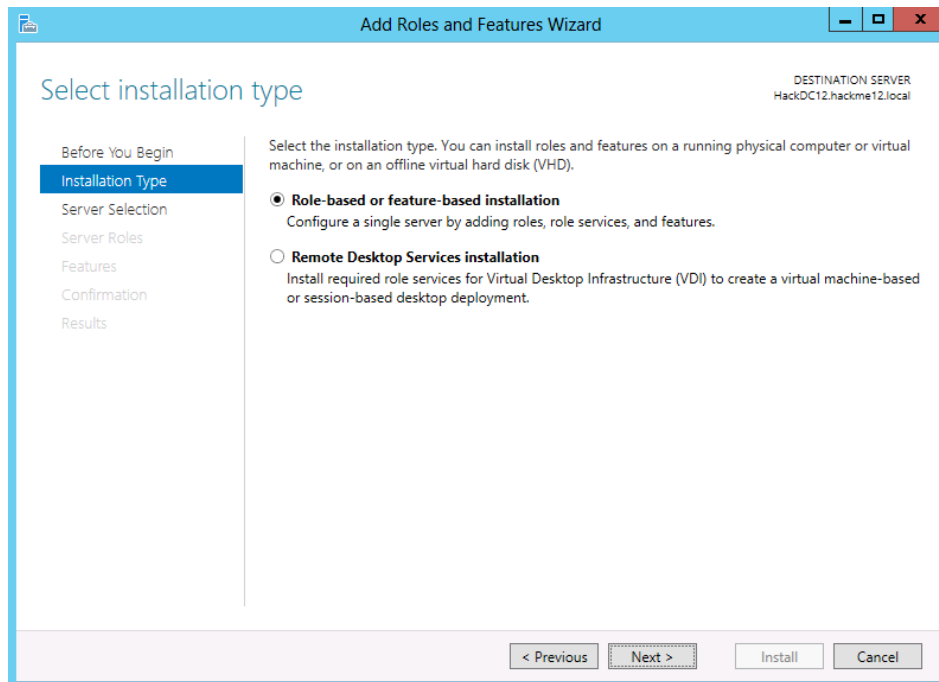
43 select Manage / “Add Roles and Features” in the server manager.



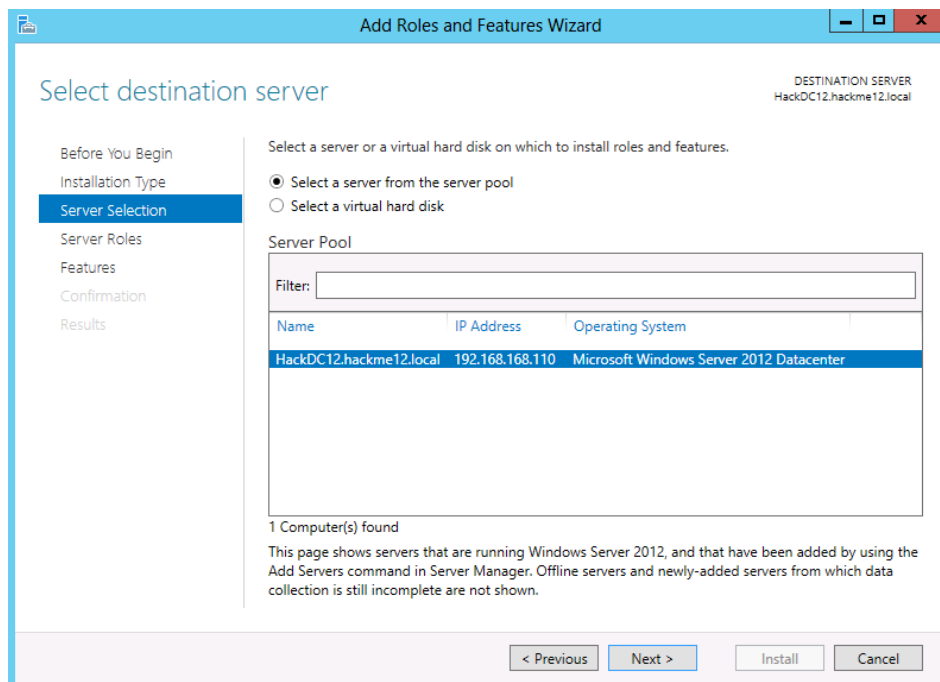
44 Click next on the welcome screen



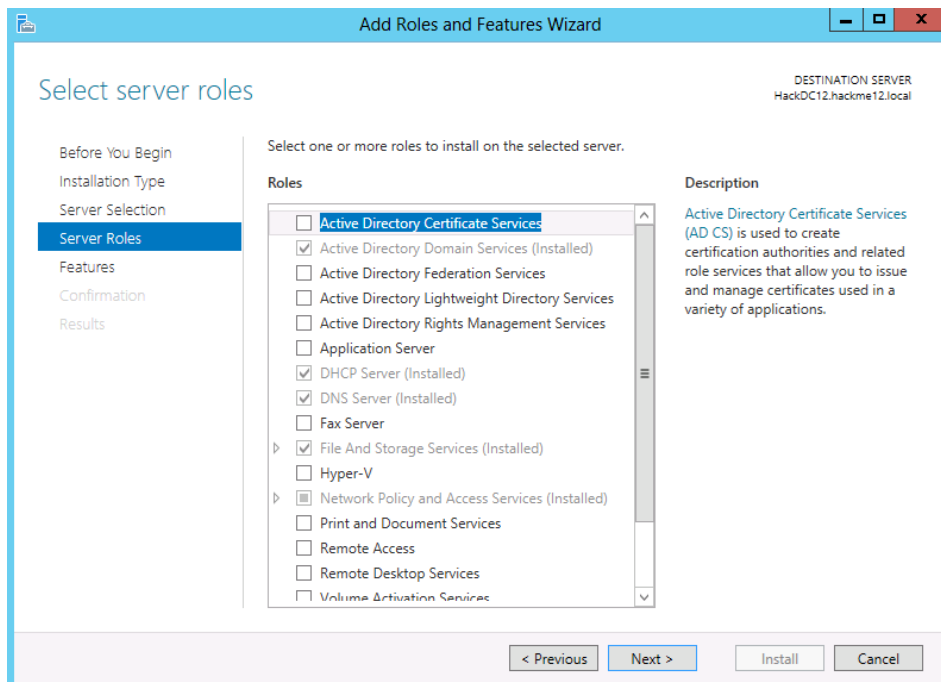
45 Select “Role-based or feature-based installation”, and click to next



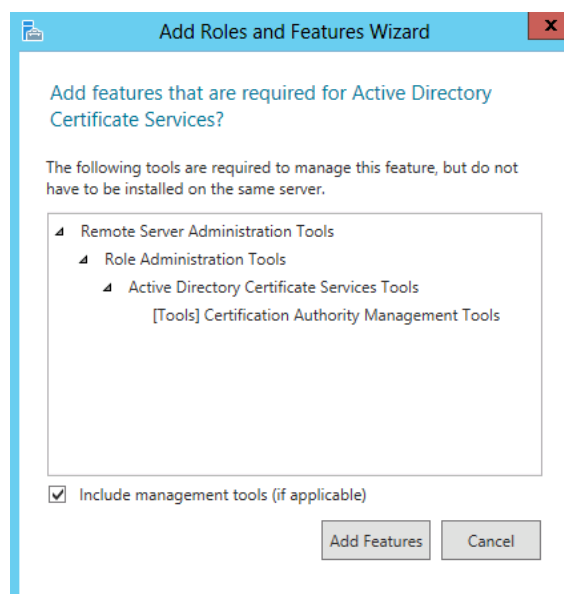
46 Select the local server as destination



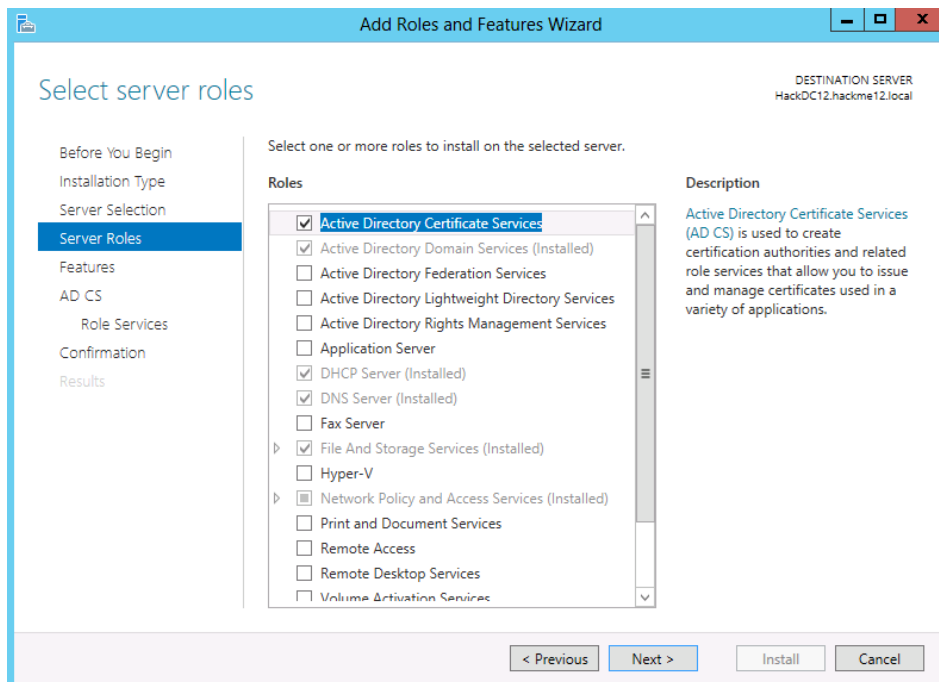
47 Select the “Active Directory Certificate Service” as server role.



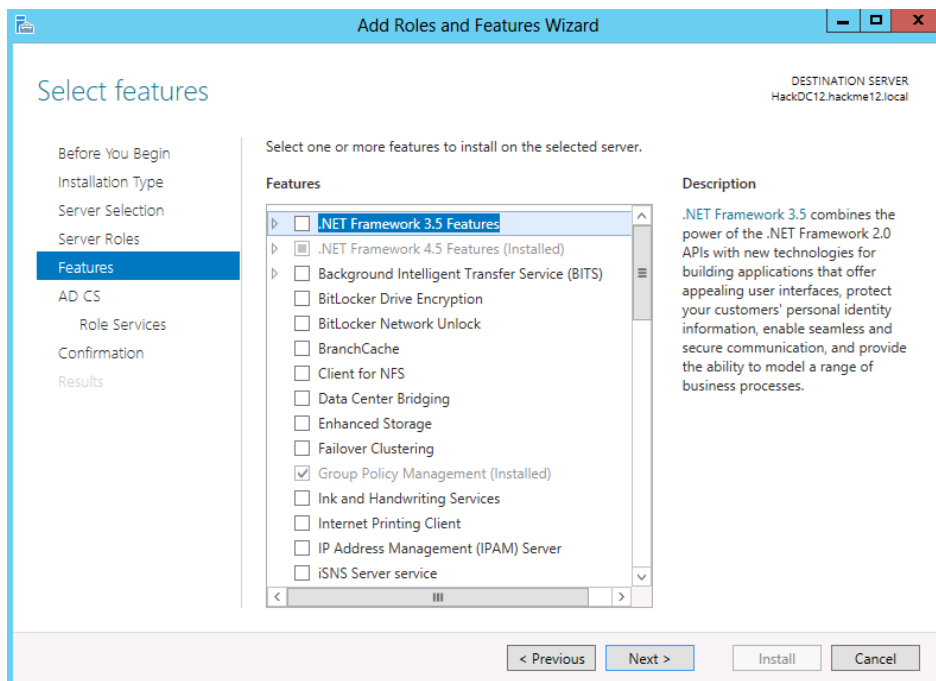
48 Again the computer informs you, it will requires some additional features to install. Click to the “Add Features” button, to accept the dependents.



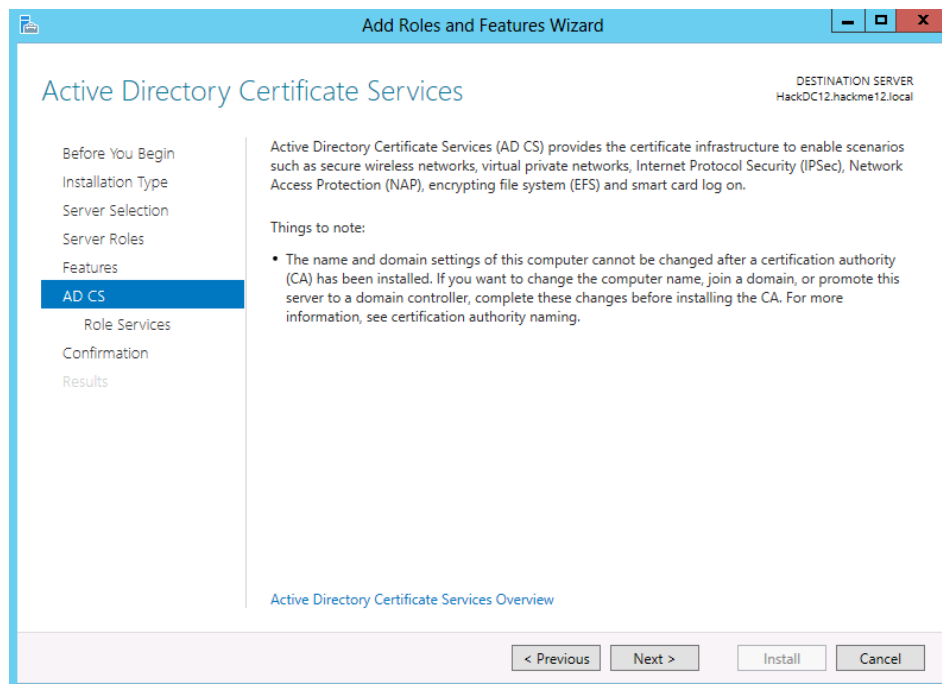
49 Click next on the “server roles” window



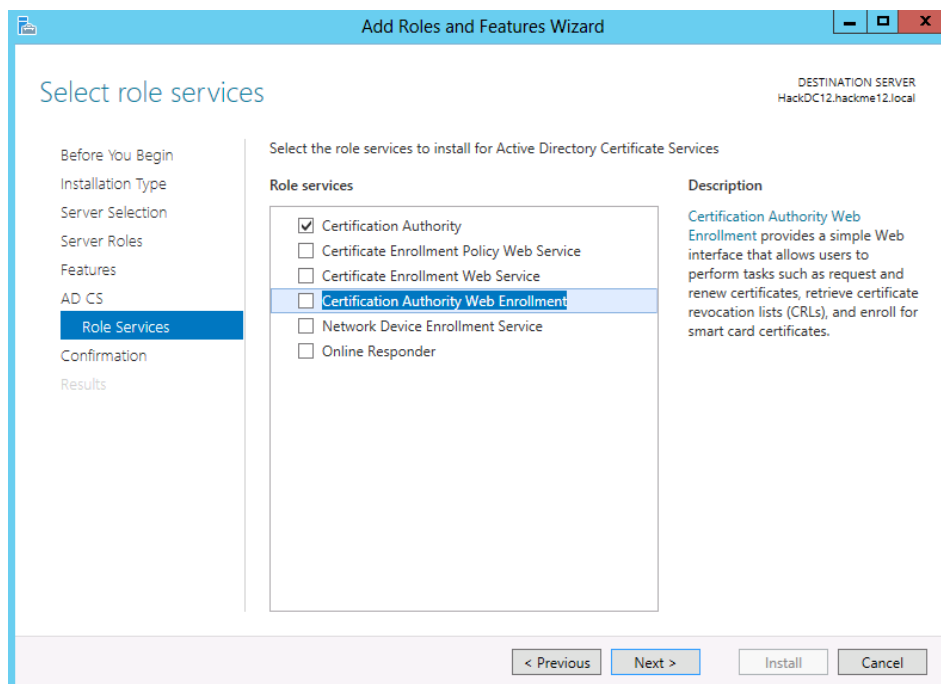
50 Click next on the “Select Feature” page



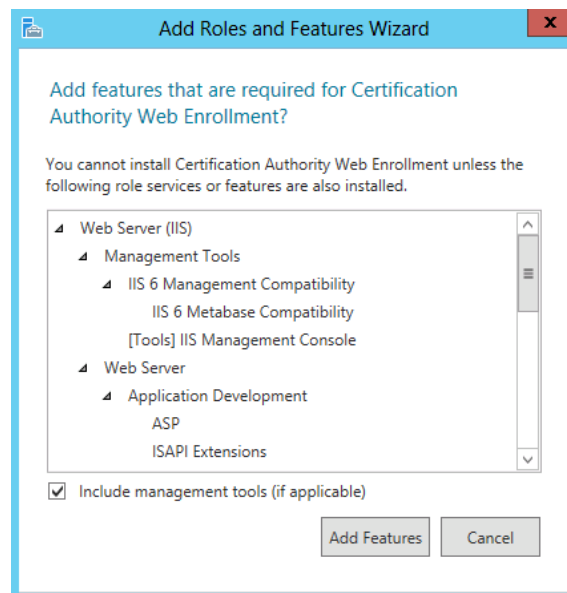
51 click next on the certificate server installation window



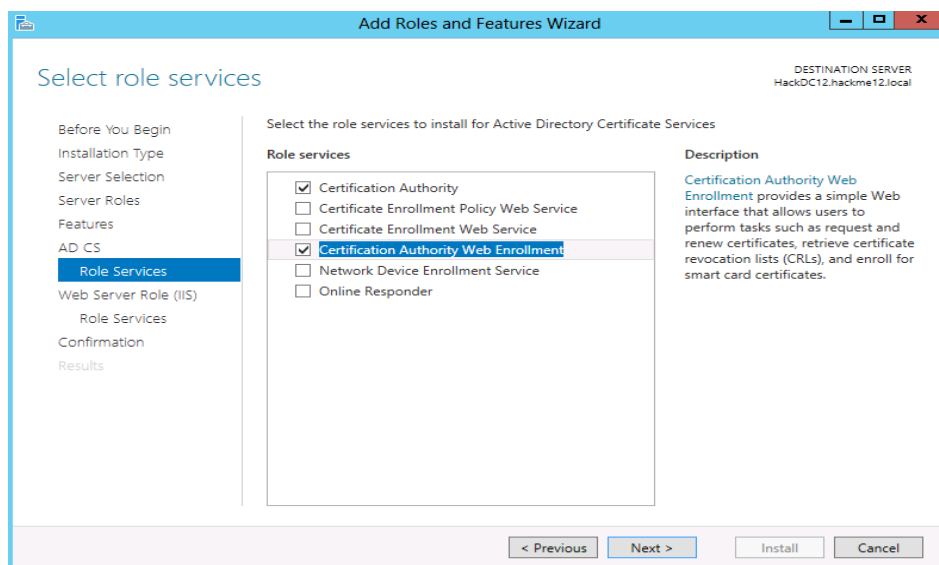
52 install the “Certification Authority Web Enrollment” role service as well.



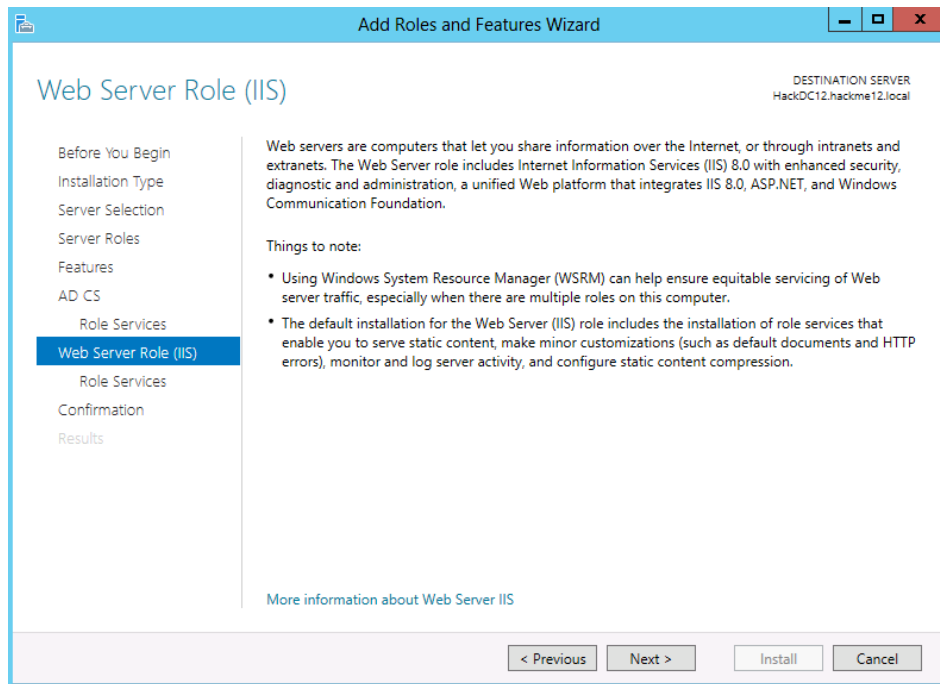
53 Again the computer informs you, it will requires some additional features to install. Click to the “Add Features” button, to accept the dependents.



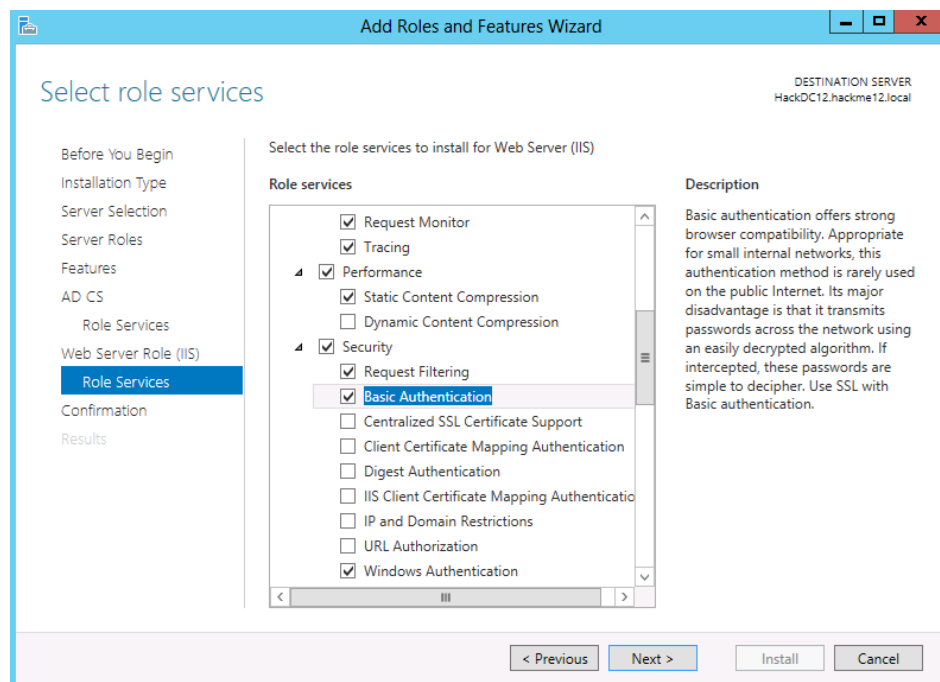
54 click next on the “select role services” window



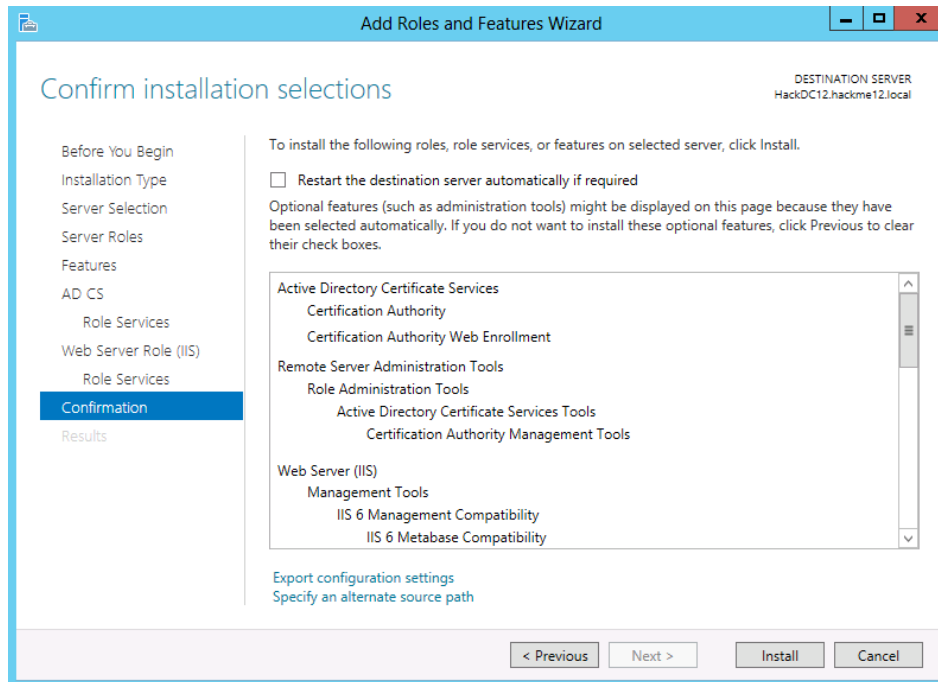
55 click next on the “Web server role (IIS)”



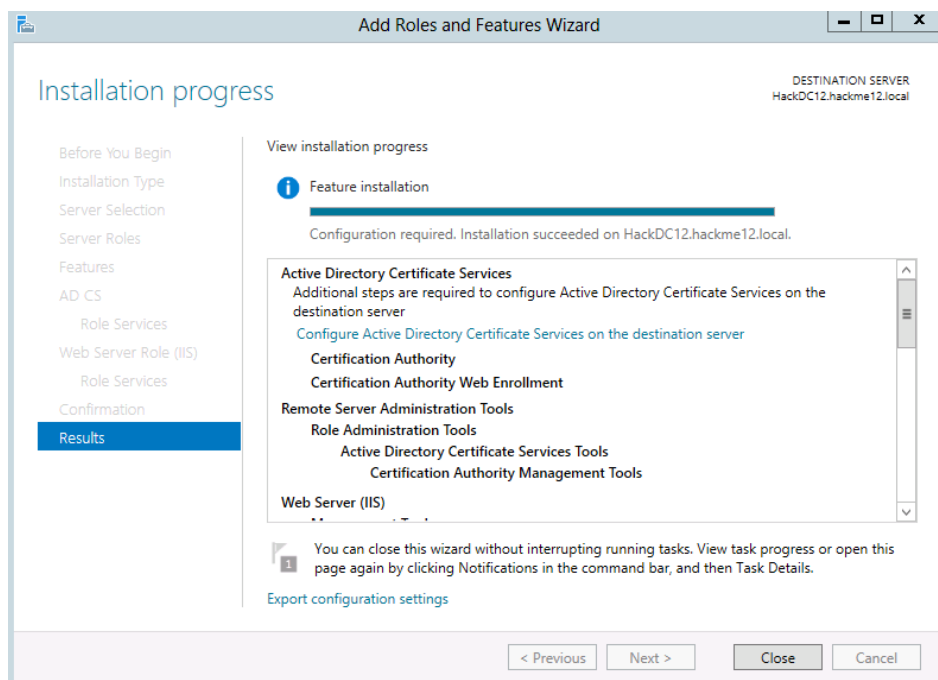
56 I used to add “Basic Authentication” as well, but it is not mandatory, just works good as a backup authentication method.



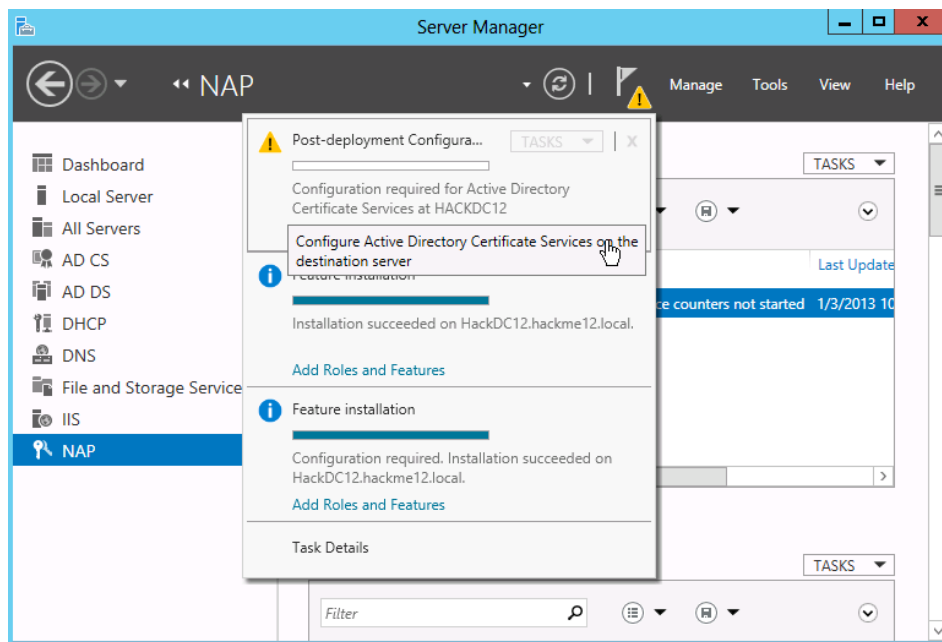
57 click install on the confirmation window



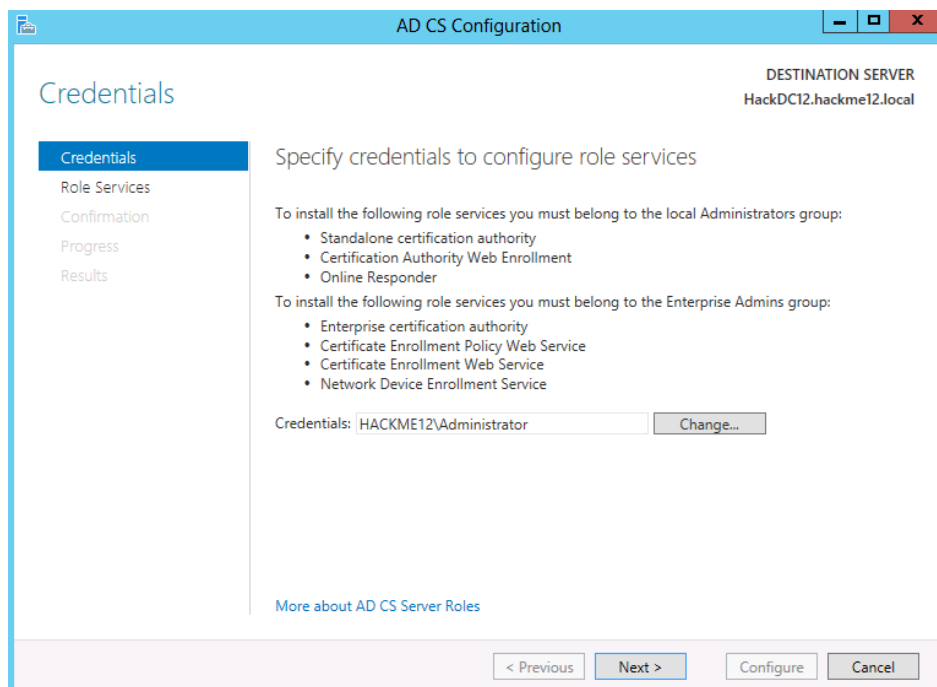
58 wait until the installation completes.



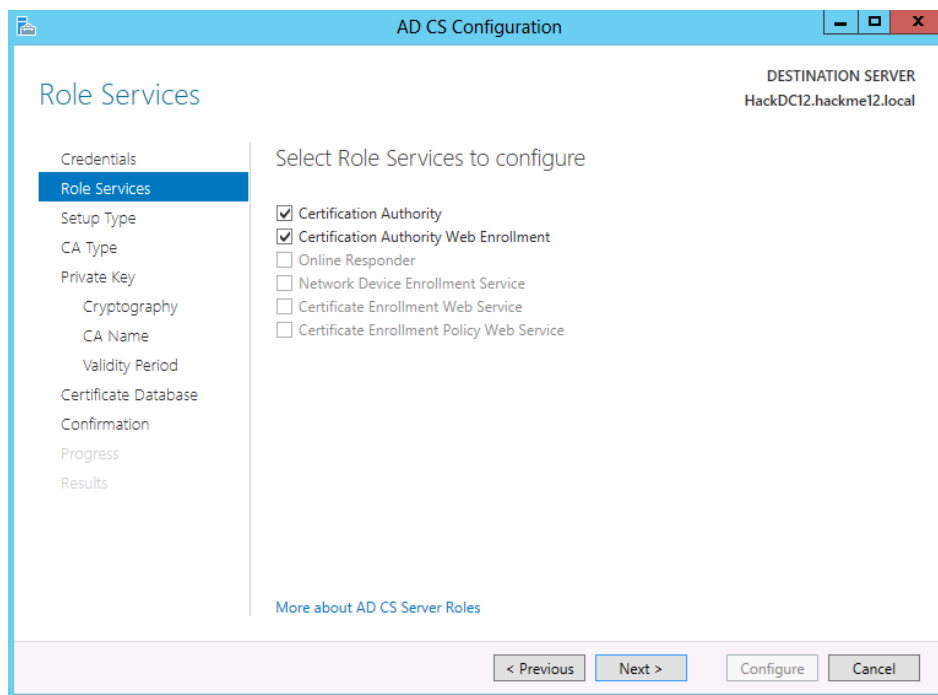
59 There are some additional task we should do, so click to the post-deployment configuration.



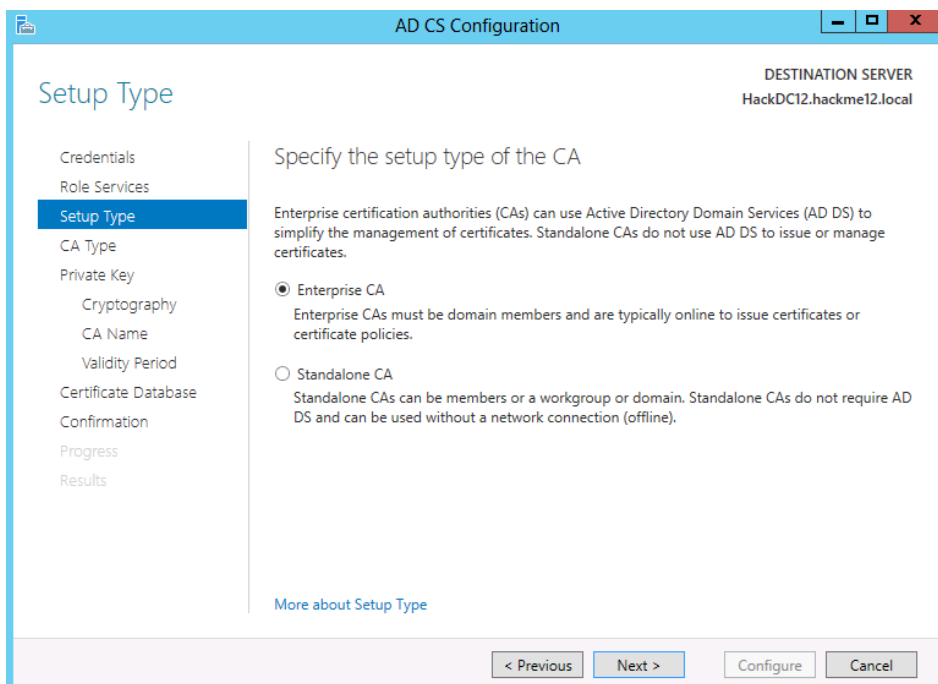
60 use a domain administrator user to configure, then click to the next button



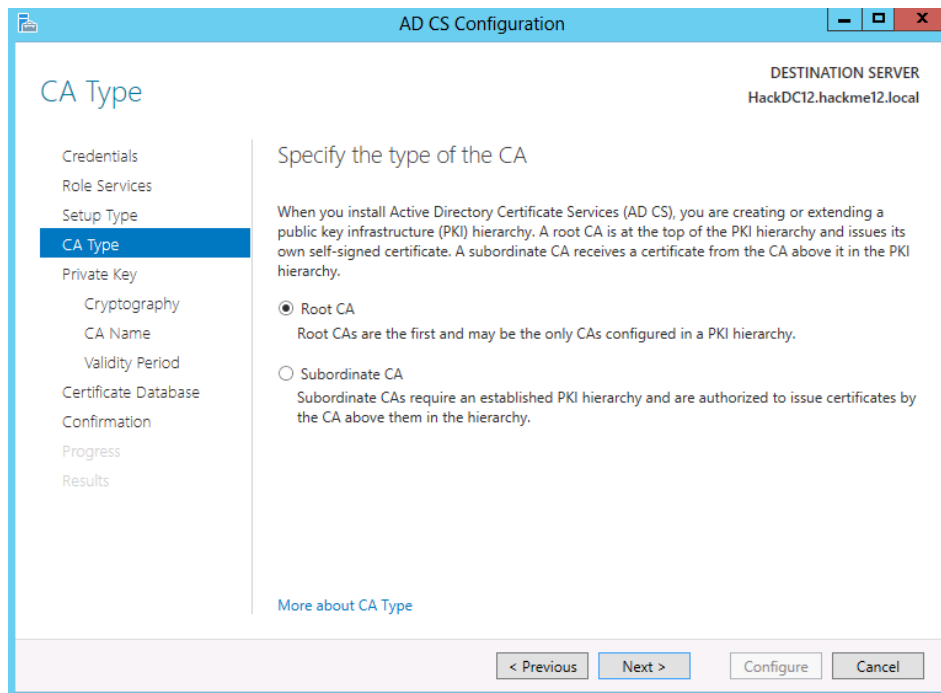
61 select the two role services, to do the post configuration:



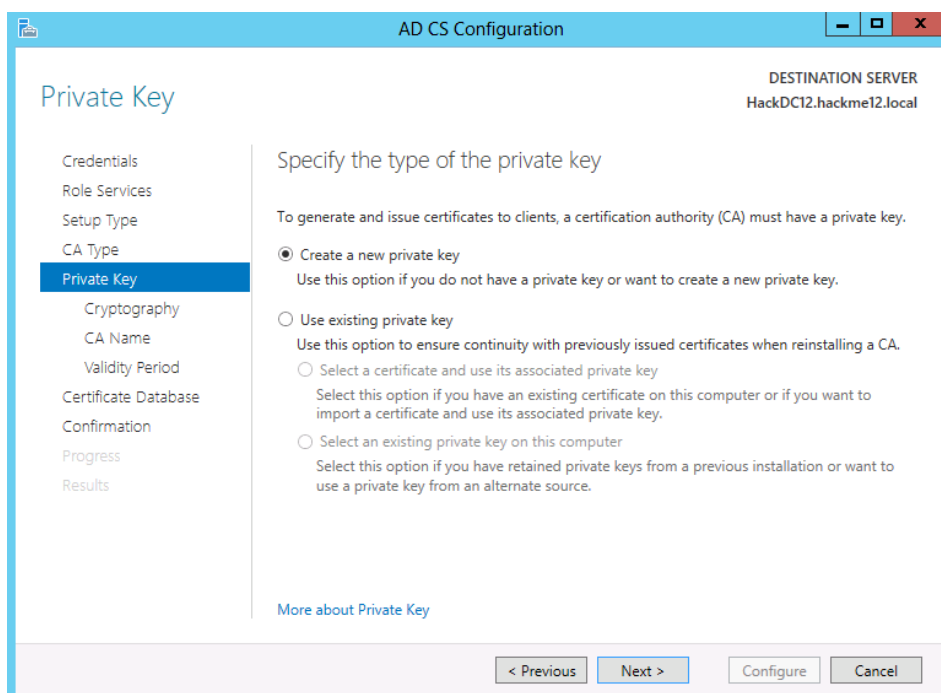
62 Select the CA type (the enterprise here has not any connection with the windows enterprise or standard connection, it means the CA is AD integrated, so the domain computers can find it automatically). Generally at least two level hierarchy recommended (a Standalone root CA, and an Enterprise issue CA). Now in the test environment we will install only an enterprise root CA, because it requires less resource.



63 Select "Root CA" as CA type



64 Select the “Create a new private key”, because we want to create a new certificate server.



65 Set the key length and authentication algorithm. I used the largest available ones. If you want to install certificate network devices as well check what is supported by the IOS. Now we do not install certificate to the switch, the authentication will be done on the RADIUS server.

66 change the CA name, or set some additional parameter if you want, then click to next.

67 set the validity period.

The screenshot shows the 'AD CS Configuration' window with the 'Validity Period' tab selected. The left sidebar lists various configuration steps, with 'Validity Period' highlighted. The main area is titled 'Specify the validity period' and contains a dropdown menu set to '5 Years', a 'CA expiration Date' of '1/3/2018 10:17:00 PM', and a warning message. At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
HackDC12.hackme12.local

Validity Period

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):
5 Years

CA expiration Date: 1/3/2018 10:17:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous Next > Configure Cancel

68 select the place of the CA database and transaction log files:

The screenshot shows the 'AD CS Configuration' window with the 'CA Database' tab selected. The left sidebar lists various configuration steps, with 'CA Database' highlighted. The main area is titled 'Specify the database locations' and contains two text input fields for 'Certificate database location' and 'Certificate database log location', both set to 'C:\Windows\system32\CertLog'. At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
HackDC12.hackme12.local

CA Database

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the database locations

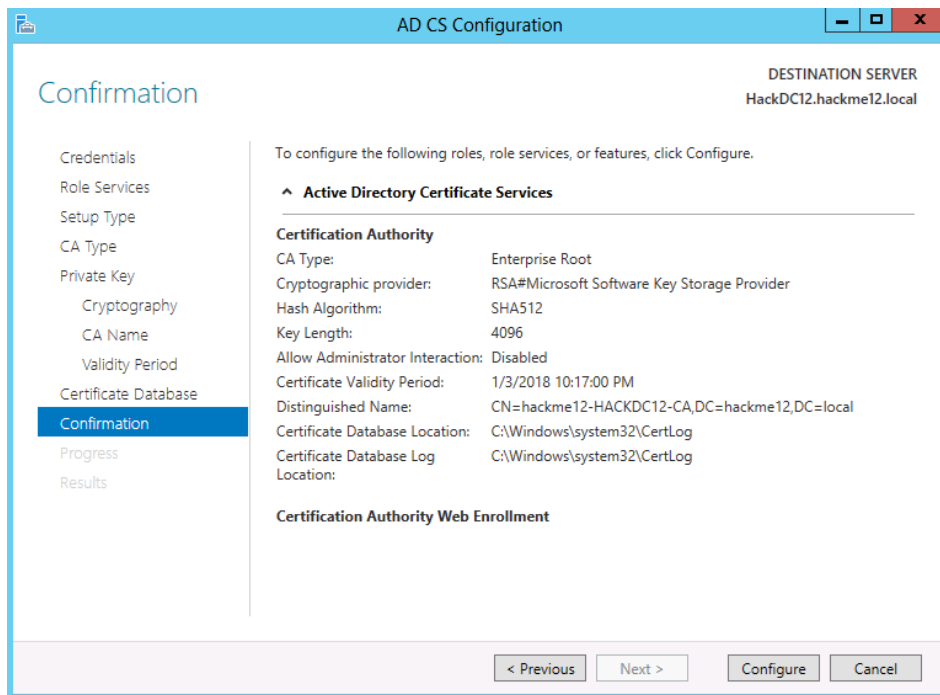
Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

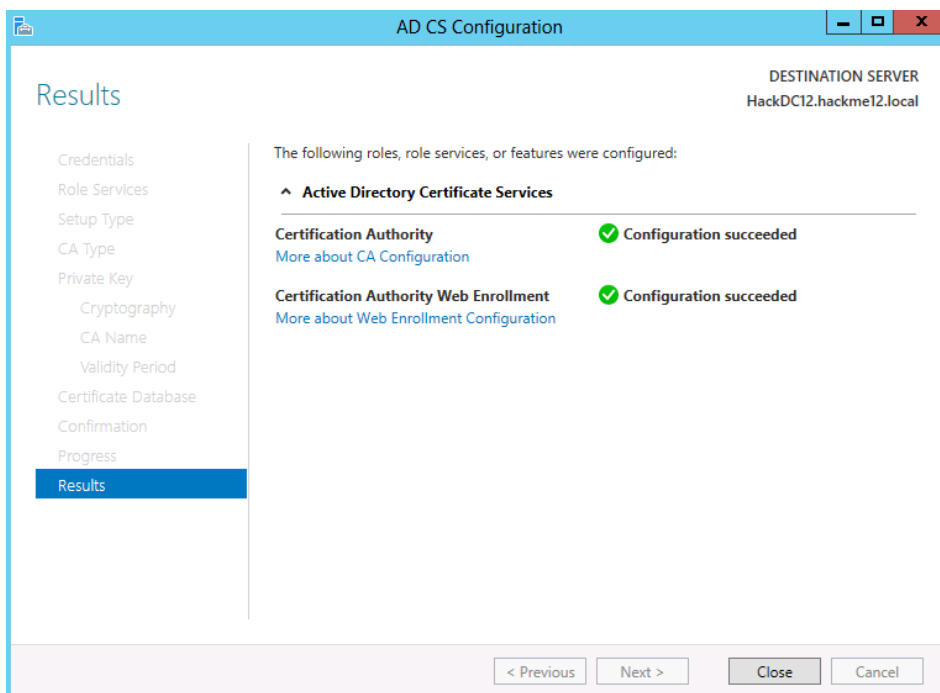
[More about CA Database](#)

< Previous Next > Configure Cancel

69 on the confirmation window click to configure.



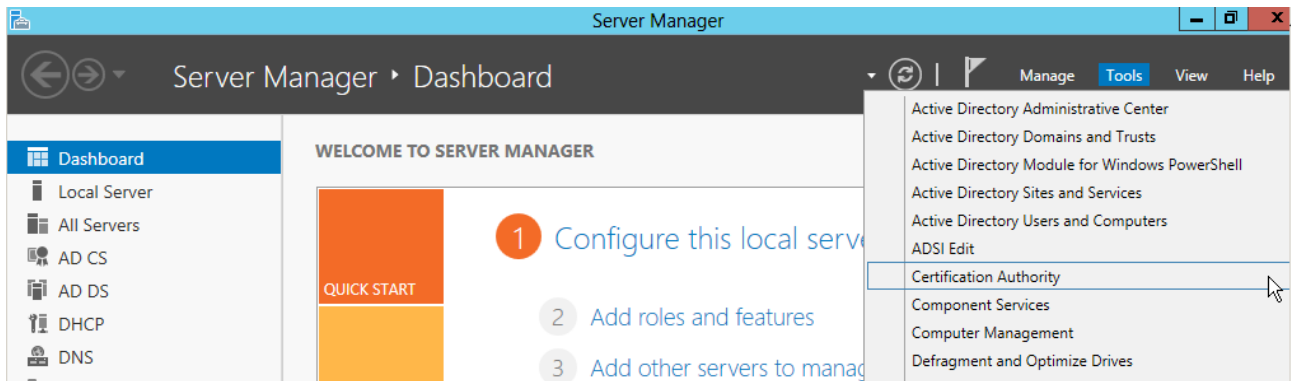
70 Wait until the installation finishes.



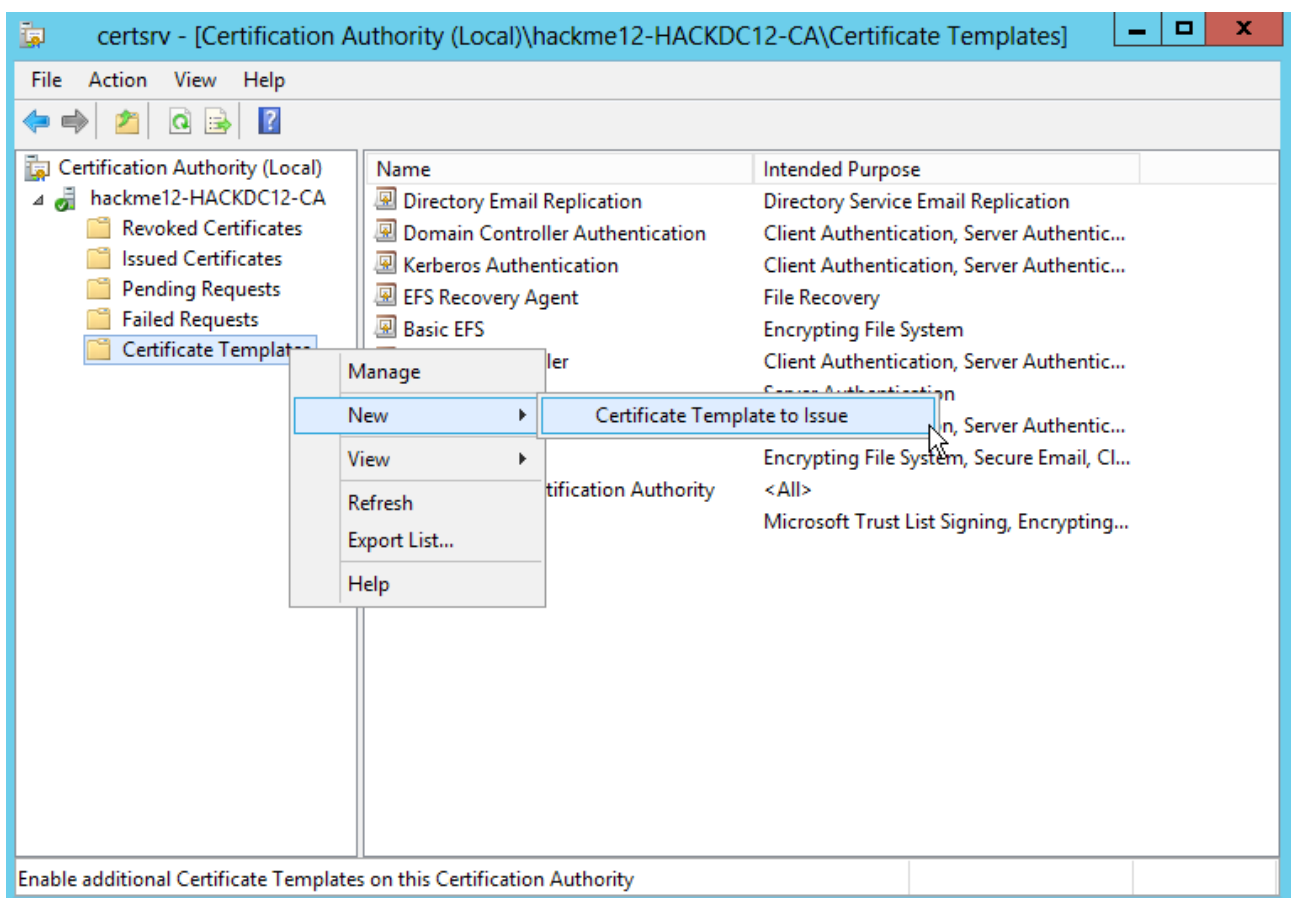
Configure the certificate authority

By default the Certificate authority does not issue certificate good for RAS and IAS server, so we should enable that certificate template as well.

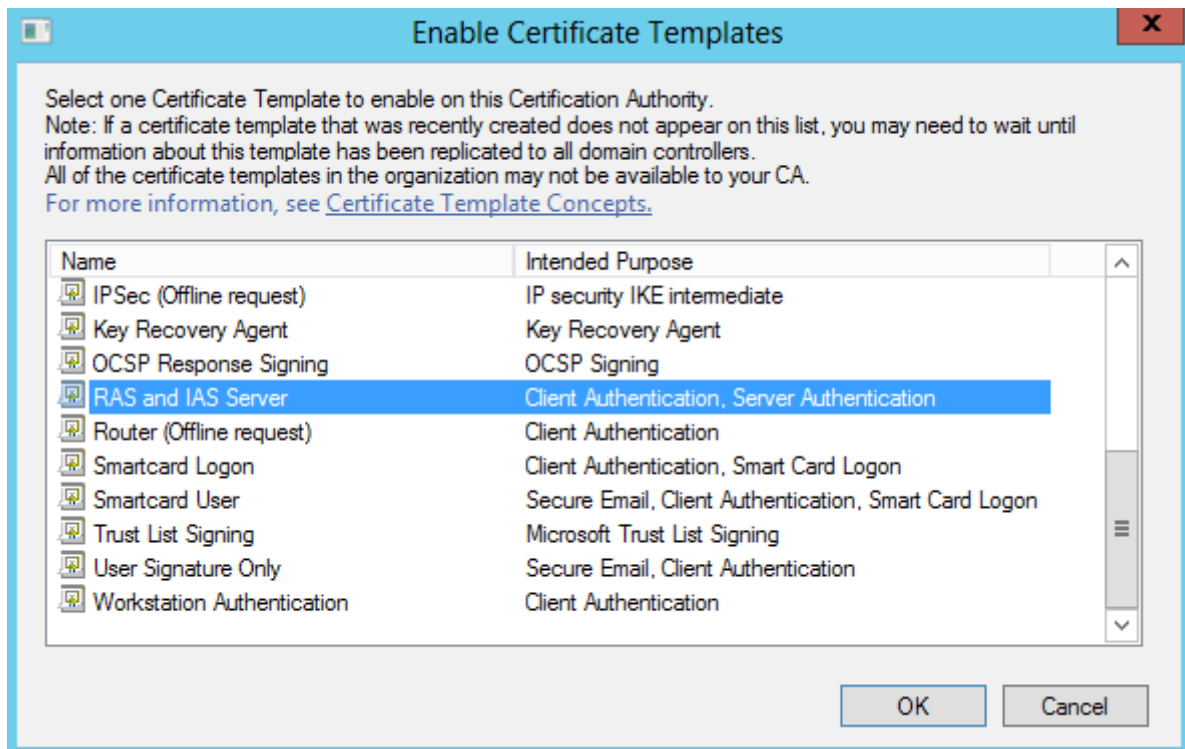
1. start the Certification Authority management console



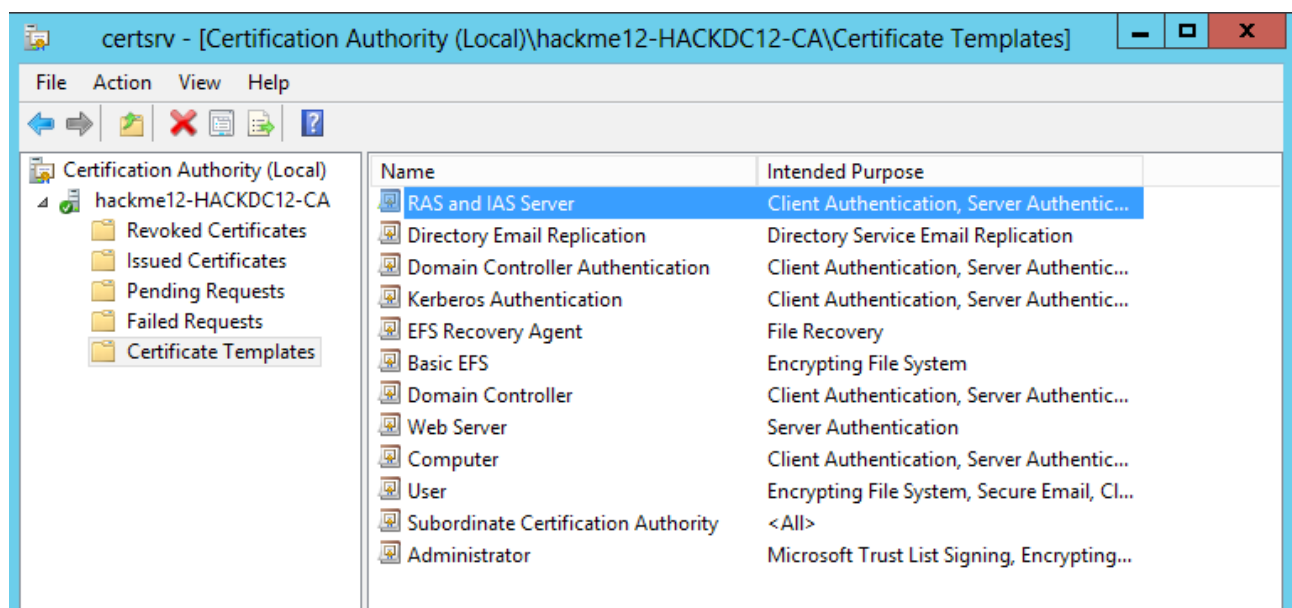
2. right click tot he “Certificate Templates”, then from the popup menu select new / Certificate Template to Issue



3. from the Certificate templates select the “RAS and IAS Server”, then click to OK



4. check, if this template really appears among the templates.

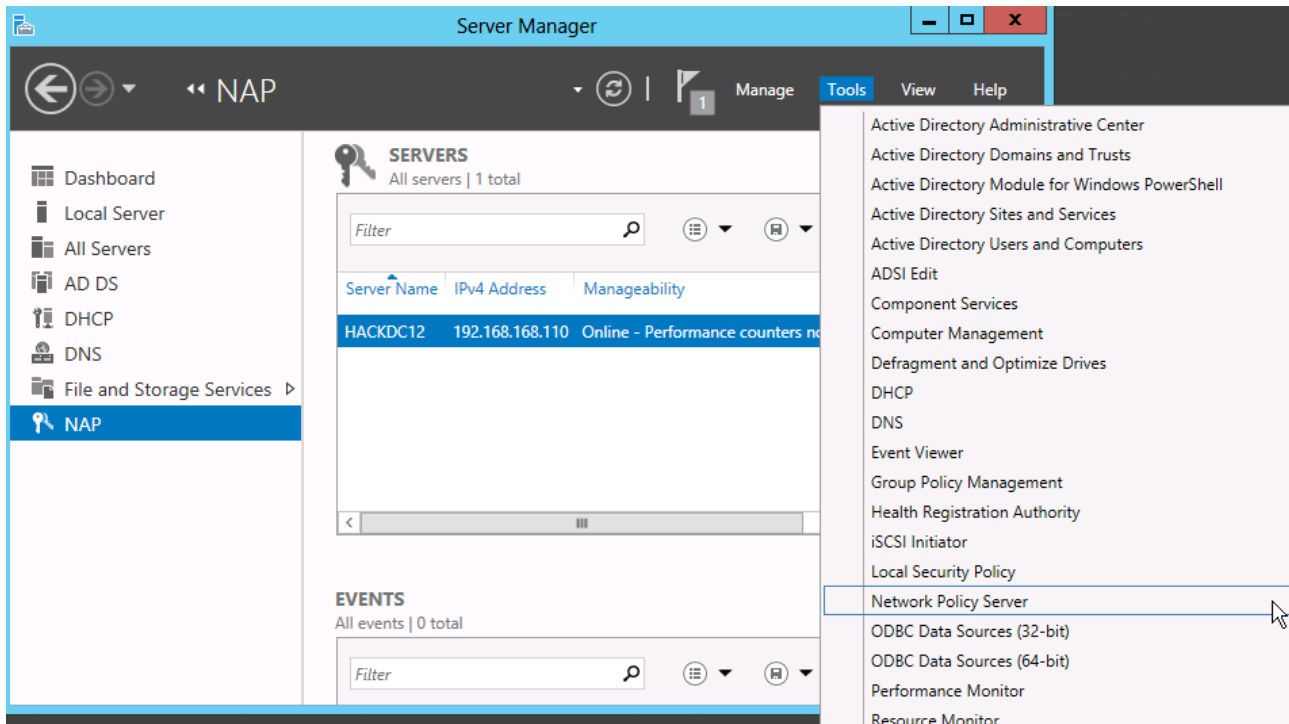


5. give some time to your computer, to request a certificate automatically, you may can reboot it, just to be sure. It is recommended, to run a `gpupdate /force` on the client, may be to reboot it, to get the the certificate of this newly installed enterprise root ca through the AD communication.

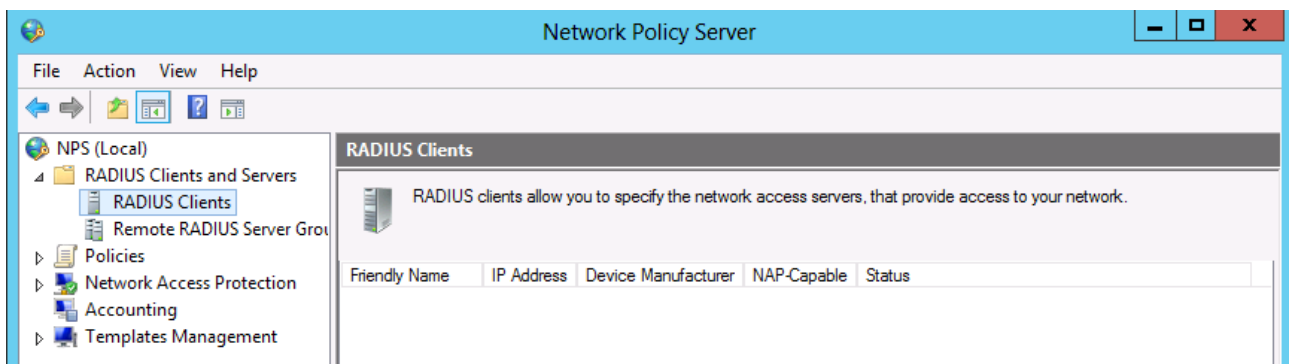
Configure the RADIUS server

Set up the switch as RADIUS client

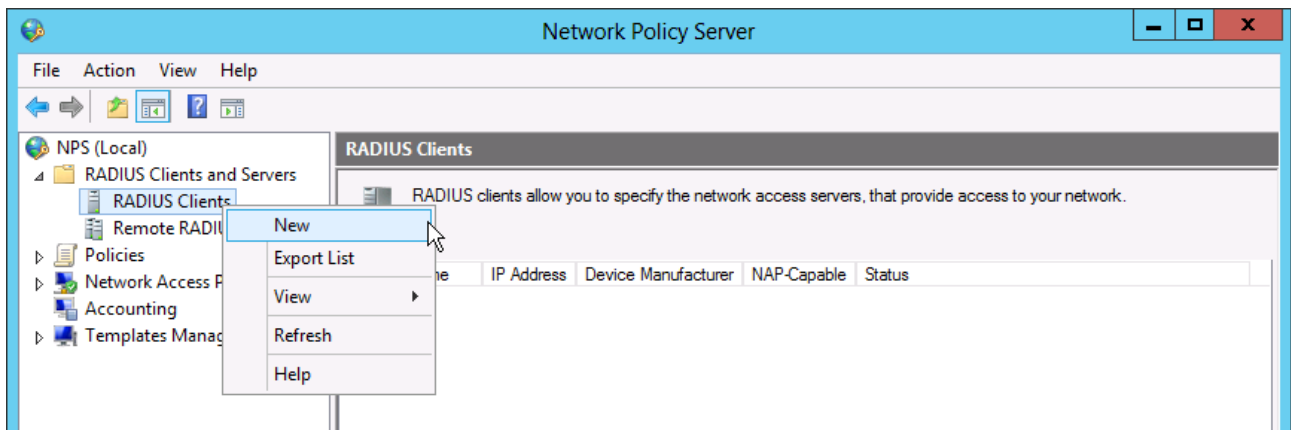
71 start the NAP server management tool



72 Select the RADIUS Clients, to configure the switch as RADIUS client.



73 right click to the Radius Clients and select “New” from the popup menu



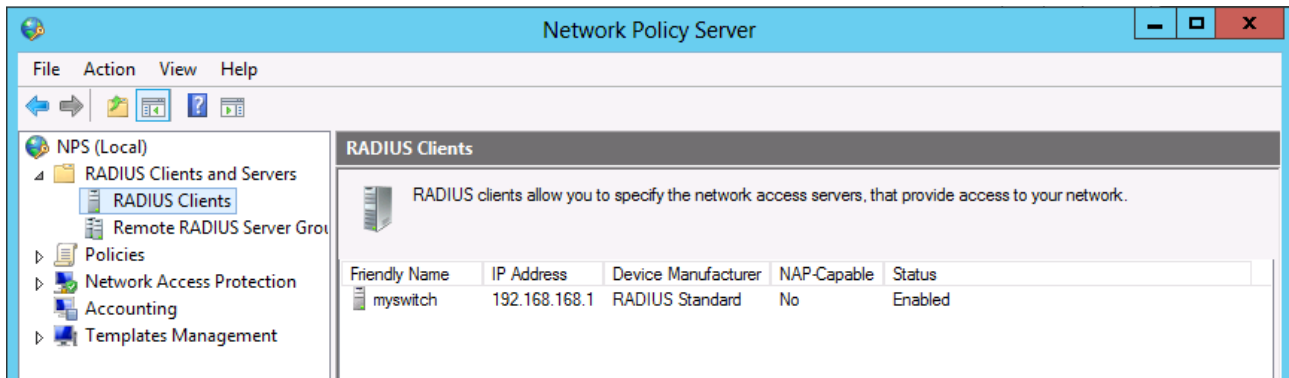
74 give a friendly name to the switch and configure the IP address of it. I will use for the switch the IP 192.168.168.1. After it we must configure a shared secret between the switch and the RADIUS server, what they will use, to mutually authenticate eachother. I used the password cisco123. It can be anything in general at least a 10 character long key is recommended, because it is a quite weak authentication method.

 The 'New RADIUS Client' dialog box is shown with the 'Settings' tab active.

- ☒ Enable this RADIUS client
- ☐ Select an existing template: (empty dropdown)
- Name and Address**
 - Friendly name: myswitch
 - Address (IP or DNS): 192.168.168.1 [Verify...]
- Shared Secret**
 - Select an existing Shared Secrets template: None
 - 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: [masked]
 - Confirm shared secret: [masked]

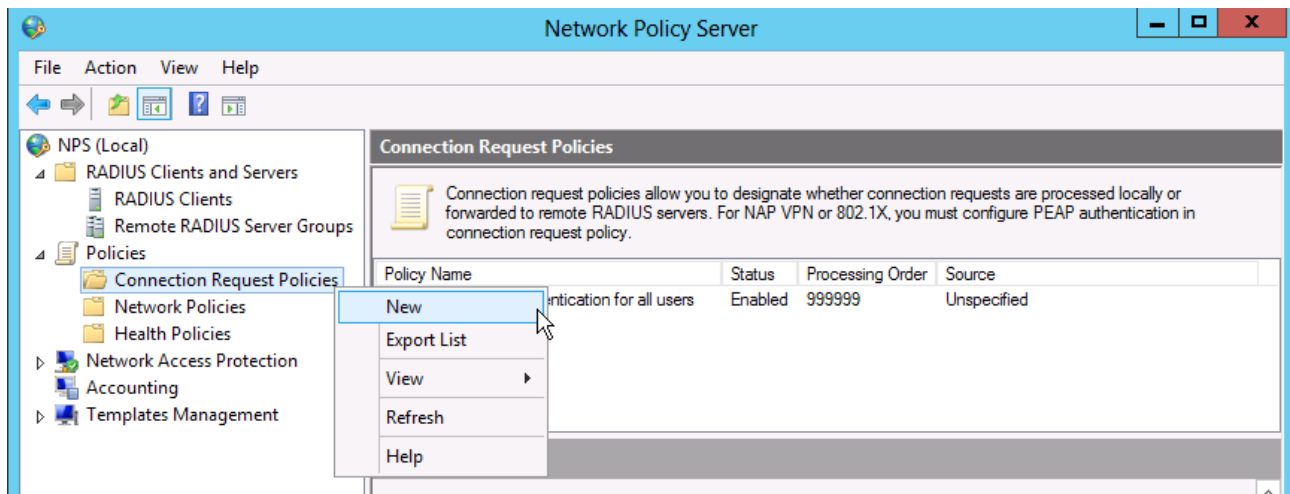
 At the bottom are 'OK' and 'Cancel' buttons.

75 Check if the new RADIUS client is created.

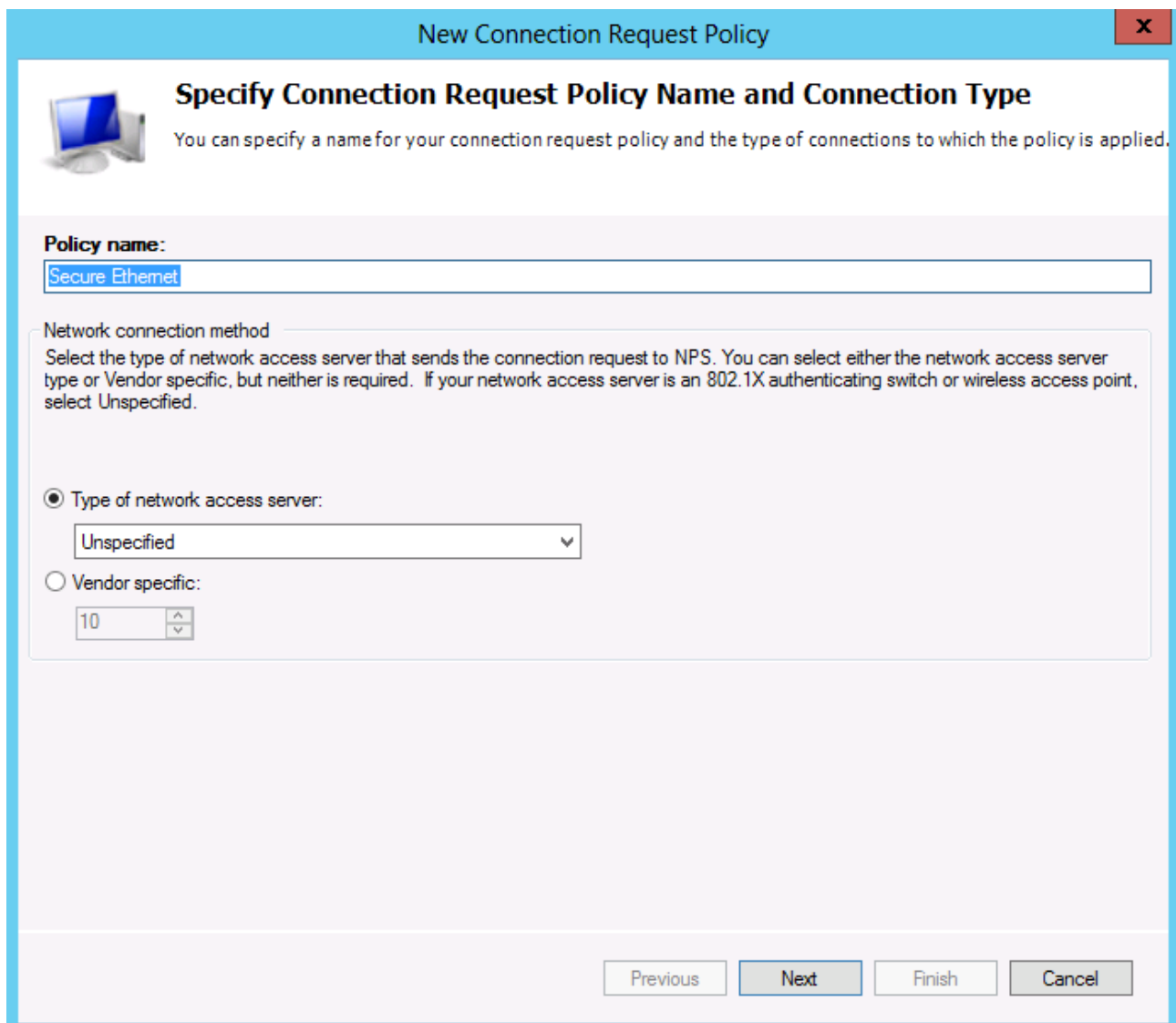


Set up the Connection Request Policy on the RADIUS Server

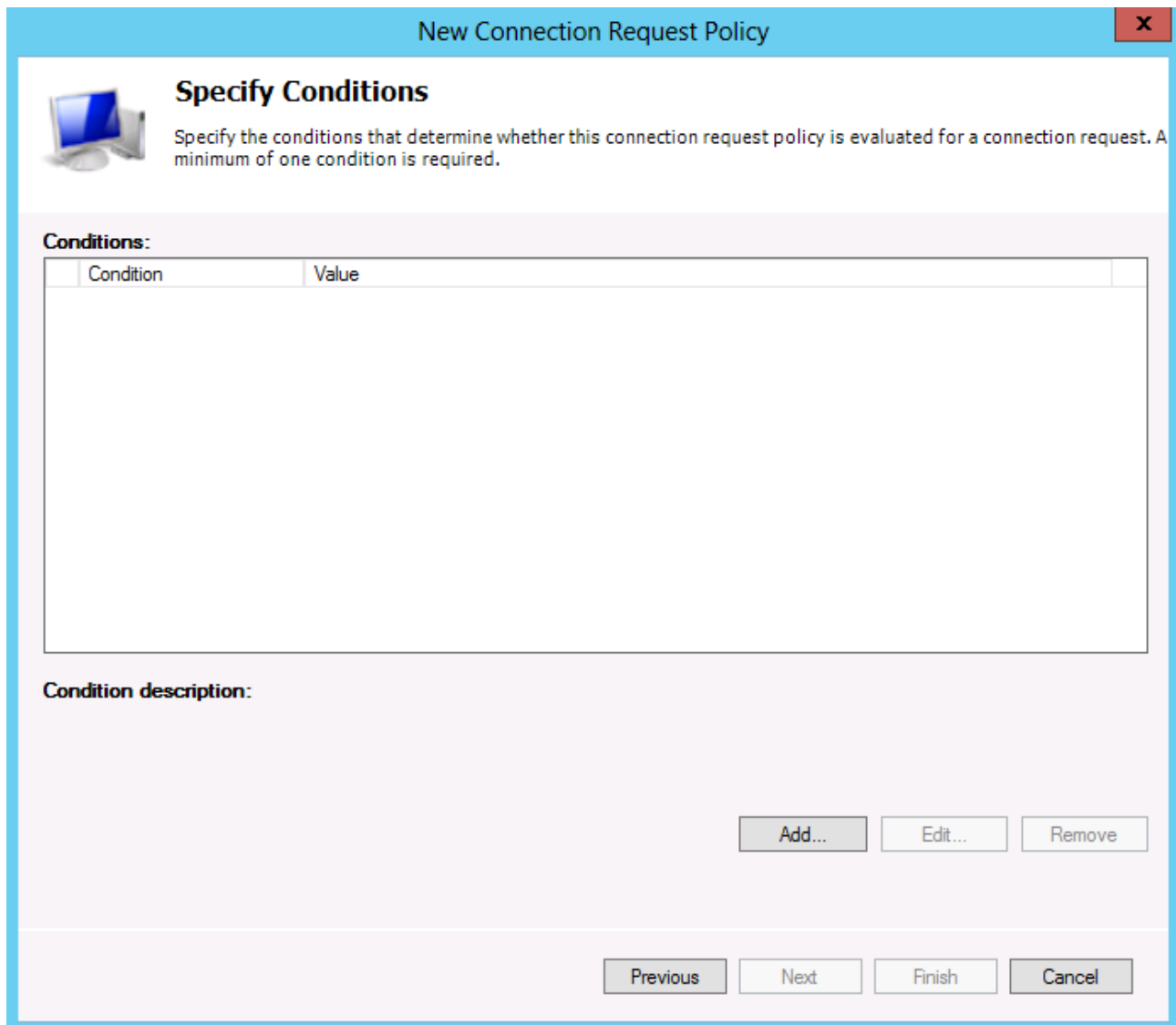
76 right click to the “Connection Request Policies”, and select New from the popup menu.



77 give a name to the “Connection Request Policy”, and leave the type as “Unspecified”



78 On the “Specify Conditions” window click to the “Add...” button, to define a condition.



The screenshot shows a window titled "New Connection Request Policy" with a close button (X) in the top right corner. The main area is titled "Specify Conditions" and includes a small icon of a computer monitor. Below the title, there is a text box with the instruction: "Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required." Below this text is a table with two columns: "Condition" and "Value". The table is currently empty. Below the table, there is a section labeled "Condition description:". At the bottom right of the window, there are three buttons: "Add...", "Edit...", and "Remove". At the very bottom of the window, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

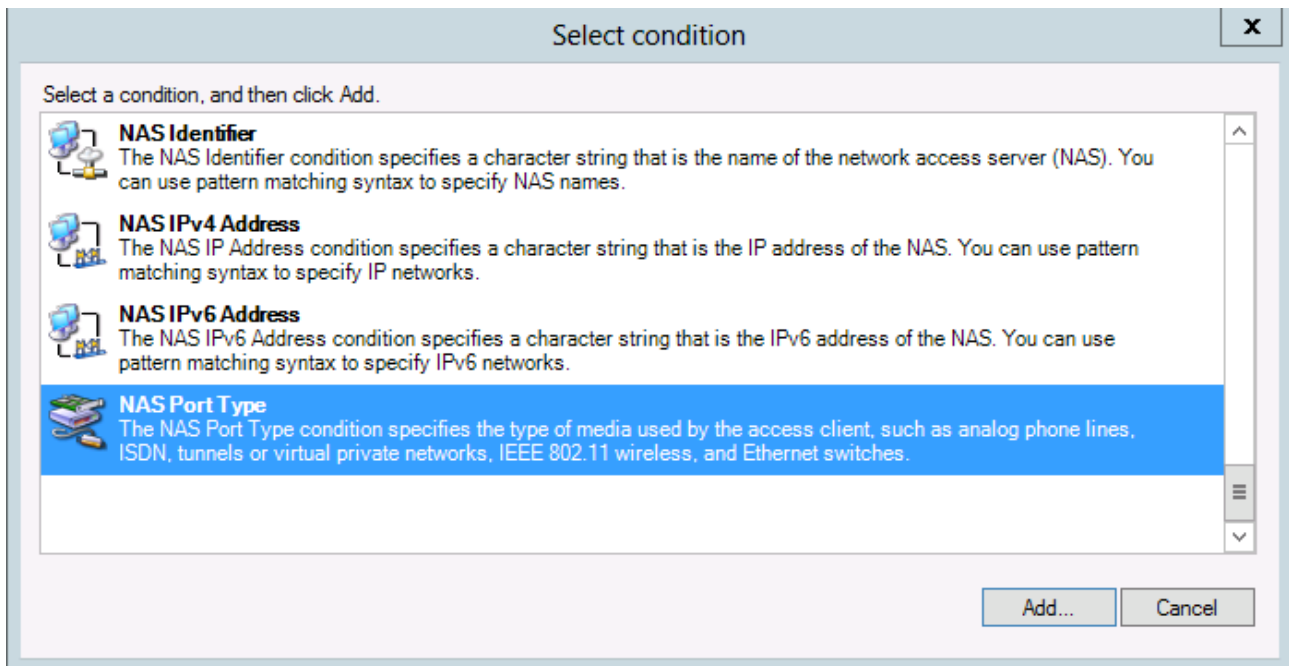
Condition	Value
-----------	-------

Condition description:

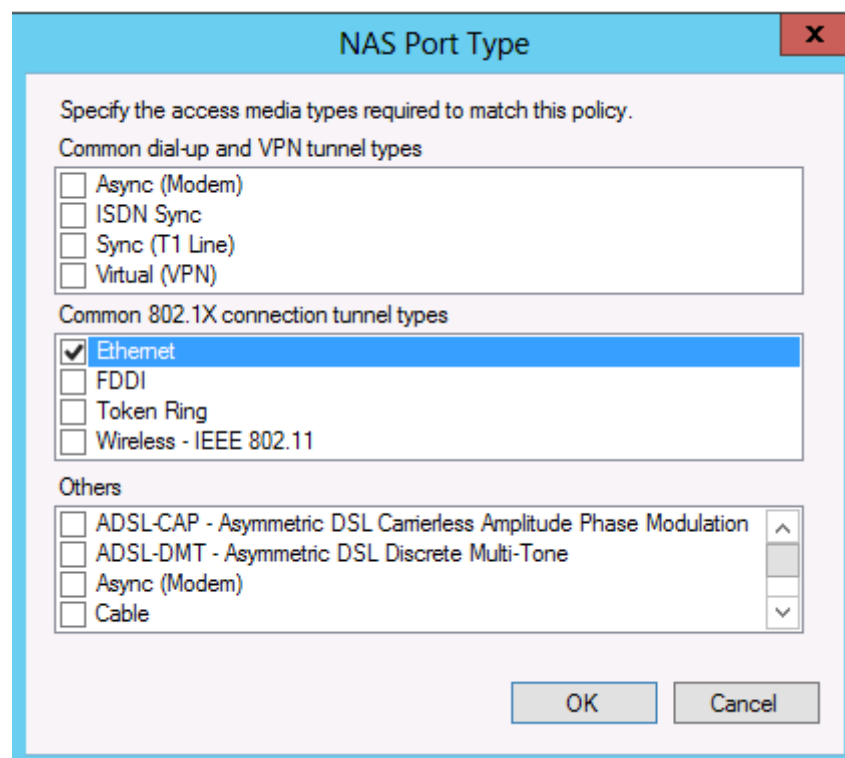
Add... Edit... Remove

Previous Next Finish Cancel

79 Select NAS port type as condition.




80 Select Ethernet as port type (we want to answer to the 802.1x requests)



81. on the “Specify Connection Request Forwarding” we do not want to forward the request to select “Authenticate request on this server” and click to next button.

New Connection Request Policy



Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request

→ Authentication

Accounting

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

☒ Authenticate requests on this server

☐ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

New...

☐ Accept users without validating credentials

Previous


Next

Finish

Cancel

82 On the "Specify Authentication Methods" window do not select any authentication method (we will configure them later on the Network Policies), just click to the next button.

New Connection Request Policy



Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.

☐ 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:

Move Up

Move Down

Add...

Edit...

Remove

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.

Previous


Next

Finish

Cancel

83 On the “Configure Settings” window click to the next button

New Connection Request Policy



Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

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

Settings:

Specify a Realm Name

Attribute

RADIUS Attributes

Standard

☒ Vendor Specific

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute:

Called-Station-Id

Rules:

Find	Replace With
------	--------------

Add

Edit

Remove

Move Up

Move Down

Previous

Next

Finish

Cancel

84 On the completing window click to the Finish button

New Connection Request Policy

Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

Secure Ethernet

Policy conditions:

Condition	Value
NAS Port Type	Ethernet

Policy settings:

Condition	Value
Authentication Provider	Local Computer

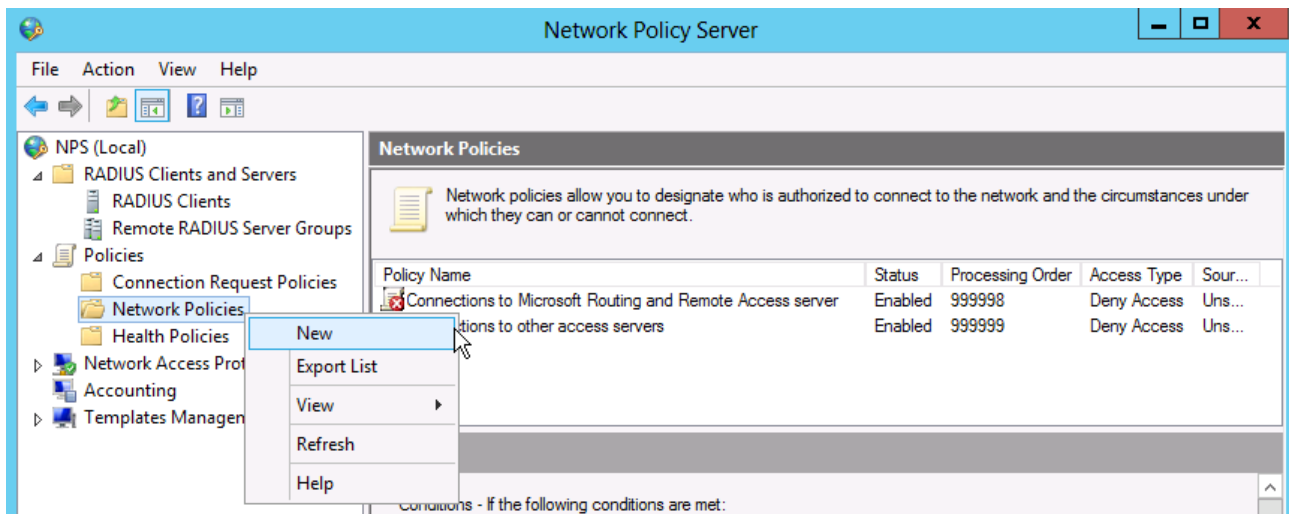
To close this wizard, click Finish.

85 check if the policy is created

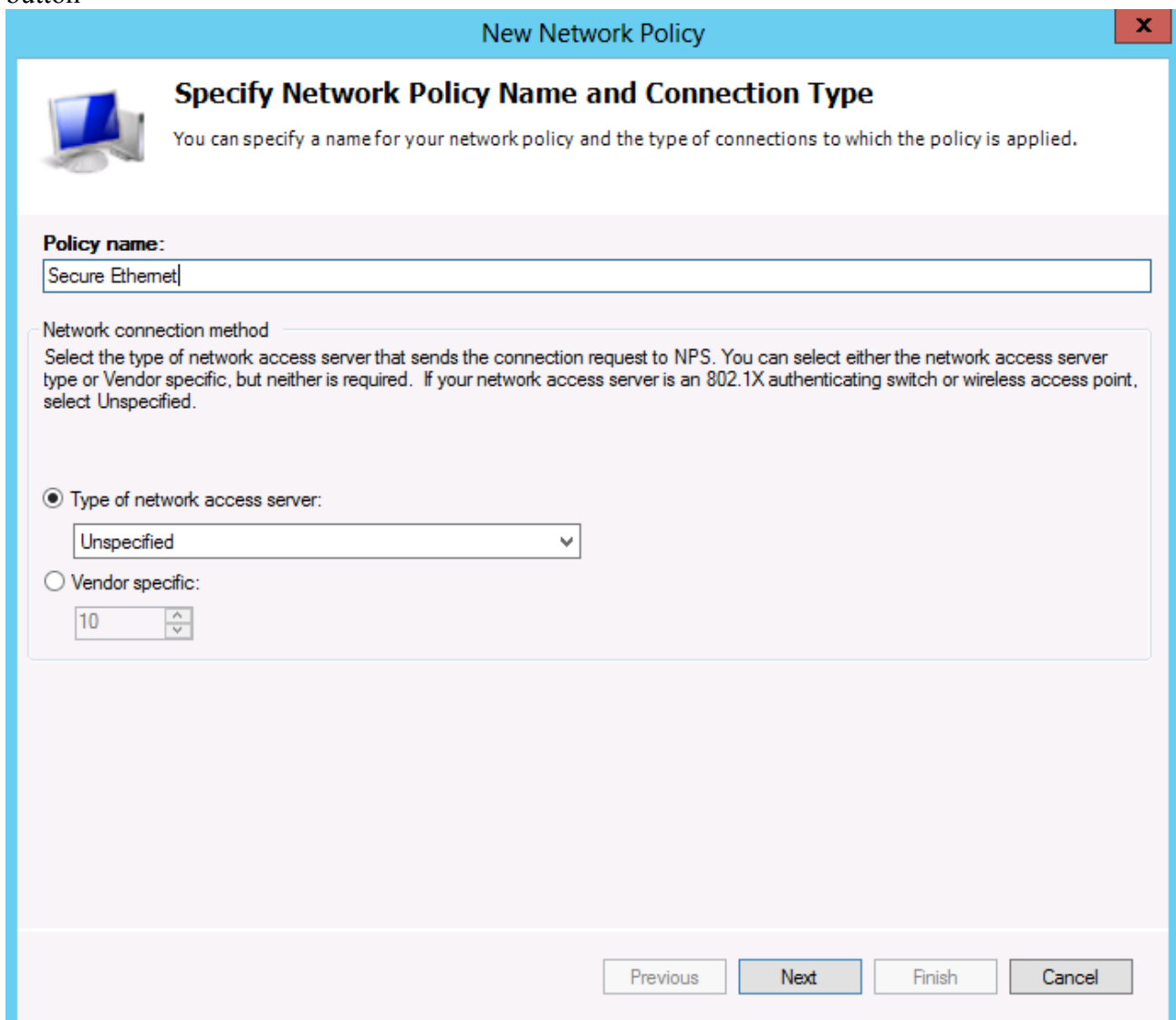
Network Policy Server															
<div> <div> <div>NPS (Local)</div> <div> <div> <div>RADIUS Clients and Servers</div> <div> <div>RADIUS Clients</div> <div>Remote RADIUS Server Groups</div> </div> </div> <div> <div>Policies</div> <div> <div>Connection Request Policies</div> <div>Network Policies</div> <div>Health Policies</div> </div> </div> <div> <div>Network Access Protection</div> <div>Accounting</div> <div>Templates Management</div> </div> </div> </div> <div> <div>Connection Request Policies</div> <div> <div> <div> <div>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.</div> </div> <table> <tr> <th>Policy Name</th><th>Status</th><th>Processing Order</th><th>Source</th></tr> <tr> <td>Secure Ethernet</td><td>Enabled</td><td>1</td><td>Unspecified</td></tr> <tr> <td>Use Windows authentication for all users</td><td>Enabled</td><td>999999</td><td>Unspecified</td></tr> </table> </div> </div> </div></div>				Policy Name	Status	Processing Order	Source	Secure Ethernet	Enabled	1	Unspecified	Use Windows authentication for all users	Enabled	999999	Unspecified
Policy Name	Status	Processing Order	Source												
Secure Ethernet	Enabled	1	Unspecified												
Use Windows authentication for all users	Enabled	999999	Unspecified												

Set up the Network Policy on the RADIUS Server

86 Right click to the “Network Policies” and from the popup menu select the New command



87 Give a name to the Network Policy, leave the type of it as Unspecified the click to the Next button



88 On the Specify Conditions window click to the “Add...” button

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

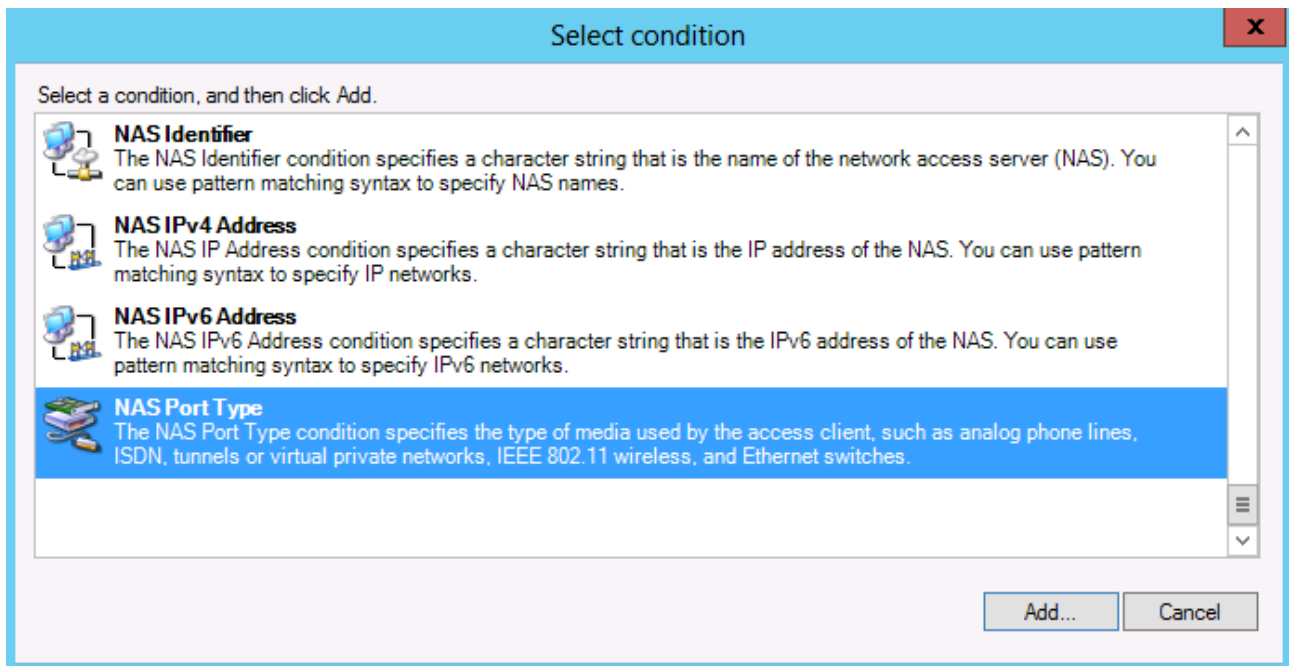
Condition	Value
-----------	-------

Condition description:

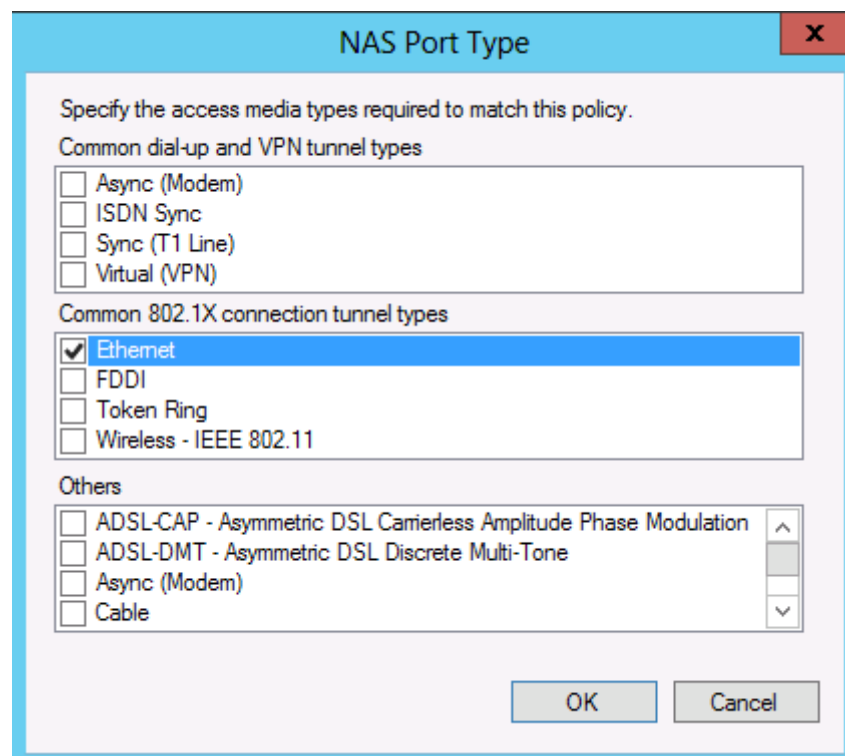
Add... **Edit...** **Remove**

Previous **Next** **Finish** **Cancel**

89 Select NAS port type as condition.



90 Select Ethernet as port type, then click to the OK button



91 Click again to the “Add...” button

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

	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.

Add...
Edit...
Remove

Previous
Next
Finish
Cancel

92 Select “Windows Groups” as condition, then click to the “Add...” button

Select condition

Select a condition, and then click Add.

Groups

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

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

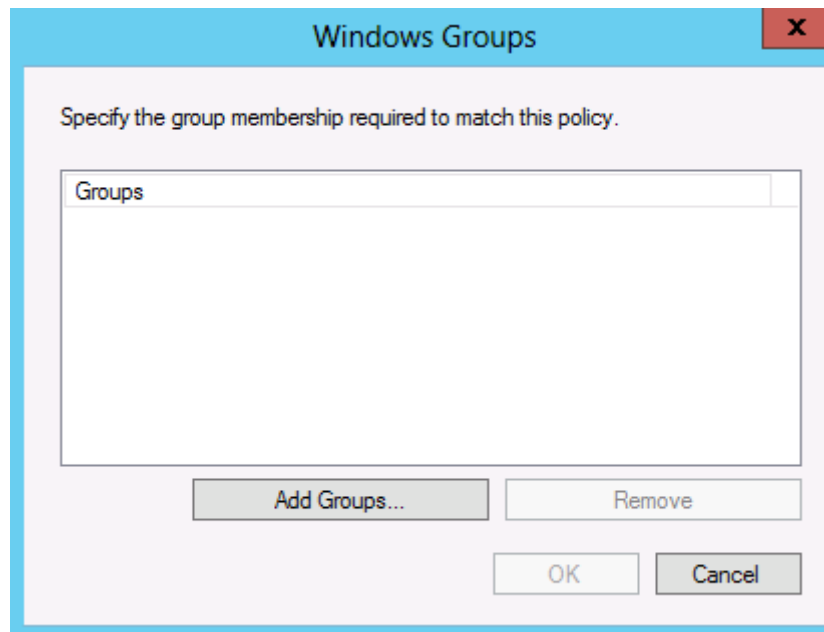
User Groups
 The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

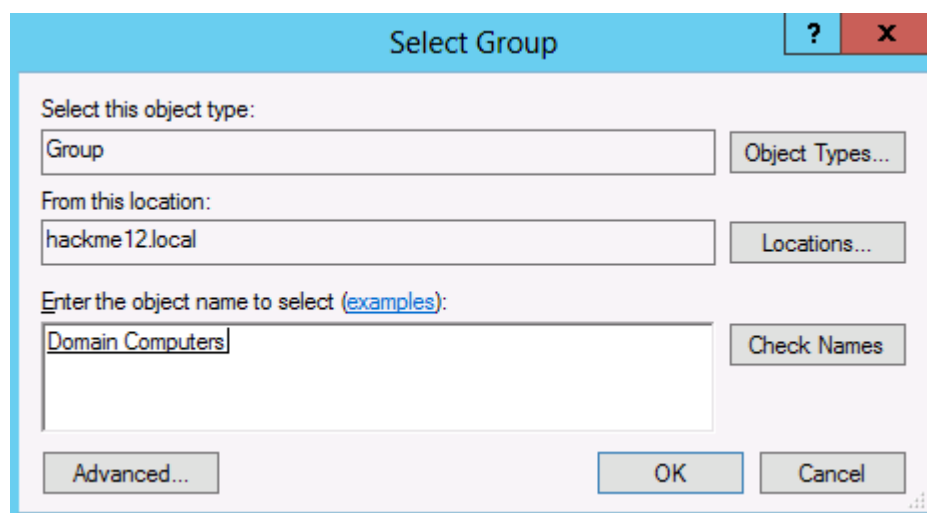
Location Groups
 The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

Add...
Cancel

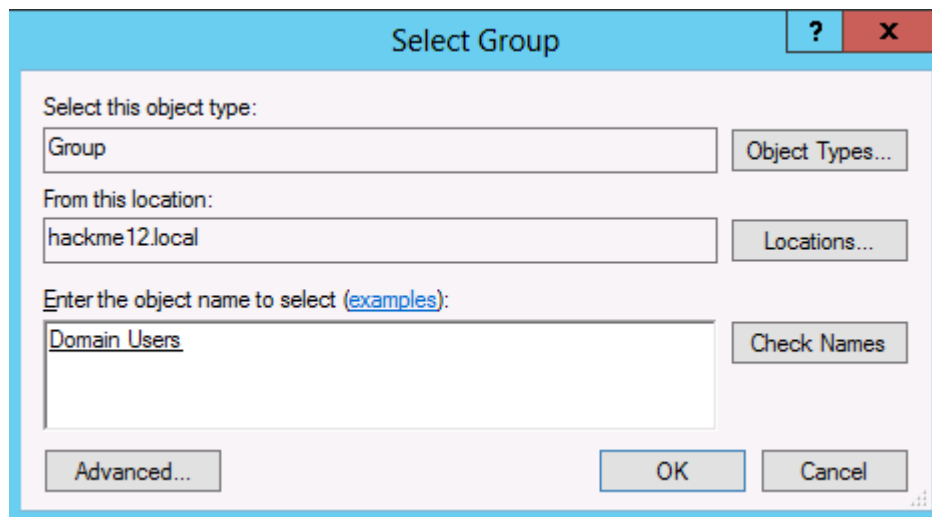
93 Click to the “Add Groups...” button



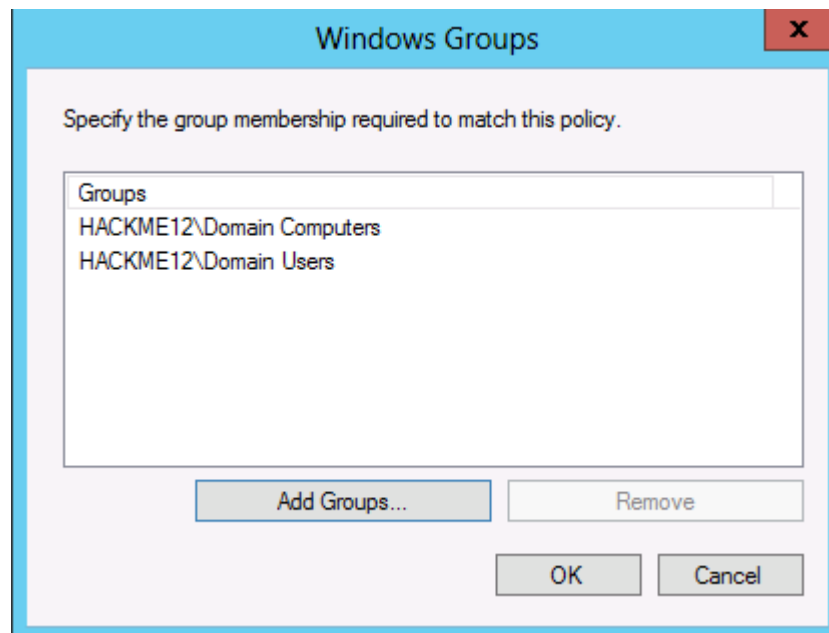
94 Add the “Domain Computers” (when the user is not logged in the computer will use it's own account, to authenticate. Without it there can be problems with downloading computer policies, login and things like that). Then click to the OK button



95 Then add the “Domain Users”. After the user logged in, the computer will reauthenticate, because may be depending on the logged on user you want to set up different VLAN, or whatever. If you do not want it there is a registry key, to use the computer account after the user logged in.




96 Check, you added both groups, then click to the OK button



97 Check, if there is “OR” condition between the two groups, then click to the Next button



New Network Policy



Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
 NAS Port Type	Ethernet
 Windows Groups	HACKME12\Domain Computers OR HACKME12\Domain Users

Condition description:

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

Add...

Edit...

Remove

Previous


Next

Finish

Cancel

98 we want to enable the communication if someone authenticated so select Access Granted on the “Specify Access Permission” windows, then click to the next button

New Network Policy x



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous

Next


Finish

Cancel

99 On the “Configure Authentication Methods” window click to the “Add...” button under the EAP types

New Network Policy

X



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

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

Previous

Next

Finish

Cancel

100 and from the popup menu select Microsoft Protected EAP (PEAP), and click to the OK button.

Add EAP

X

Authentication methods:

Microsoft: Smart Card or other certificate

Microsoft: Protected EAP (PEAP)

Microsoft: Secured password (EAP-MSCHAP v2)

<

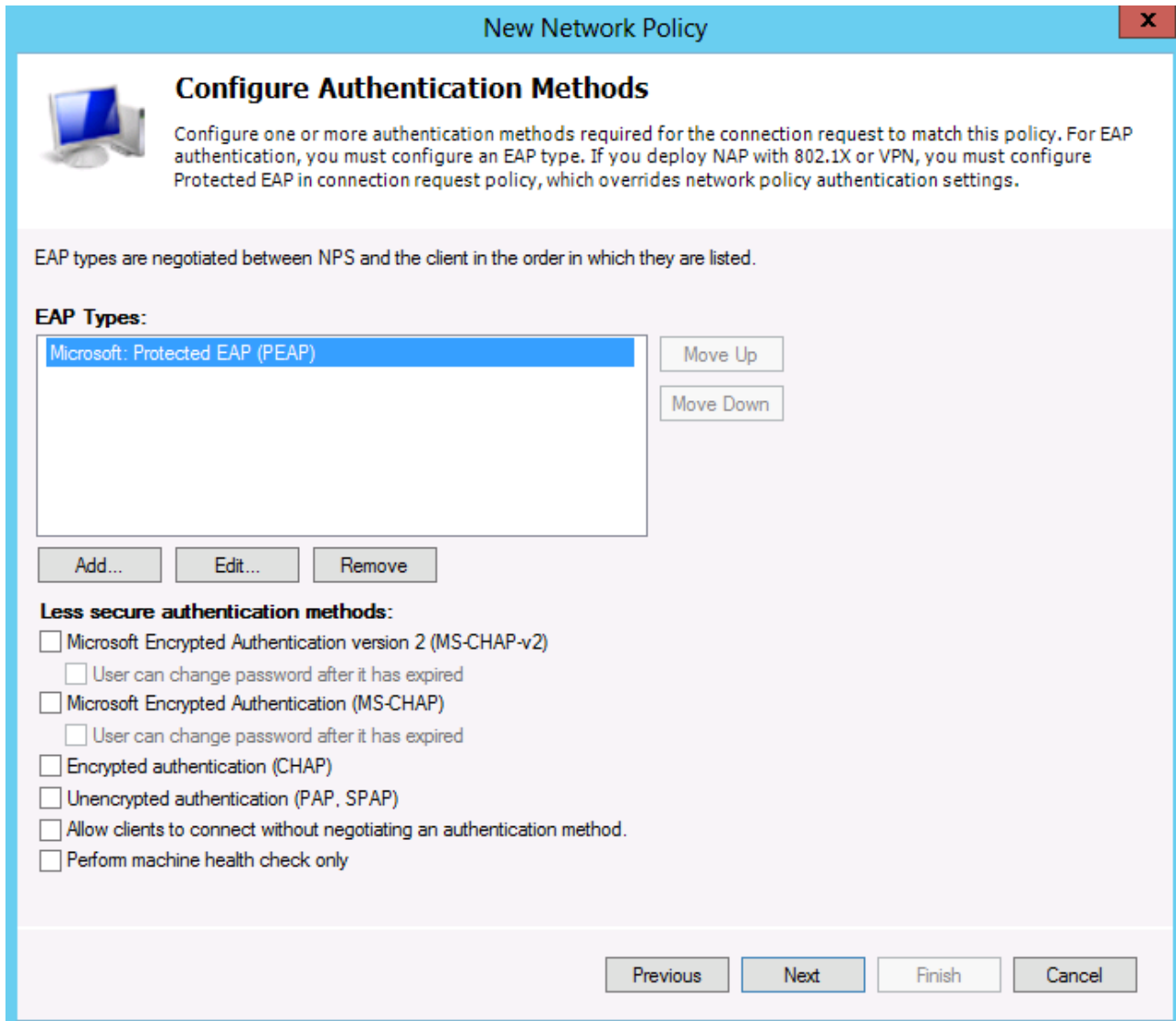
|||

>

OK

Cancel

101 Select the newly added EAP type, and click to the “Edit...” button



The screenshot shows the 'New Network Policy' dialog box with the 'Configure Authentication Methods' tab selected. The title bar reads 'New Network Policy' with a close button. Below the title bar is a section titled 'Configure Authentication Methods' with a computer icon and explanatory text: 'Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.'

Below this is a note: 'EAP types are negotiated between NPS and the client in the order in which they are listed.'

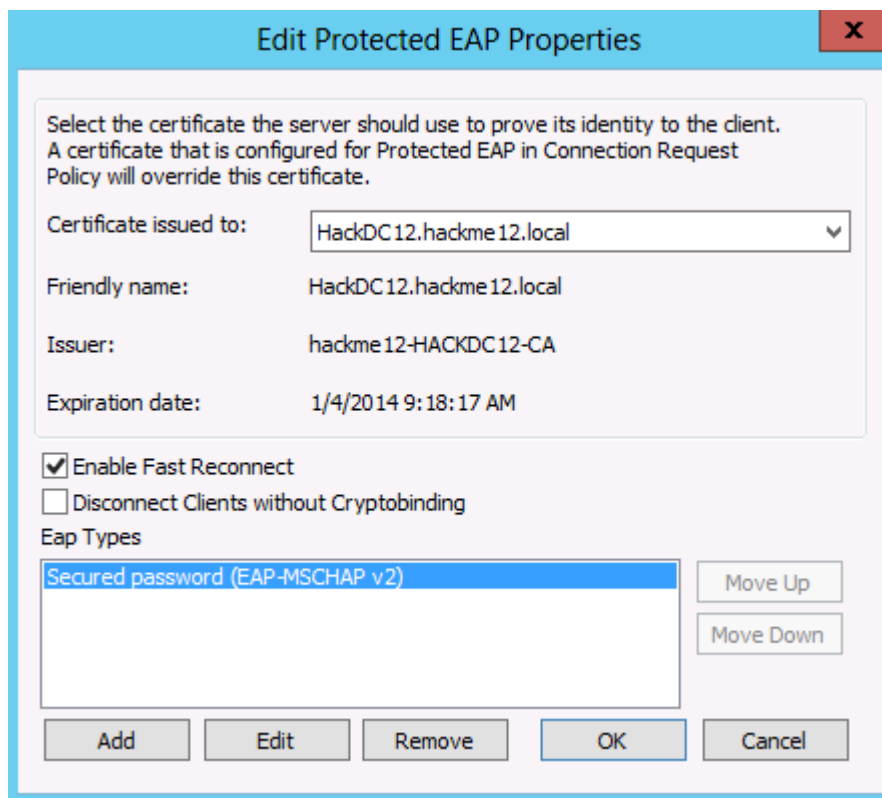
The 'EAP Types:' section contains a list box with 'Microsoft: Protected EAP (PEAP)' selected. To the right of the list box are 'Move Up' and 'Move Down' buttons. Below the list box are 'Add...', 'Edit...', and 'Remove' buttons.

The 'Less secure authentication methods:' section contains several unchecked checkboxes:

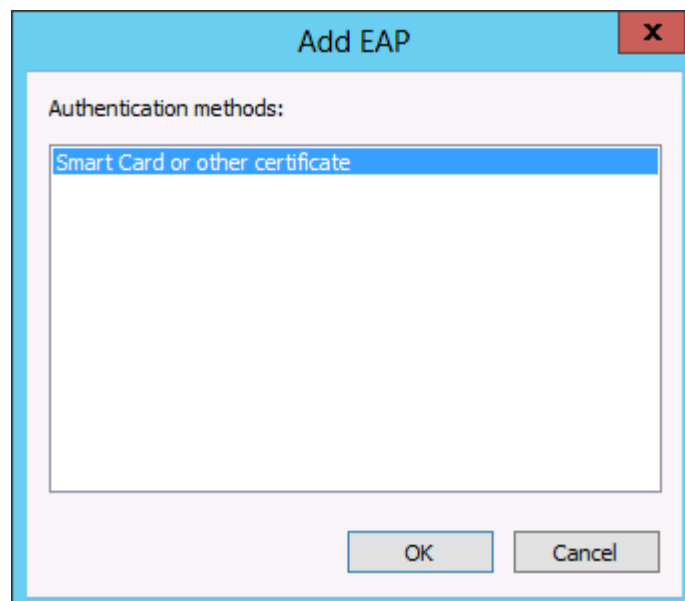
- ☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☐ User can change password after it has expired
- ☐ Microsoft Encrypted Authentication (MS-CHAP)
 - ☐ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow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

At the bottom right are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

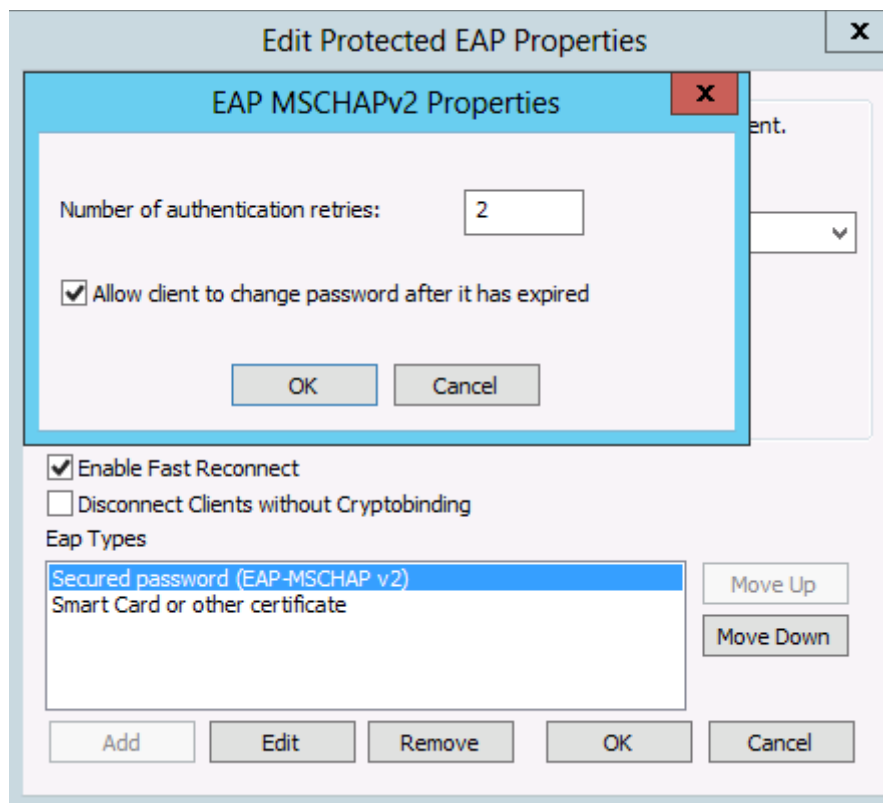
102 Select the certificate we want to use Hopefully you already got one, if not, then request server certificate for IAS and authentication server type. **Do NOT use the certificate of the CA server itself, that will not work!** Then click to the “Add...” button, to add other authentication type:



103 Select “Smart Card or other certificate” as authentication method, then click to the OK button:




104 I set the “Allow client to change password after it has expired”, to make



105 On the Configure Authentication Methods click next

New Network Policy



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Microsoft: Protected EAP (PEAP)

Move Up

Move Down

Add...

Edit...

Remove

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

Previous


Next

Finish

Cancel

106 On the “Configure Constraints” window click to the next button

New Network Policy




Configure Constraints


Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.


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


Constraints:


Constraints

 Idle Timeout

 Session Timeout

 Called Station ID

 Day and time restrictions

 NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

^

v

Previous


Next

Finish

Cancel

107 On the Configure Settings window click to the “Add...” button

New Network Policy



Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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

Settings:

RADIUS Attributes

☒ Standard

☐ Vendor Specific

Network Access Protection

☐ NAP Enforcement

☒ Extended State

Routing and Remote Access

☐ Multilink and Bandwidth Allocation Protocol (BAP)

☐ IP Filters

☐ Encryption

☒ IP Settings

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.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

108 Select “Tunnel-Medium-Type” then click to the “Add...” button

Add Standard RADIUS Attribute X

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

Attributes:

Name
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID
Tunnel-Client-Endpt
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Port-Group-ID

Description:

Specifies the transport medium used when creating a tunnel for protocols (for example, L2TP) that can operate over multiple transports.

109 On the Attribute Information window click again to the “Add...” button

Attribute Information X

Attribute name:
Tunnel-Medium-Type

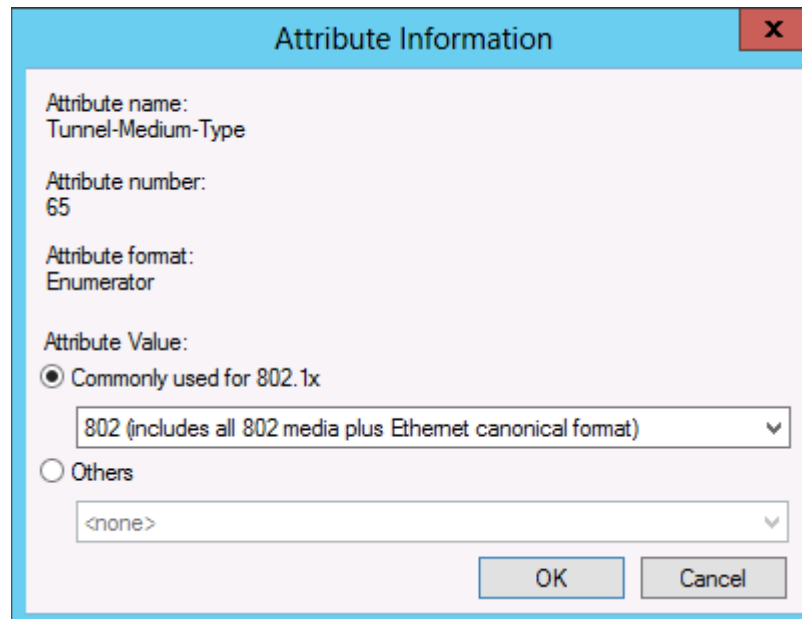
Attribute number:
65

Attribute format:
Enumerator

Attribute values:

Vendor	Value

110 Select “Commonly used for 802.1x” as attribute information

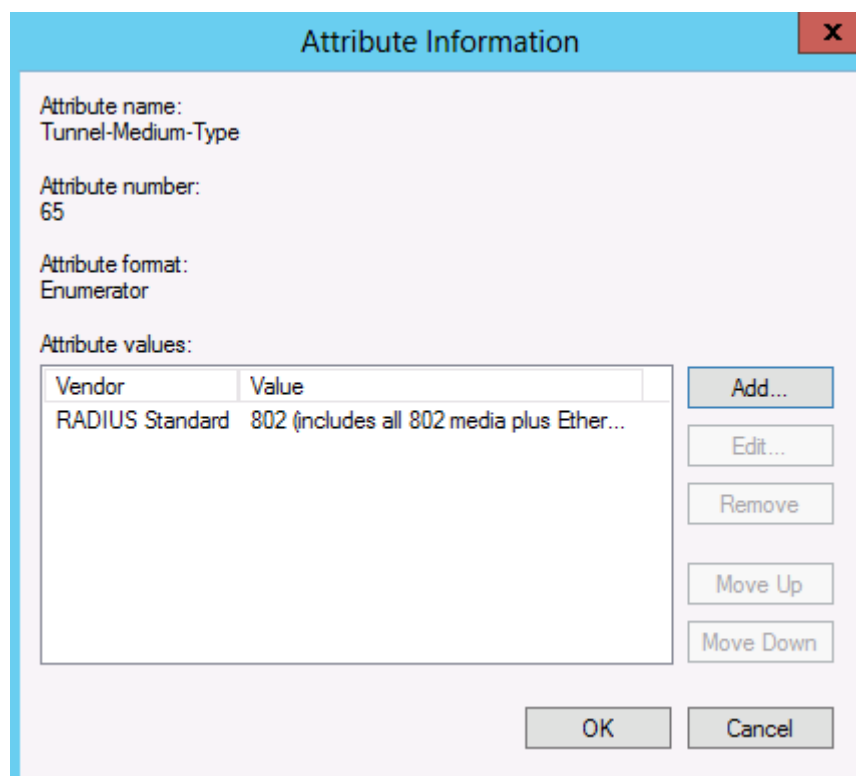


The dialog box titled "Attribute Information" has a red close button in the top right corner. It contains the following fields and options:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerator
- Attribute Value:
 - ☒ Commonly used for 802.1x
 - 802 (includes all 802 media plus Ethernet canonical format)
 - ☐ Others
 - <none>

At the bottom right are "OK" and "Cancel" buttons.

111 Click to the OK button on the “Attribute information” window



The dialog box titled "Attribute Information" has a red close button in the top right corner. It contains the following fields and options:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerator
- Attribute values:

Vendor	Value
RADIUS Standard	802 (includes all 802 media plus Ether...

To the right of the table are buttons: "Add...", "Edit...", "Remove", "Move Up", and "Move Down". At the bottom right are "OK" and "Cancel" buttons.

112 Select “Tunel-Preference” as next attribute we want to define

Add Standard RADIUS Attribute X

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

Attributes:

Name
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID
Tunnel-Client-Endpt
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID

Description:

Specifies the relative preference assigned to each tunnel when more than one set of tunneling attributes is returned to the tunnel initiator.

113 give it a value 1, then click to the OK button

Attribute Information X

Attribute name:
Tunnel-Preference

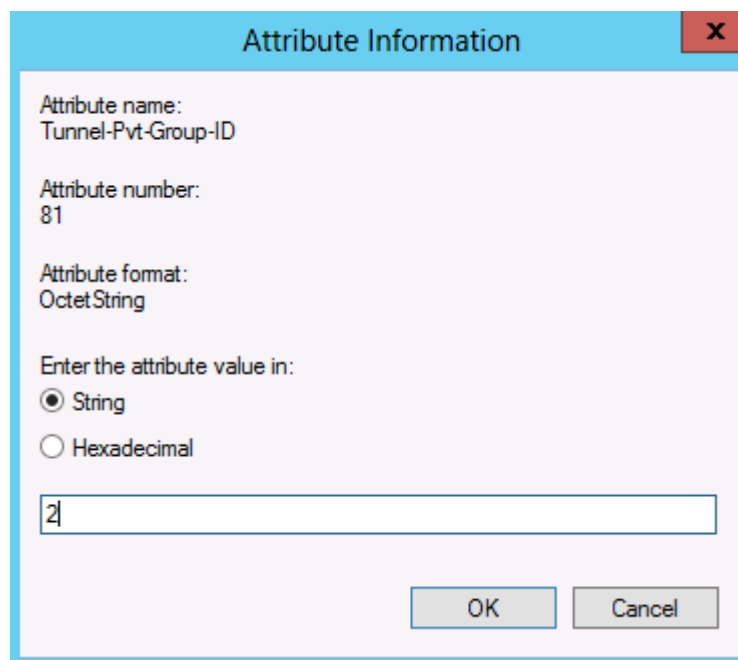
Attribute number:
83

Attribute format:
Integer

Attribute value:

114 Select Tunnel-Pvt-Group-ID as next attribute, and click to the Add... button

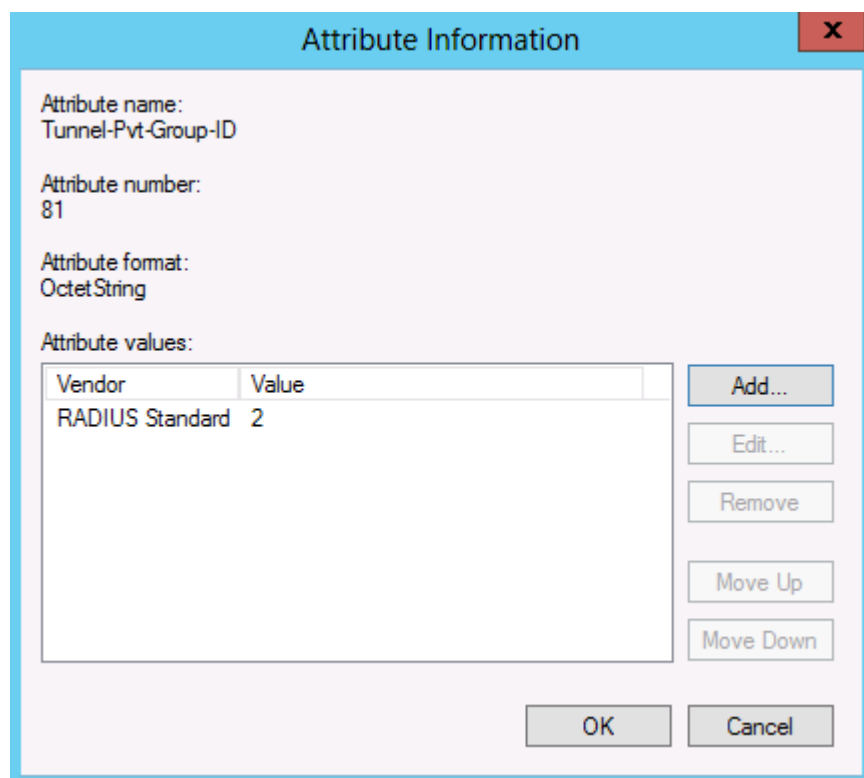
116 Define the VLAN you want the user became the member after the authentication. I will use the VLAN 2 as the authenticated users VLAN.



The 'Attribute Information' dialog box is shown. It has a title bar with a close button (X). The fields are: Attribute name: Tunnel-Pvt-Group-ID, Attribute number: 81, Attribute format: OctetString. Under 'Enter the attribute value in:', the 'String' radio button is selected. A text box contains the value '2'. At the bottom are 'OK' and 'Cancel' buttons.

Attribute name:	Tunnel-Pvt-Group-ID
Attribute number:	81
Attribute format:	OctetString
Enter the attribute value in:	<input checked="" type="radio"/> String <input type="radio"/> Hexadecimal
	<input type="text" value="2"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

117 click OK on the Attribute Information window



The 'Attribute Information' dialog box is shown after clicking OK. It now displays a table of attribute values. The table has two columns: 'Vendor' and 'Value'. The first row shows 'RADIUS Standard' and '2'. To the right of the table are buttons: 'Add...', 'Edit...', 'Remove', 'Move Up', and 'Move Down'. At the bottom are 'OK' and 'Cancel' buttons.

Attribute name:	Tunnel-Pvt-Group-ID	
Attribute number:	81	
Attribute format:	OctetString	
Attribute values:		
	Vendor	Value
	RADIUS Standard	2
	<input type="button" value="Add..."/>	
	<input type="button" value="Edit..."/>	
	<input type="button" value="Remove"/>	
	<input type="button" value="Move Up"/>	
	<input type="button" value="Move Down"/>	
	<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

118 Select Tunnel-Type as next attribute, and click to the “Add...” button

Add Standard RADIUS Attribute ✕

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

All ▼

Attributes:

Name	^
Tunnel-Password	
Tunnel-Preference	
Tunnel-Pvt-Group-ID	
Tunnel-Server-Auth-ID	
Tunnel-Server-Endpt	
Tunnel-Type	

III

Description:
Specifies the tunneling protocols used.

Add...

Close

119 On the Attribute Information window click to the “Add...” button again

Attribute Information ✕

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

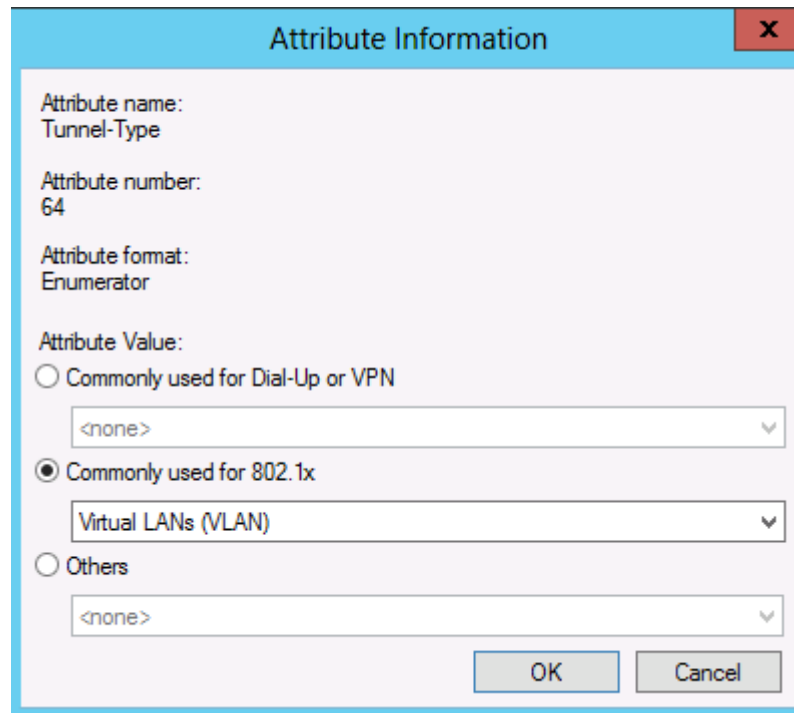
Attribute values:

Vendor	Value	
		<div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">Add...</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">Edit...</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">Remove</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">Move Up</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">Move Down</div>

OK

Cancel

120 Select Virtual LANs from the Commonly used for 802.1x, then click to the OK button

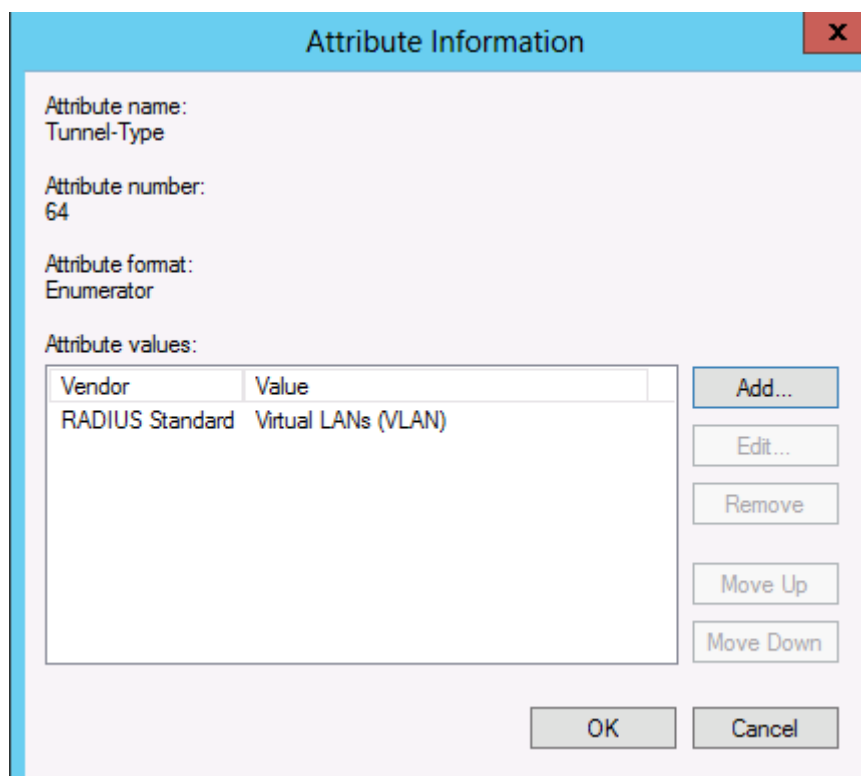


The "Attribute Information" dialog box is shown. It has a title bar with a close button (X). The dialog contains the following fields and options:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute Value:
 - ☐ Commonly used for Dial-Up or VPN
 - <none>
 - ☒ Commonly used for 802.1x
 - Virtual LANs (VLAN)
 - ☐ Others
 - <none>

At the bottom right are "OK" and "Cancel" buttons.

121 Click OK on the "Attribute information" window



The "Attribute Information" dialog box is shown. It has a title bar with a close button (X). The dialog contains the following fields and options:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

Add...

Edit...

Remove

Move Up

Move Down

At the bottom right are "OK" and "Cancel" buttons.

122 Click close on the "Add Standard RADIUS Attribute" window

Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

All

Attributes:

Name

Tunnel-Password

Tunnel-Preference

Tunnel-Pvt-Group-ID

Tunnel-Server-Auth-ID

Tunnel-Server-Endpt

Tunnel-Type

Description:


Specifies the tunneling protocols used.

Add...

Close

123 Check if all the settings are correct, then click to the next button

New Network Policy




Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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


Settings:

RADIUS Attributes

 Standard


☒ Vendor Specific


Network Access Protection


 NAP Enforcement

☒ Extended State

Routing and Remote Access

 Multilink and Bandwidth Allocation Protocol (BAP)

 IP Filters

 Encryption

☒ IP Settings

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.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Preference	1
Tunnel-Pvt-Group-ID	2
Tunnel-Type	Virtual LANs (VLAN)

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

124 on the completing window click to the Finish button

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Secure Ethernet

Policy conditions:

Condition	Value
NAS Port Type	Ethernet
Windows Groups	HACKME12\Domain Users OR HACKME12\Domain Computers

Policy settings:

Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

125 check if the New network policy is created correctly

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
- Templates Management

Network Policies

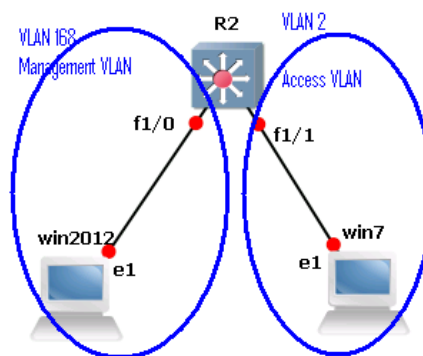
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Sour...
Secure Ethernet	Enabled	1	Grant Acce...	Uns...
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Uns...
Connections to other access servers	Enabled	999999	Deny Access	Uns...

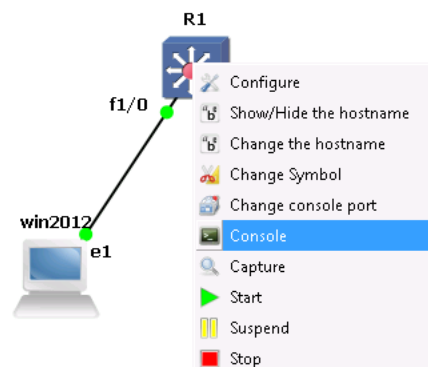
Configure the EtherSwitch router for 802.1x

Plan: We create two VLANs, the VLAN 168 for the server (it does not require 802.1x authentication, otherwise the switch were not able to contact to its RADIUS). And an access VLAN (VLAN 2), it will require 802.1x authentication, now only the win7 client will be in it. The switch will authenticate the client on the RADIUS server of the win 2012, first we accept MS-CHAPv2 later we change it to certificate based authentication. The RADIUS server will send the VLAN to the client after the authentication, where it will join (now VLAN 2). The IP addresses of the VLANs are:

- 192.168.168.0/24 in VLAN 168, the default gateway is the switch, with the IP 192.168.168.1 in this VLAN.
- 192.168.2.0/24 in VLAN 2, the default gateway is the switch with the IP 192.168.2.1 in this VLAN.



126 right click on the router, then select the console command from the popup menu



127 The switch is in exec (or admin) mode it can be seen from the # at the end of the prompt. If your switch is in user mode from any reason (it can be seen from the > at the end of the prompt) then type: enable then hit enter, to enter to the admin mode. To configure the switch use the configure terminal command.

```
R1
Connected to Dynamips VM "R1" (ID 0, type c3745) - Console port
Press ENTER to get the prompt.

R1#
R1#
R1#conf
R1#configure ter
R1#configure terminal
```

128 Create the two required VLANs (VLAN 2 and VLAN 168), and give them some name (it is not

mandatory to name them):

```
vlan 2
name Access
vlan 168
name Management
exit
```

```
R1
R1(config)#
R1(config)#vlan 2
R1(config-vlan)#name Access
R1(config-vlan)#vlan 168
R1(config-vlan)#name Management
R1(config-vlan)#exit
R1(config)#
R1(config)#
```

129 Add the port f1/0 to VLAN 168, and set it up as access port, similarly add port f1/1 to VLAN 2, and set it up as access port, then save the configuration. We set both ports to portfast mode, as one can read in the warning it is dangerous. This mode means, if the :

```
interface FastEthernet 1/0
switchport mode access
switchport access vlan 168
spanning-tree portfast
```

```
interface fastEthernet 1/1
switchport mode access
switchport access vlan 2
spanning-tree portfast
```

do write

```
R1
R1(config)#
R1(config)#interface FastEthernet 1/0
R1(config-if)#switchport mode access
R1(config-if)#switchport access vlan 168
R1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host.
Connecting hubs, concentrators, switches, bridges, etc. to this interface
when portfast is enabled, can cause temporary spanning tree loops.
Use with CAUTION

%Portfast has been configured on FastEthernet1/0 but will only
have effect when the interface is in a non-trunking mode.
R1(config-if)#do write
Building configuration...
[OK]
R1(config-if)#
R1(config-if)#interface fastEthernet 1/1
R1(config-if)#switchport mode access
R1(config-if)#switchport access vlan 2
R1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host.
Connecting hubs, concentrators, switches, bridges, etc. to this interface
when portfast is enabled, can cause temporary spanning tree loops.
Use with CAUTION

%Portfast has been configured on FastEthernet1/1 but will only
have effect when the interface is in a non-trunking mode.
R1(config-if)#do write
Building configuration...
[OK]
R1(config-if)#
*Mar 1 00:29:53.163: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
R1(config-if)#
```

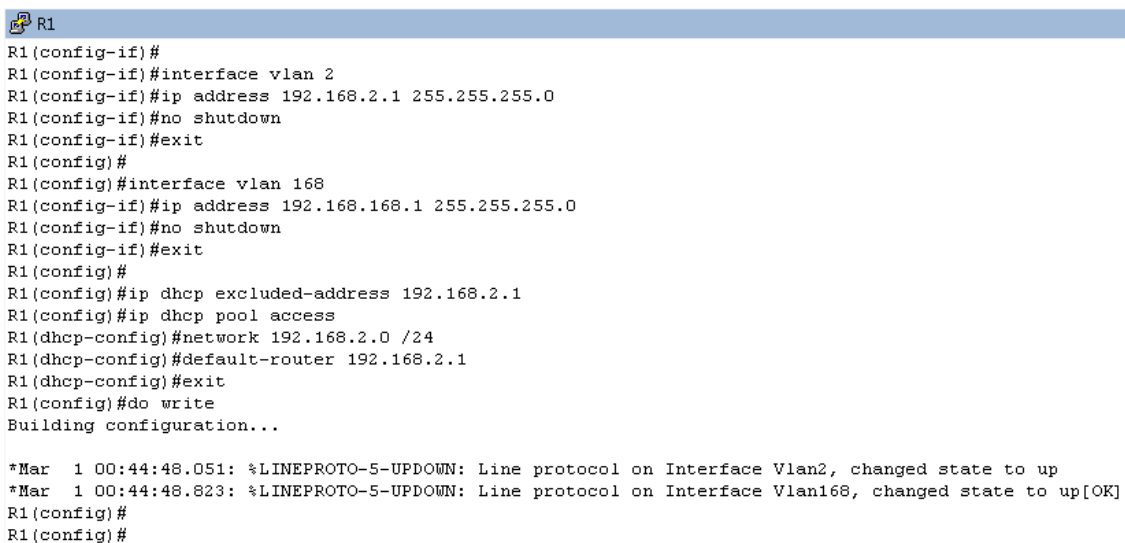
130 Define the IP address for both VLANs, then create a DHCP server on the switch, what will give IP address to the client machines in VLAN 2. Obviously exclude the IP address of the switch itself. Then save the configuration:

```
interface vlan 2
ip address 192.168.2.1 255.255.255.0
no shutdown
exit

interface vlan 168
ip address 192.168.168.1 255.255.255.0
no shutdown
exit

ip dhcp excluded-address 192.168.2.1
ip dhcp pool access
network 192.168.2.0 /24
default-router 192.168.2.1
dns-server 192.168.168.110
exit

do write
```



```
R1
R1(config-if)#
R1(config-if)#interface vlan 2
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#interface vlan 168
R1(config-if)#ip address 192.168.168.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#ip dhcp excluded-address 192.168.2.1
R1(config)#ip dhcp pool access
R1(dhcp-config)#network 192.168.2.0 /24
R1(dhcp-config)#default-router 192.168.2.1
R1(dhcp-config)#exit
R1(config)#do write
Building configuration...

*Mar  1 00:44:48.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
*Mar  1 00:44:48.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan168, changed state to up[OK]
R1(config)#
R1(config)#
```

131 And finally set up the 802.1x authentication.

Create a new authentication authorization audit (aaa) model, and set it up, to use radius authentication for 802.1x, and the RADIUS server is the windows 2012 server with IP address 192.168.168.110, the port is the usual 1812 UDP, and the radius shared secret is “cisco123”. Then enable the dot1x in general.

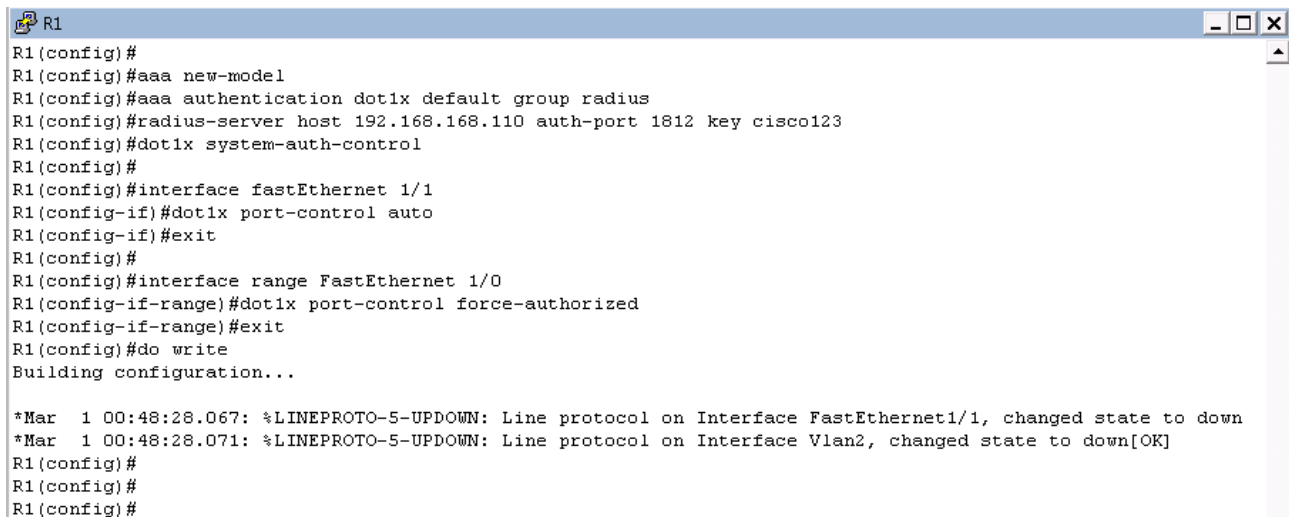
```
aaa new-model
aaa authentication dot1x default group radius
radius-server host 192.168.168.110 auth-port 1812 key cisco123
dot1x system-auth-control
```

Set up the f1/1 interface to require authentication (auto mode).

```
interface fastEthernet 1/1
dot1x port-control auto
exit
```

set up the port f1/0 to do not require authentication (force-authorized)

```
interface FastEthernet 1/0
dot1x port-control force-authorized
exit
do write
```

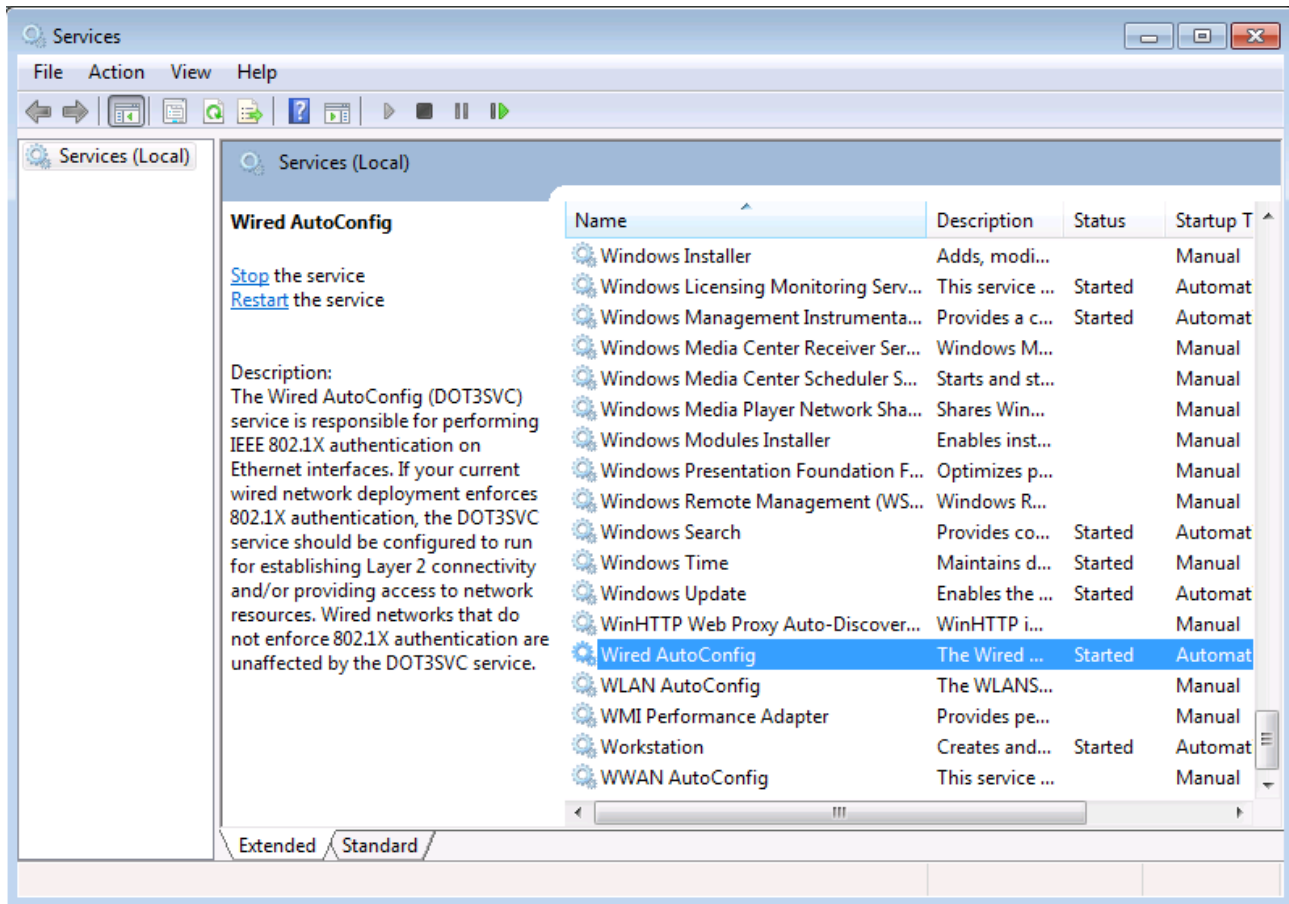


```
R1
R1(config)#
R1(config)#aaa new-model
R1(config)#aaa authentication dot1x default group radius
R1(config)#radius-server host 192.168.168.110 auth-port 1812 key cisco123
R1(config)#dot1x system-auth-control
R1(config)#
R1(config)#interface fastEthernet 1/1
R1(config-if)#dot1x port-control auto
R1(config-if)#exit
R1(config)#
R1(config)#interface range FastEthernet 1/0
R1(config-if-range)#dot1x port-control force-authorized
R1(config-if-range)#exit
R1(config)#do write
Building configuration...

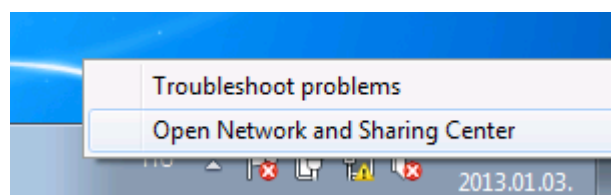
*Mar  1 00:48:28.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to down
*Mar  1 00:48:28.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down[OK]
R1(config)#
R1(config)#
R1(config)#
```

Test the 802.1x authentication on the client

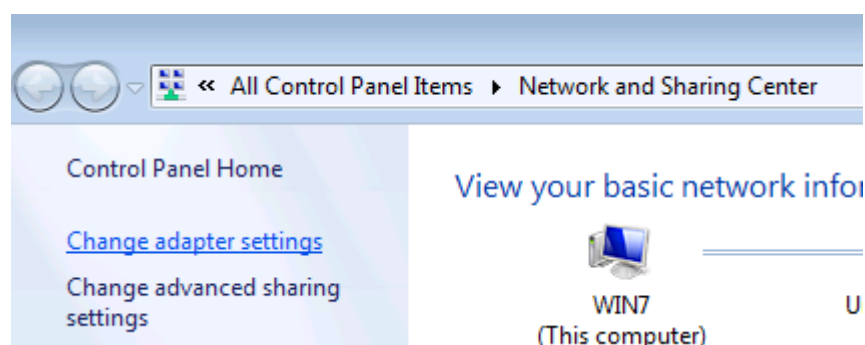
132 go to the Administrative tools / services, and if it is not started start the “Wired AutoConfig” service. I also recommend, to set it automatic.



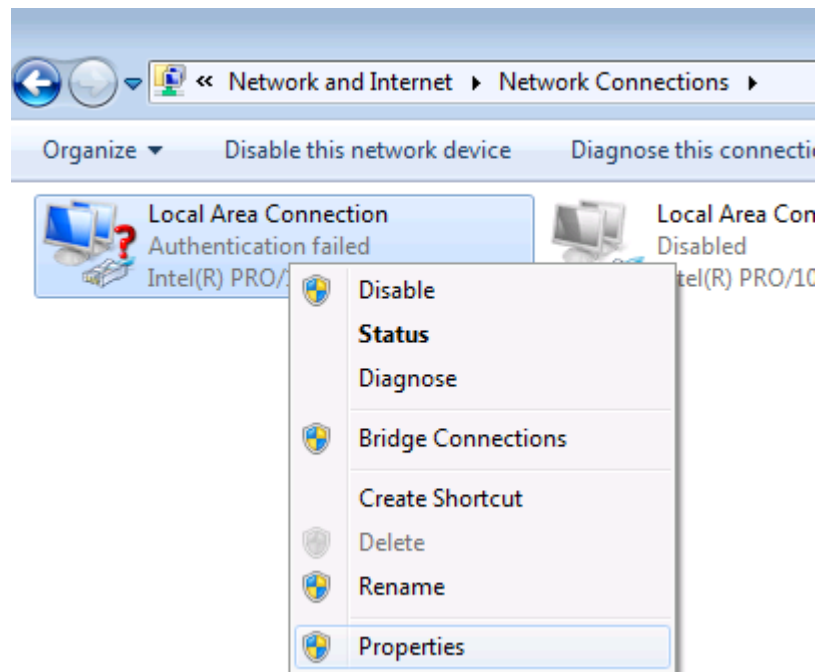
133 Log on to the windows 7 machine and open the network sharing center



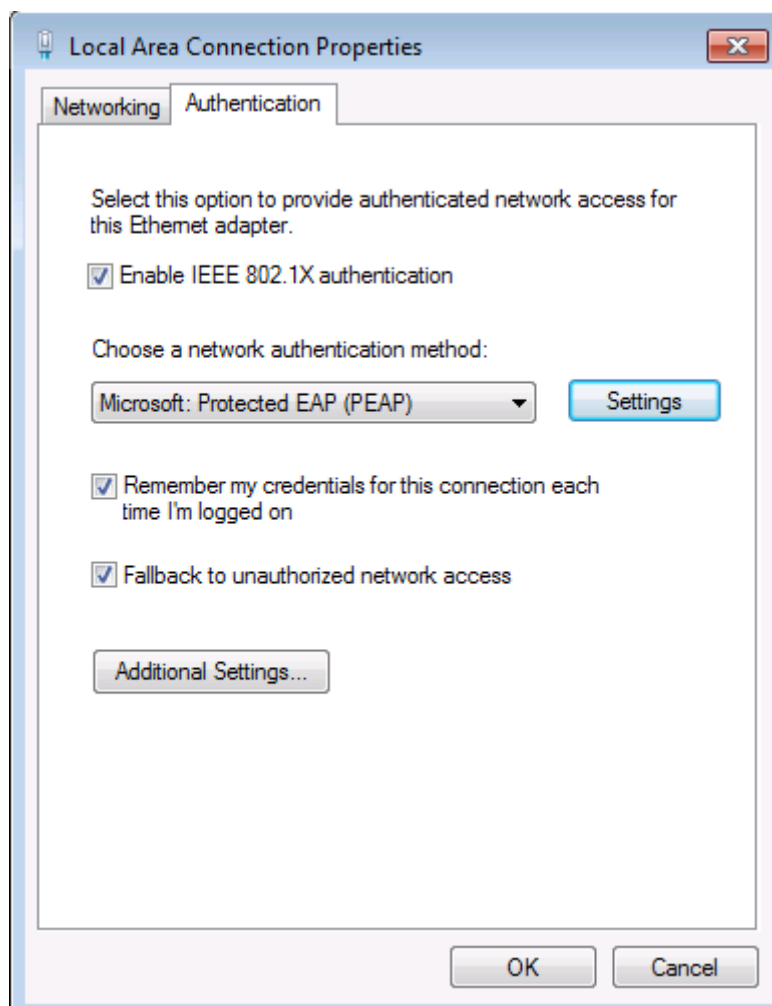
134 click to the “Change adapter settings”



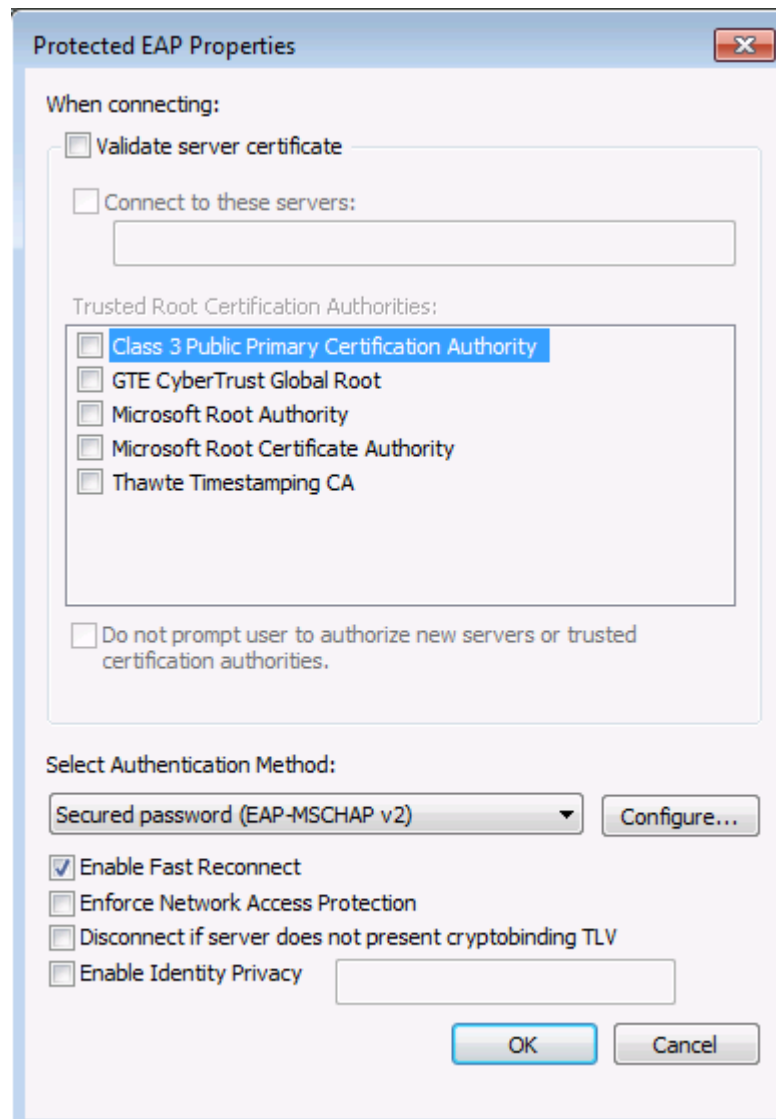
135 You can see a from the question mark the authentication is working, but you were not able to authenticate yet. Right click to the Local Area Connection, and select the Properties from the popup menu



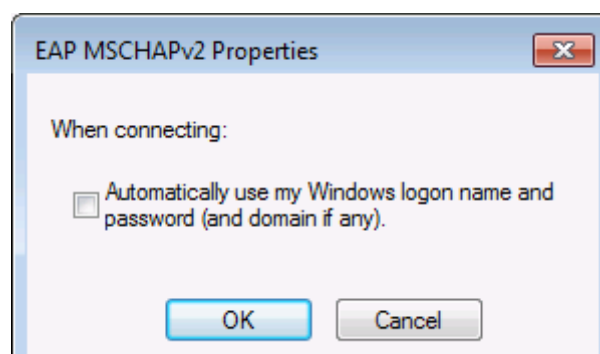
136 Go to the Authentication tab (if you do not see this tab start the “Wired AutoConfig” service, then reopen this properties window), and click to the Settings button



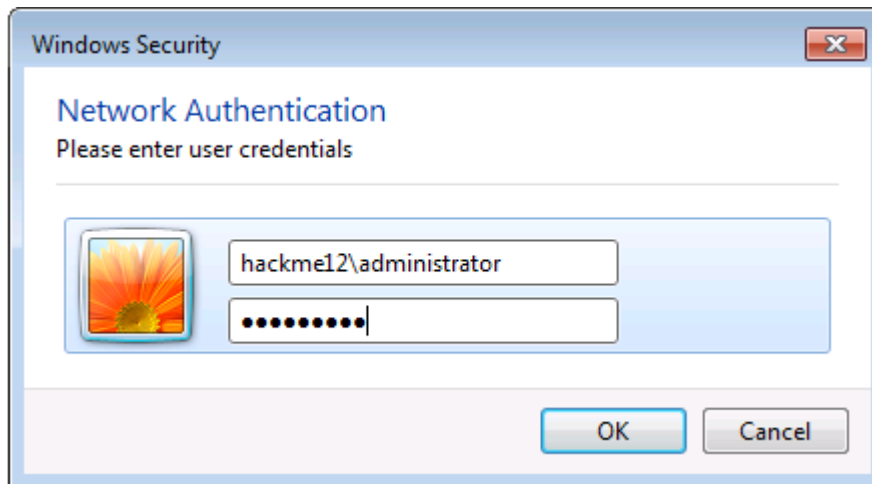
137 clear the checkmark from the “Validate Server Certificate” checkbox (first we test it with these settings, later we put it back). Then click to the Configure button next to the “Secure Password EAP-MSCHAPv2”



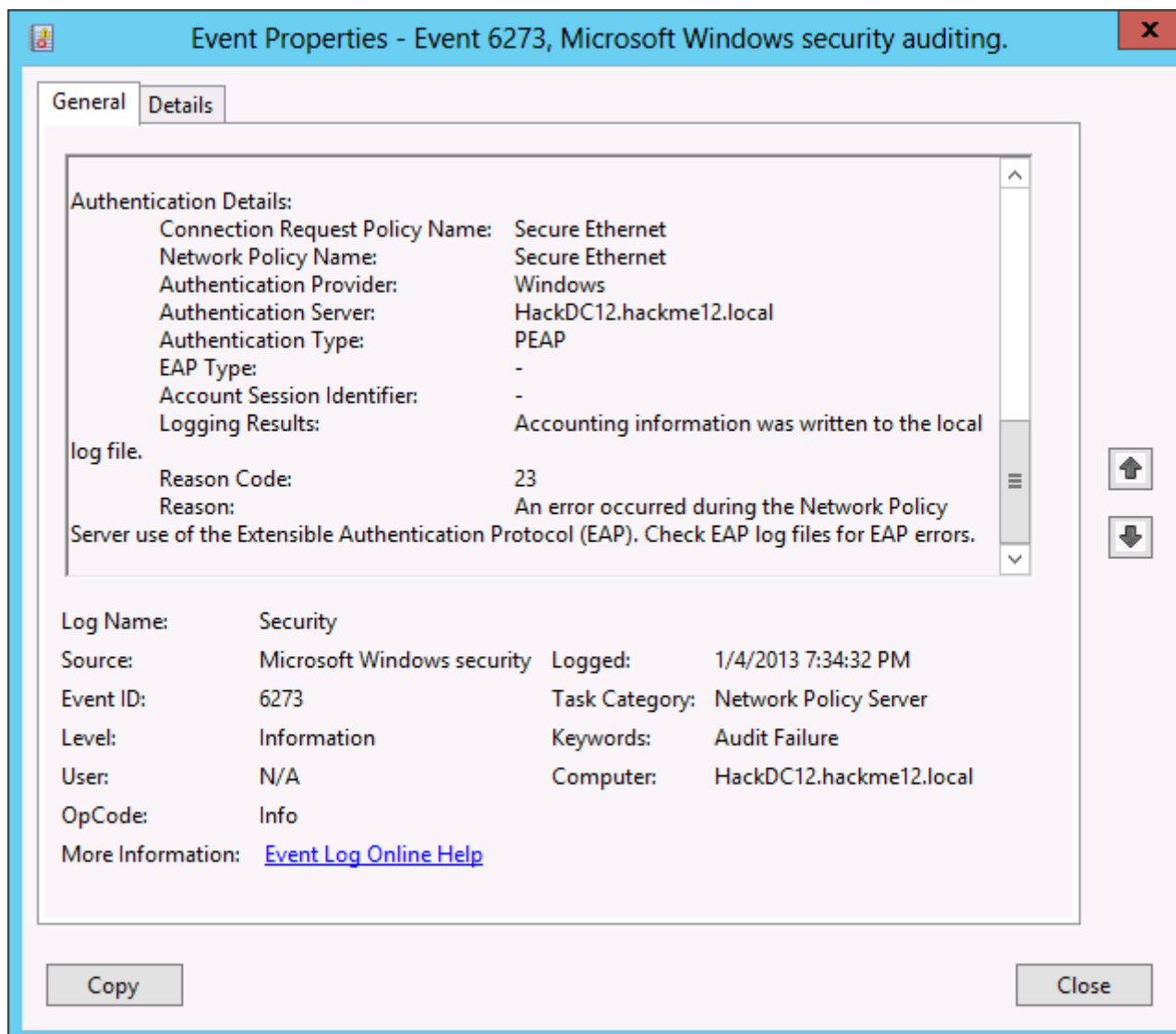
138 Clear the checkmark before the “Automatically use my Windows logon name and password (and domain if any)” (again we do it to see the steps of the authentication cleaner, later we will put it back). Then click OK on the all the network settings windows.

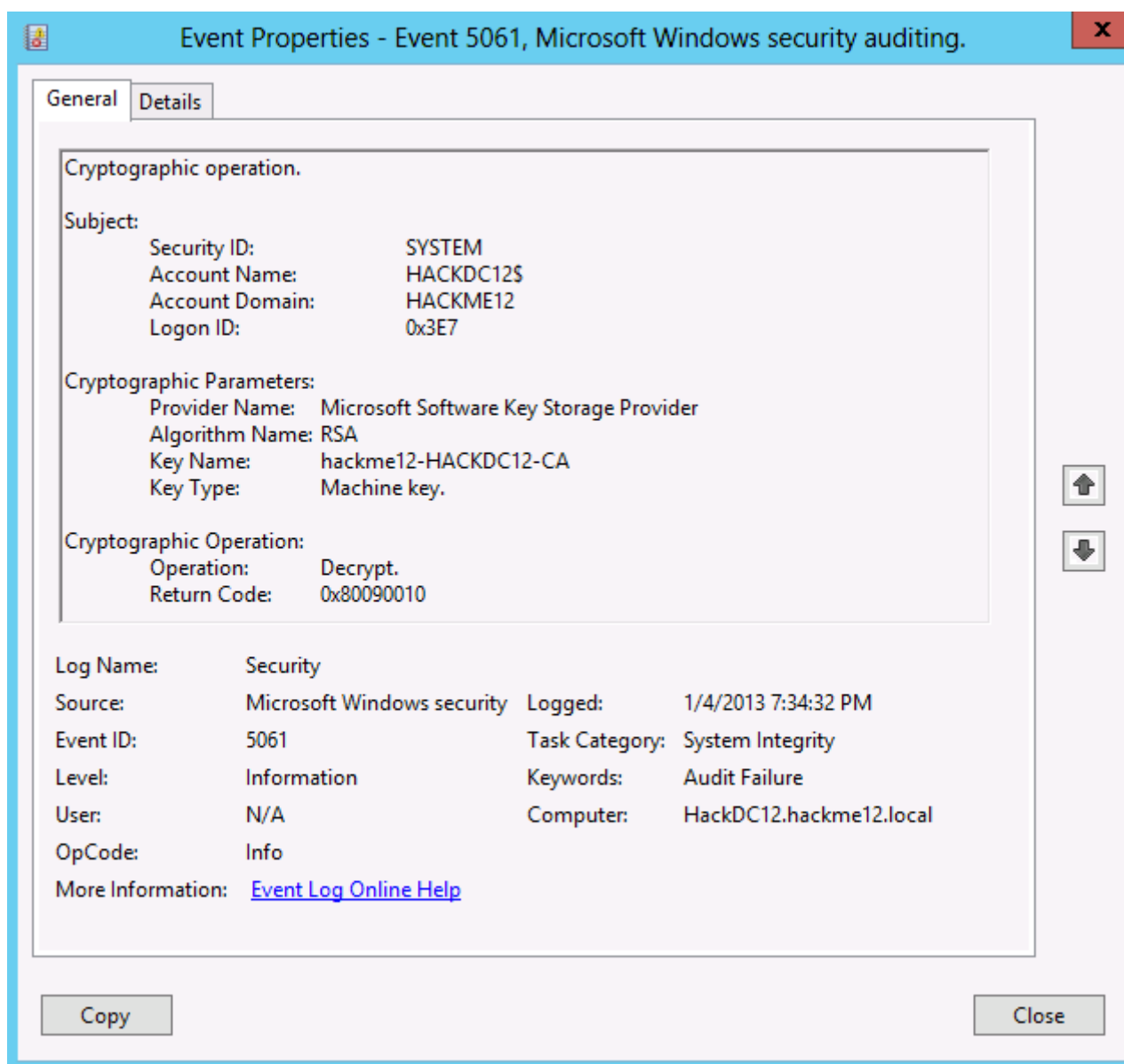


139 Because previously we cleared the checkmark the computer asks for a username and password. Type it, and click to the OK button.

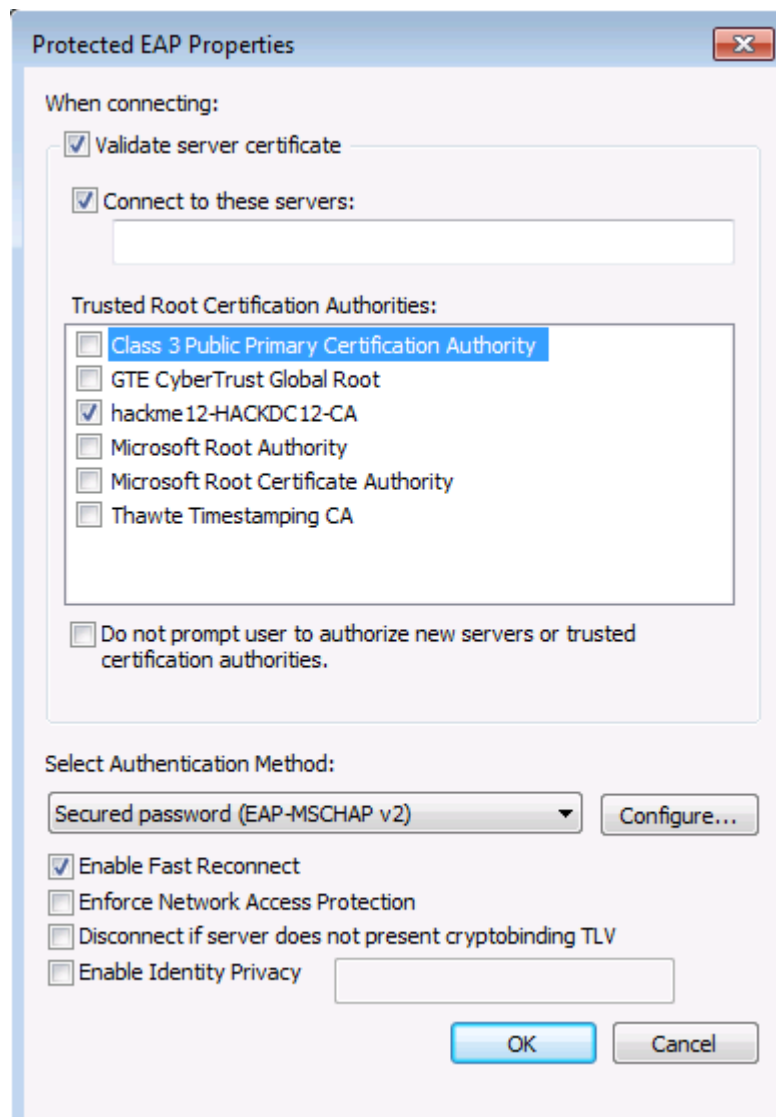


140 Hopefully the authentication will be successful, you can see it from the disappearing question mark. If the authentication is not successful and you get error messages like the following ones on the server, then most probably the certificate on your RADIUS server is not the correct one:

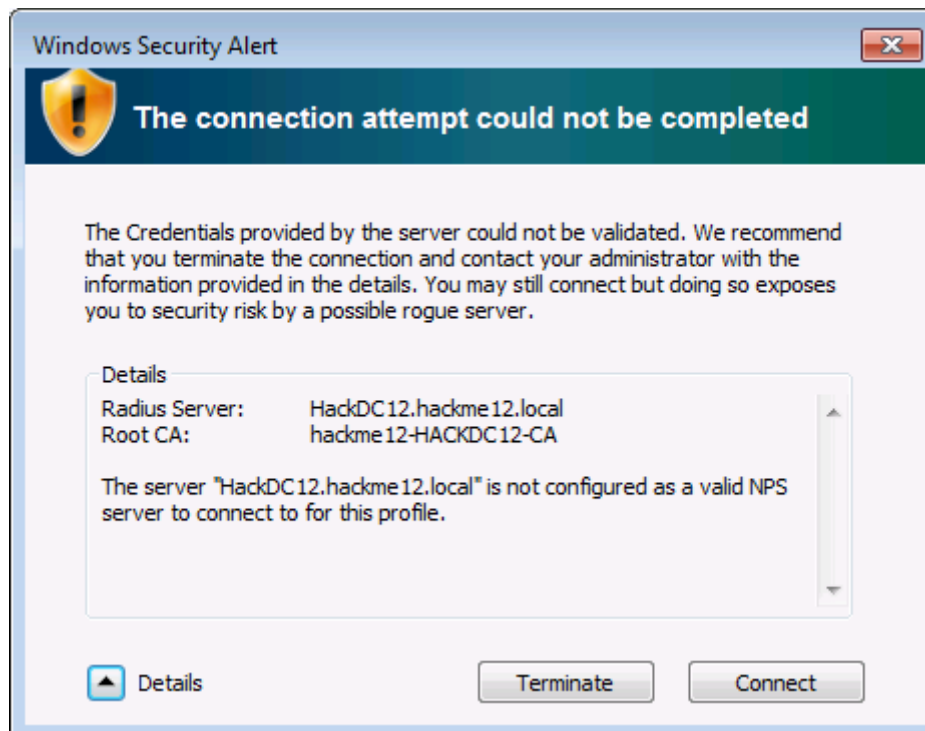




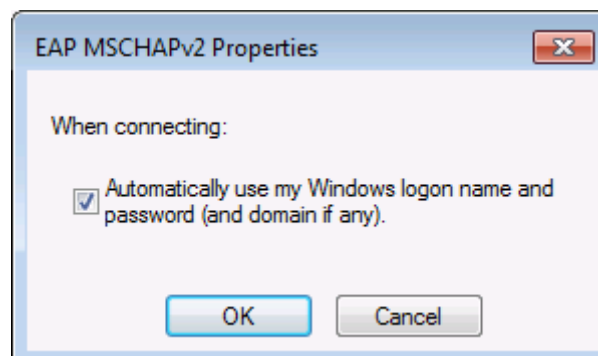
140 If the authentication was working we can put back the check mark before the “Validate Server Certificate”, and select out Certificate server as “Trusted Root Certification Authorities”, then click OK on all the Network settings windows.



141 Now you will get a warning about the certificates, and you should accept the certificate of the RADIUS server by clicking to the connect button:



142 Then put back the checkmark before the “Automatically use my Windows logon name and password (and domain if any)”, and click OK on every network configuration windows.

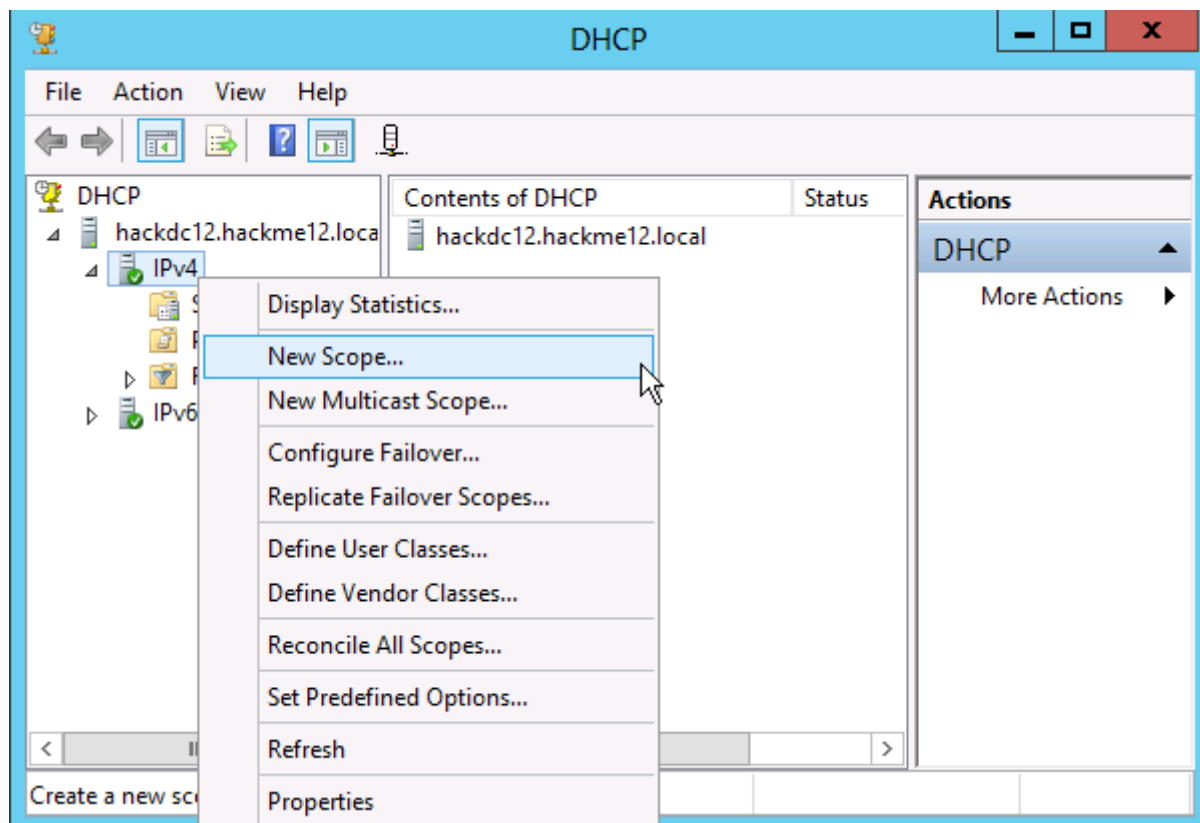


143 Disable and Enable the network card, to see if the computer authenticates automatically with your username and password.

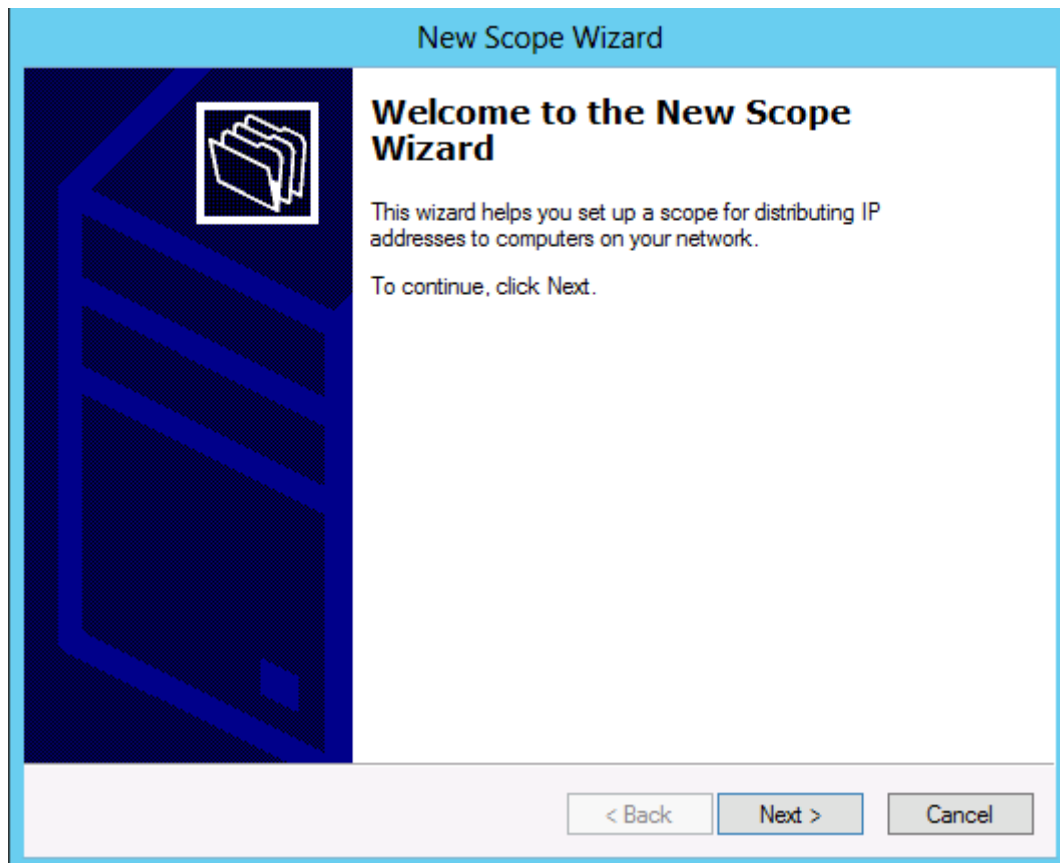
NAP with DHCP enforce

Set up DHCP server on the windows 2012 machine

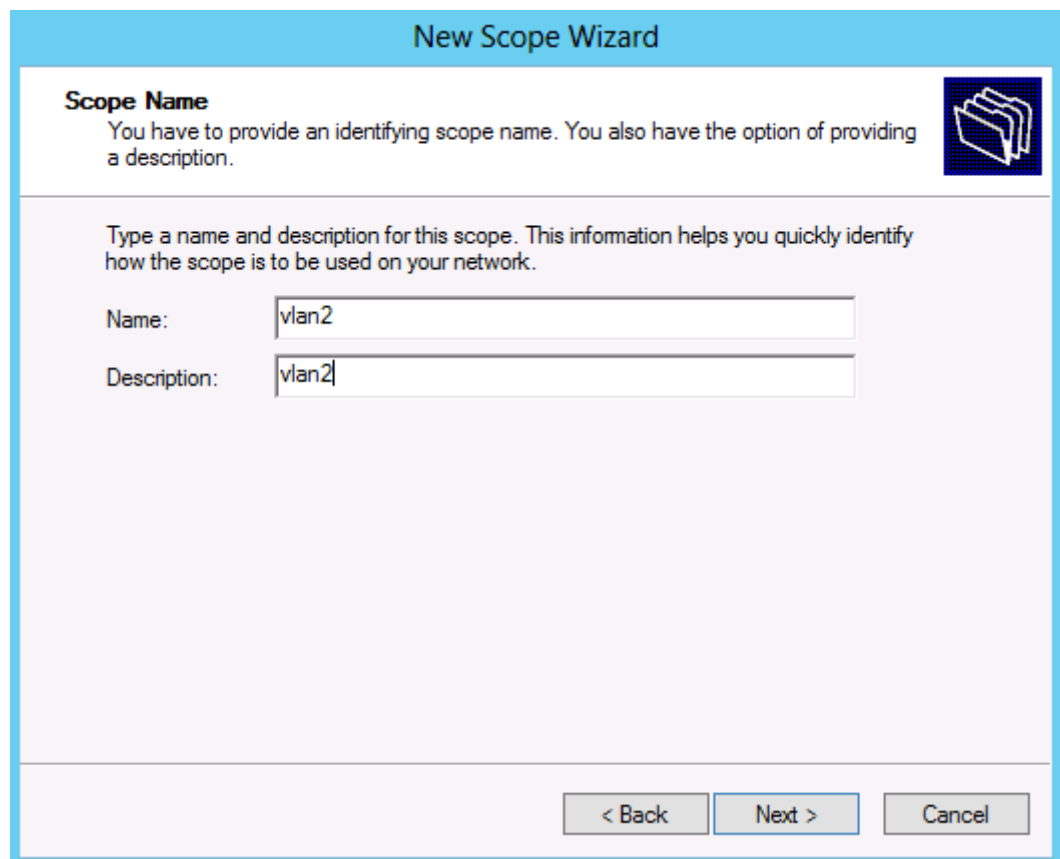
144 create a new IP4 scope, by click to the IPv4 and select the “New Scope...” from the popup menu.



145 click to the next button on the welcome page of the wizard.

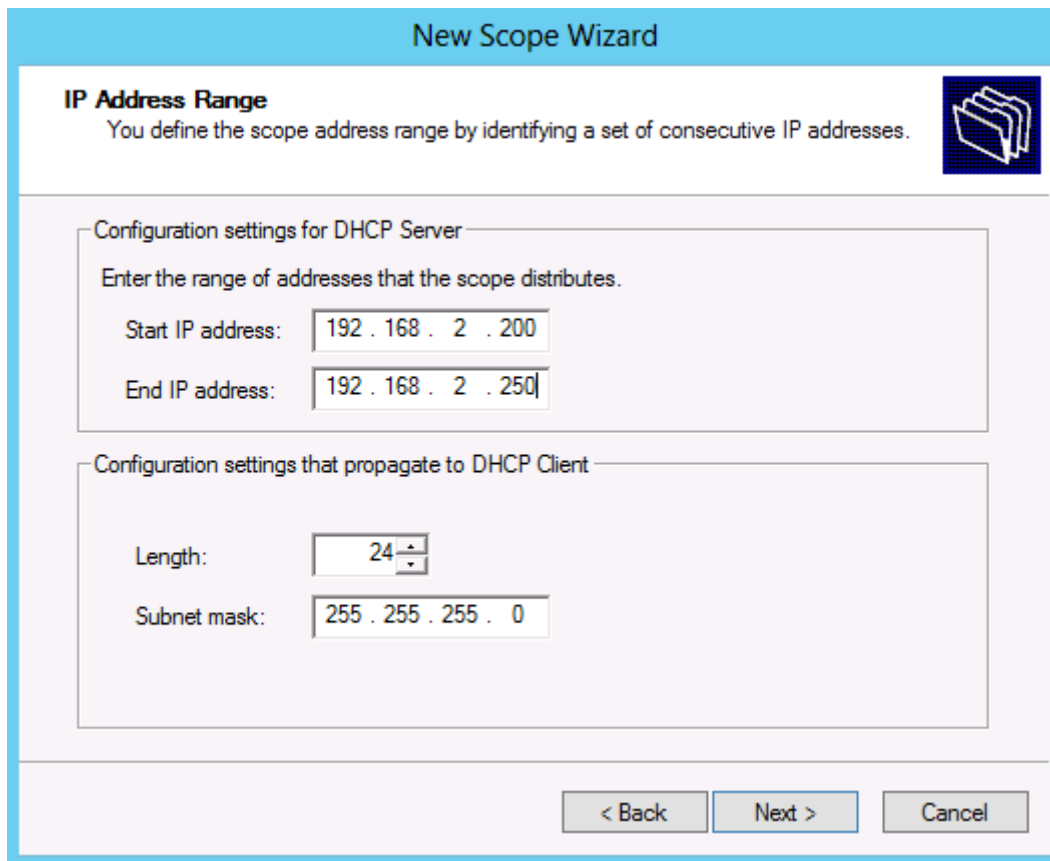


146 We will use this scope to give IP address to the computers in VLAN 2 so I give it a name vlan2, but of course it can be anything.



The image shows the 'New Scope Wizard' window at the 'Scope Name' step. The title bar is light blue and contains the text 'New Scope Wizard'. The main area has a light blue background. On the left, there is a dark blue vertical bar with a white icon of a folder. To the right of the bar, the text 'Scope Name' is displayed in bold. Below this, a paragraph states: 'You have to provide an identifying scope name. You also have the option of providing a description.' Below this, there is a text box for 'Name' containing the text 'vlan2' and a text box for 'Description' containing the text 'vlan2'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

147 set up a scope range, I used the range 192.168.2.200..250.



The image shows a Windows XP-style dialog box titled "New Scope Wizard". The main heading is "IP Address Range" in bold. Below it, a subtitle reads: "You define the scope address range by identifying a set of consecutive IP addresses." To the right of the subtitle is a small icon of a folder with a document. The dialog is divided into two main sections by a horizontal line. The top section is titled "Configuration settings for DHCP Server" and contains the instruction "Enter the range of addresses that the scope distributes." Below this instruction are two input fields: "Start IP address:" with the value "192 . 168 . 2 . 200" and "End IP address:" with the value "192 . 168 . 2 . 250". The bottom section is titled "Configuration settings that propagate to DHCP Client" and contains two input fields: "Length:" with a value of "24" and a small up/down arrow, and "Subnet mask:" with the value "255 . 255 . 255 . 0". At the bottom right of the dialog are three buttons: "< Back", "Next >", and "Cancel".

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 2 . 200

End IP address: 192 . 168 . 2 . 250

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

148. If you want to define exclusion, set them up, I do not need any

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

Subnet delay in milli second:

< Back
Next >
Cancel

149 For lease duration I used the default value. It is only a test environment, so it can be anything.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:

Hours:

Minutes:

< Back
Next >
Cancel

150 Configure the DHCP options

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

151 Add the IP address of the switch (192.168.2.1) as default router

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

. . .
192.168.2.1

152 set up the DNS information. Now the DNS server is our windows 2012 machine

192.168.168.110.

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text" value="192.168.168.110"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>		<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

< Back Next > Cancel

153 Set up WINS server if required, I do not need it now so click to next

New Scope Wizard

WINS Servers

Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

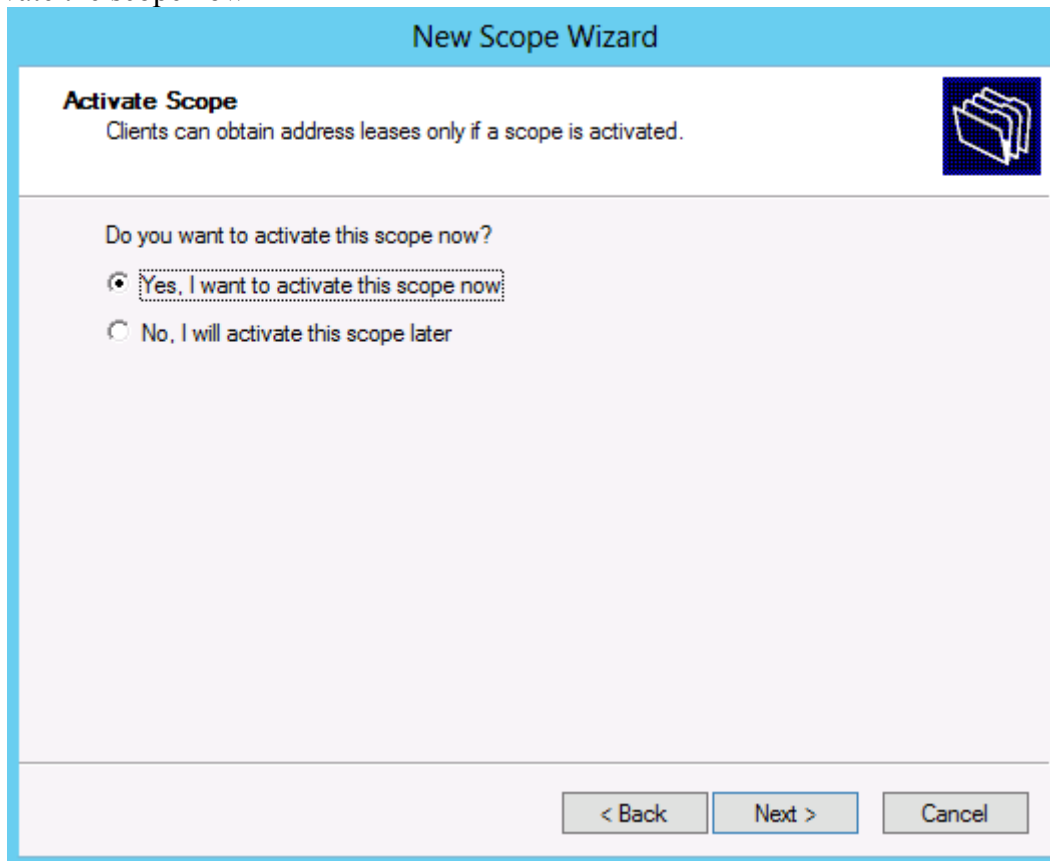
Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:	IP address:	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>		<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

< Back Next > Cancel

154 Activate the scope now



New Scope Wizard

Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

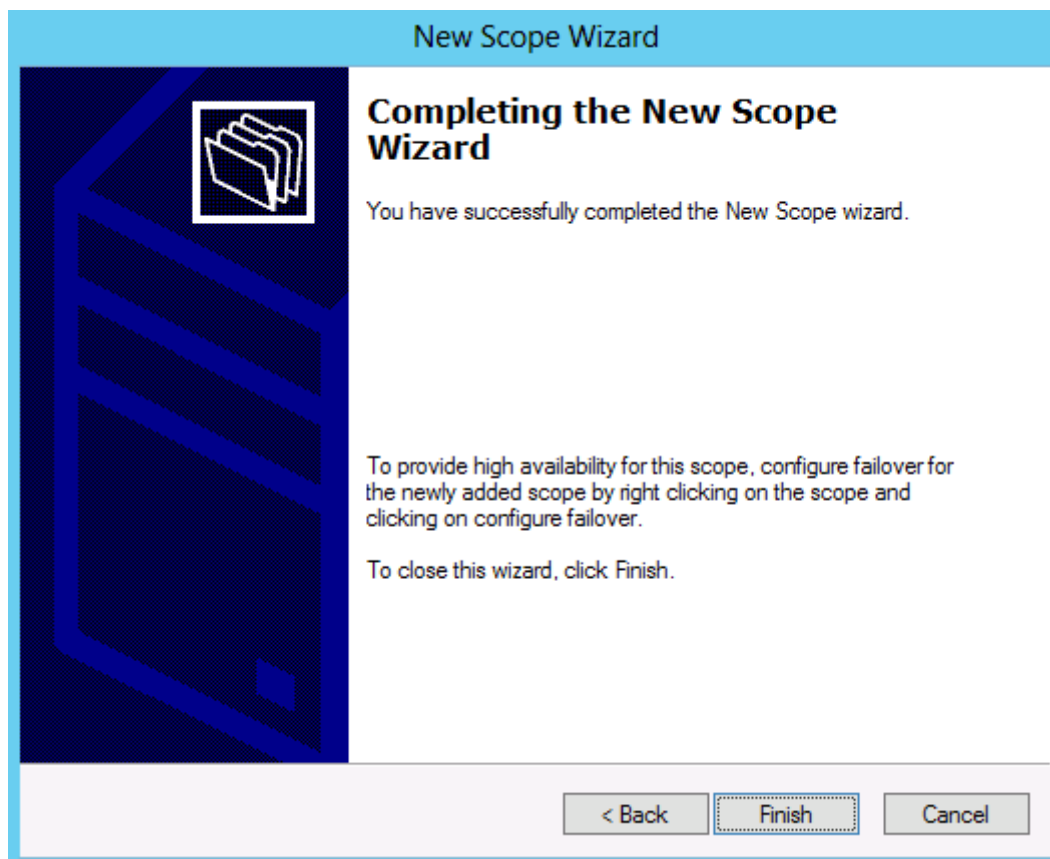
☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

< Back Next > Cancel

This screenshot shows the 'Activate Scope' step of the 'New Scope Wizard'. The window has a light blue title bar and a white background. At the top, the title 'New Scope Wizard' is centered. Below it, the section 'Activate Scope' is followed by the text 'Clients can obtain address leases only if a scope is activated.' To the right of this text is a small icon of a folder with a document. The main area contains a question 'Do you want to activate this scope now?' with two radio button options: 'Yes, I want to activate this scope now' (which is selected) and 'No, I will activate this scope later'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

155 click finish button



New Scope Wizard

Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

To close this wizard, click Finish.

< Back Finish Cancel

This screenshot shows the 'Completing the New Scope Wizard' step. The window has a light blue title bar and a white background. On the left side, there is a large blue graphic of a server rack. The main area contains the title 'Completing the New Scope Wizard' followed by the text 'You have successfully completed the New Scope wizard.' Below this, there are two paragraphs of instructions: 'To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.' and 'To close this wizard, click Finish.' At the bottom, there are three buttons: '< Back', 'Finish' (which is highlighted with a dotted border), and 'Cancel'.


Set up the DHCP relay on the switch

156 We should delete the previously created pool, and instead it set up the switch on VLAN2 as DHCP relay agent. To do it use the following commands:

```
no ip dhcp pool access
```

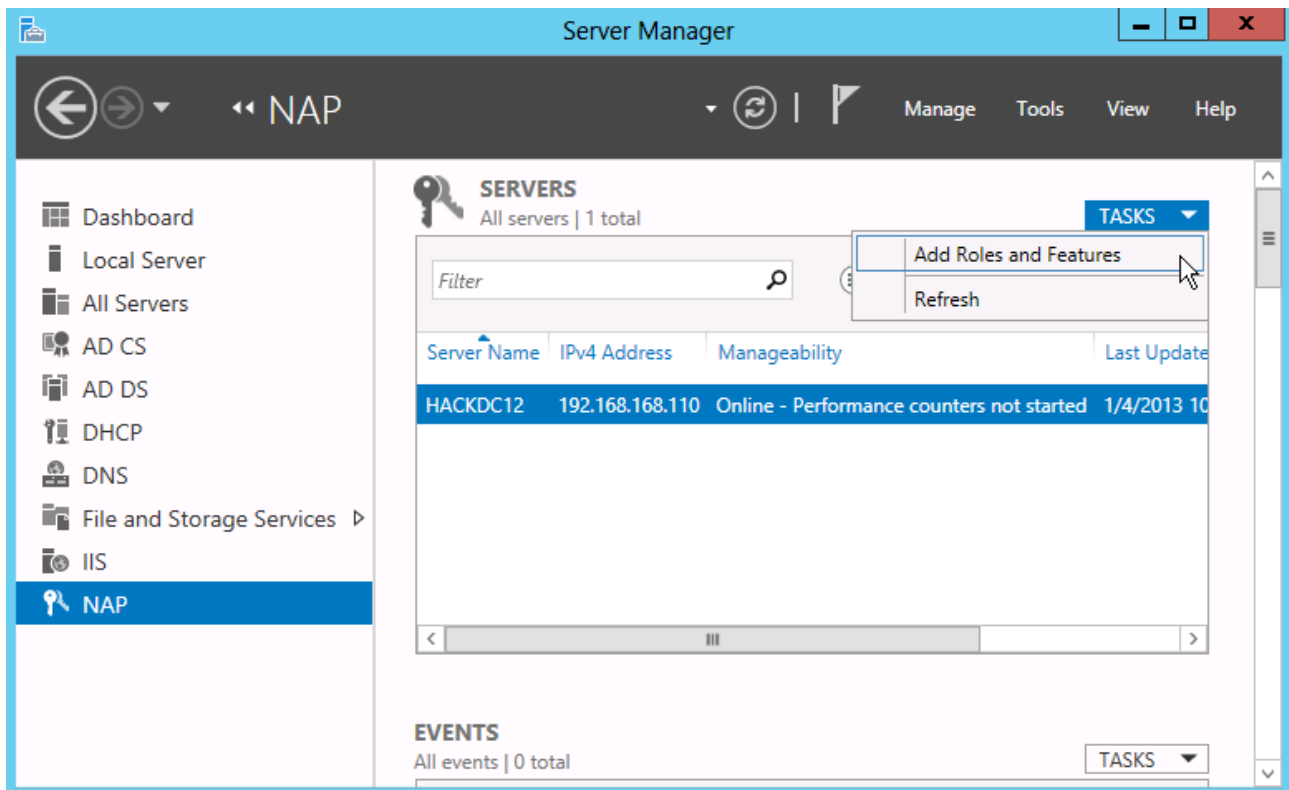
Enter to the context of VLAN 2, then set up the Relay agent

```
interface vlan 2
ip helper-address 192.168.168.110
no autostate
do write
```

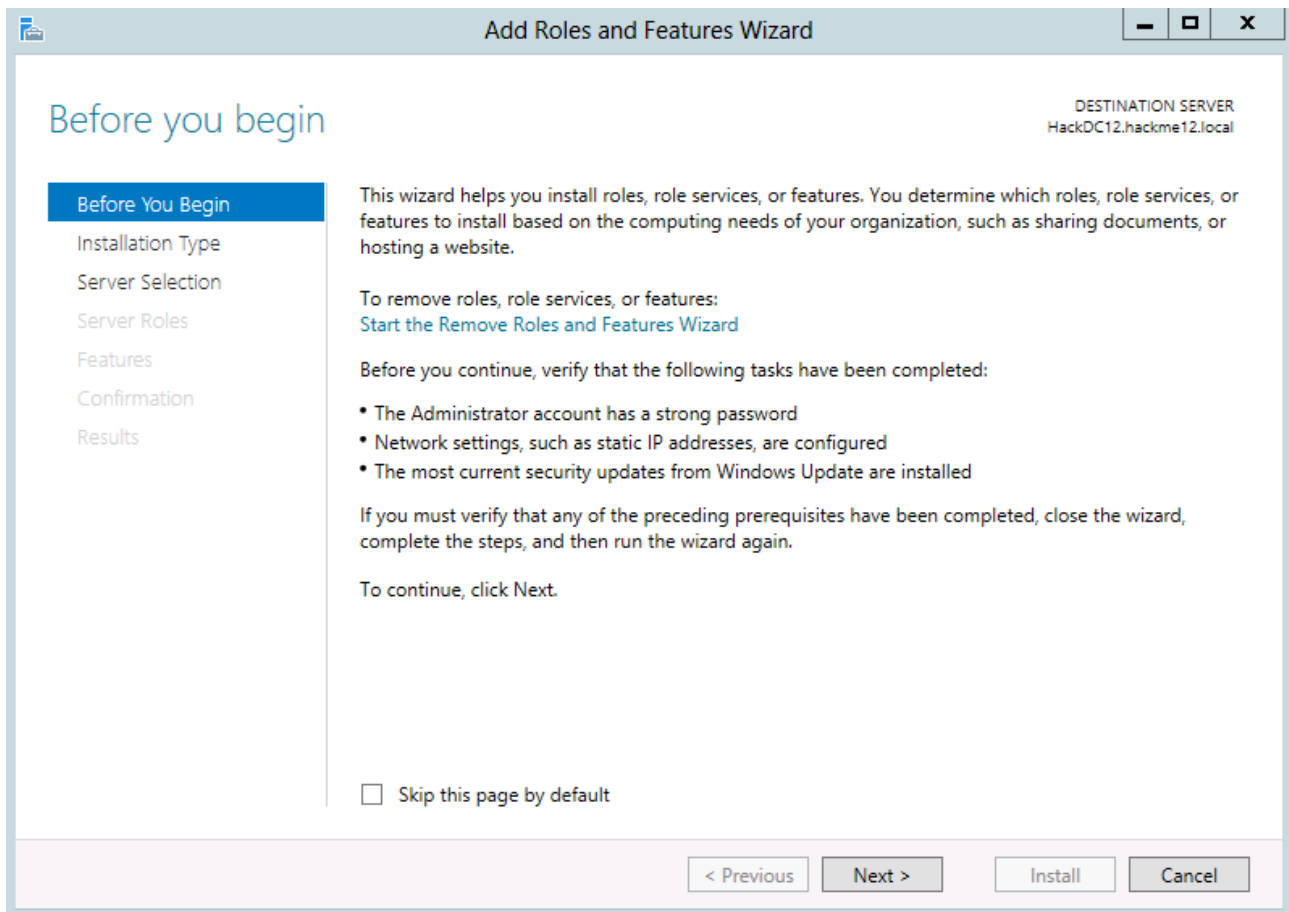
 R1
myswitch(config)#
myswitch(config)#no ip dhcp pool access
myswitch(config)#interface vlan 2
myswitch(config-if)#ip helper-address 192.168.168.110
myswitch(config-if)#do write
Building configuration...
[OK]
myswitch(config-if)#
myswitch(config-if)#

Add the “Health roles” to the already installed NAP Service

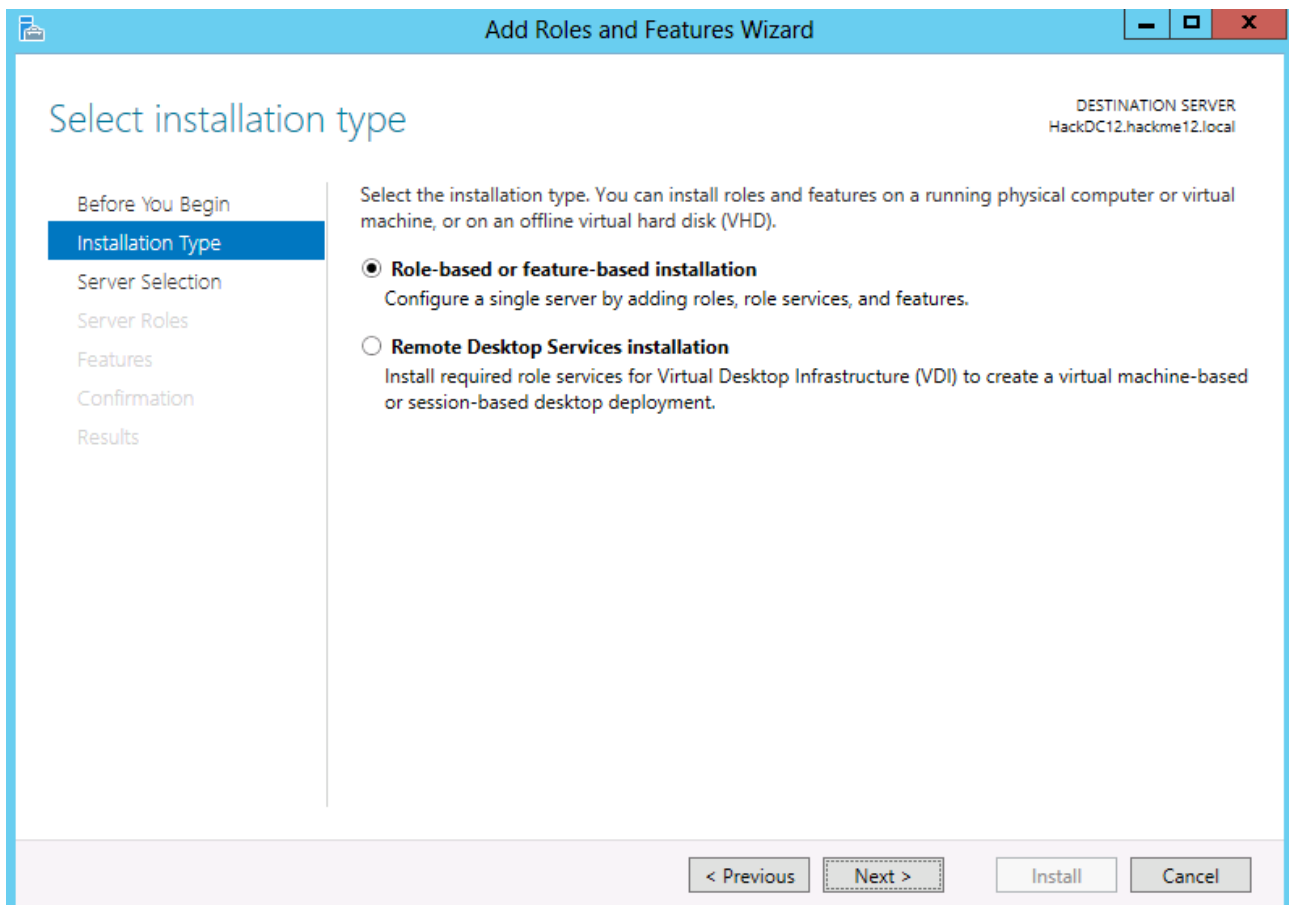
157 Select the NAP service, and from the TASKS combo box select the “Add Roles and Features” commands



158 Click next on the welcome screen



159 Select the “Role-based or feature-based installation” then click to next



160 Select the local server from the pool

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar is blue with the text 'Add Roles and Features Wizard' and standard window controls. The main content area has a light blue header with the text 'Select destination server'. On the right side of the header, it says 'DESTINATION SERVER HackDC12.hackme12.local'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted in blue), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the following text: 'Select a server or a virtual hard disk on which to install roles and features.' Below this are two radio buttons: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Below the radio buttons is a section titled 'Server Pool'. It contains a 'Filter:' text box. Below the filter is a table with three columns: 'Name', 'IP Address', and 'Operating System'. The table has one row with the following data: 'HackDC12.hackme12.local', '192.168.168.110', and 'Microsoft Windows Server 2012 Datacenter'. Below the table, it says '1 Computer(s) found'. At the bottom of the main area, there is a paragraph: 'This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

DESTINATION SERVER
HackDC12.hackme12.local

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

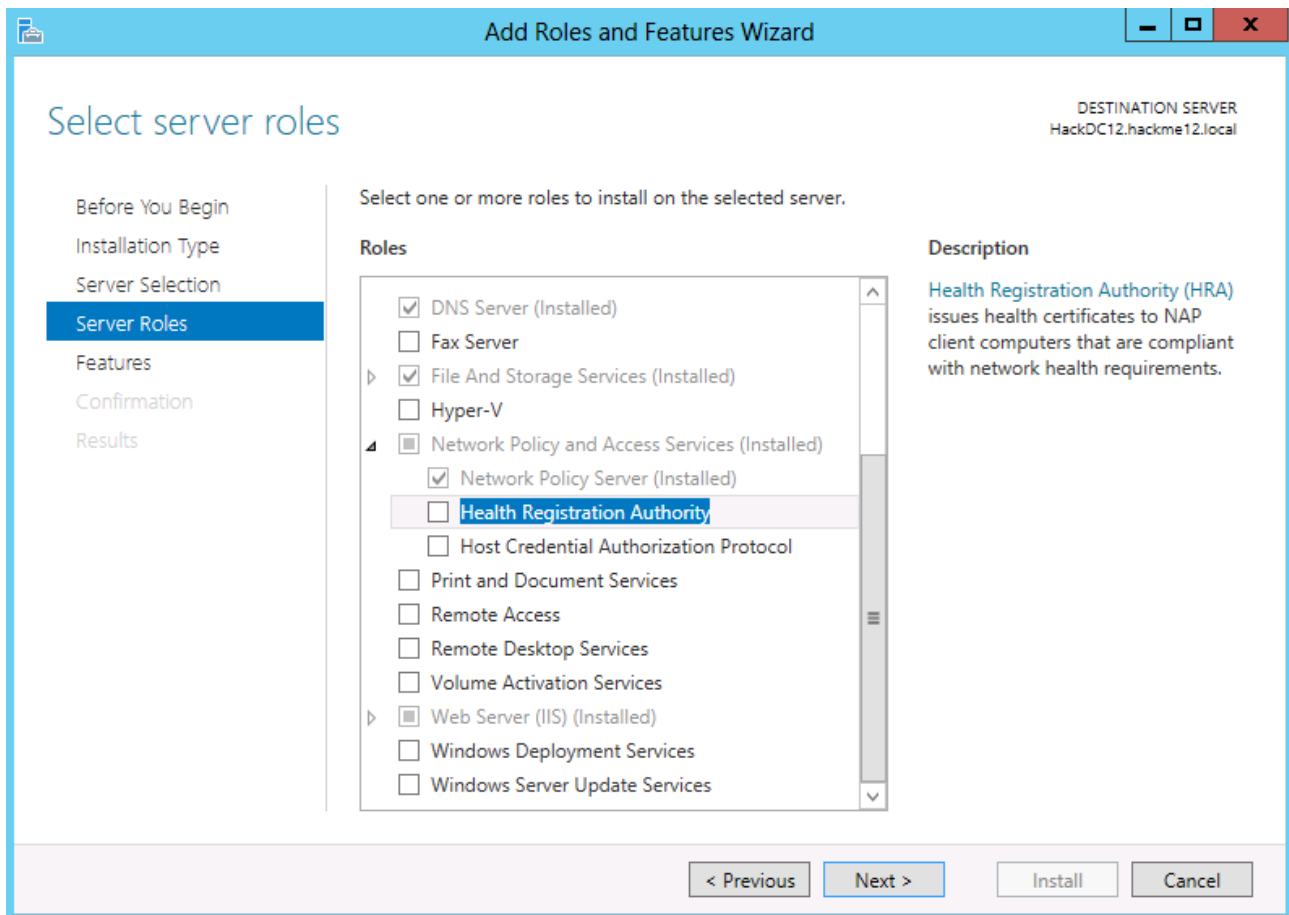
Name	IP Address	Operating System
HackDC12.hackme12.local	192.168.168.110	Microsoft Windows Server 2012 Datacenter

1 Computer(s) found

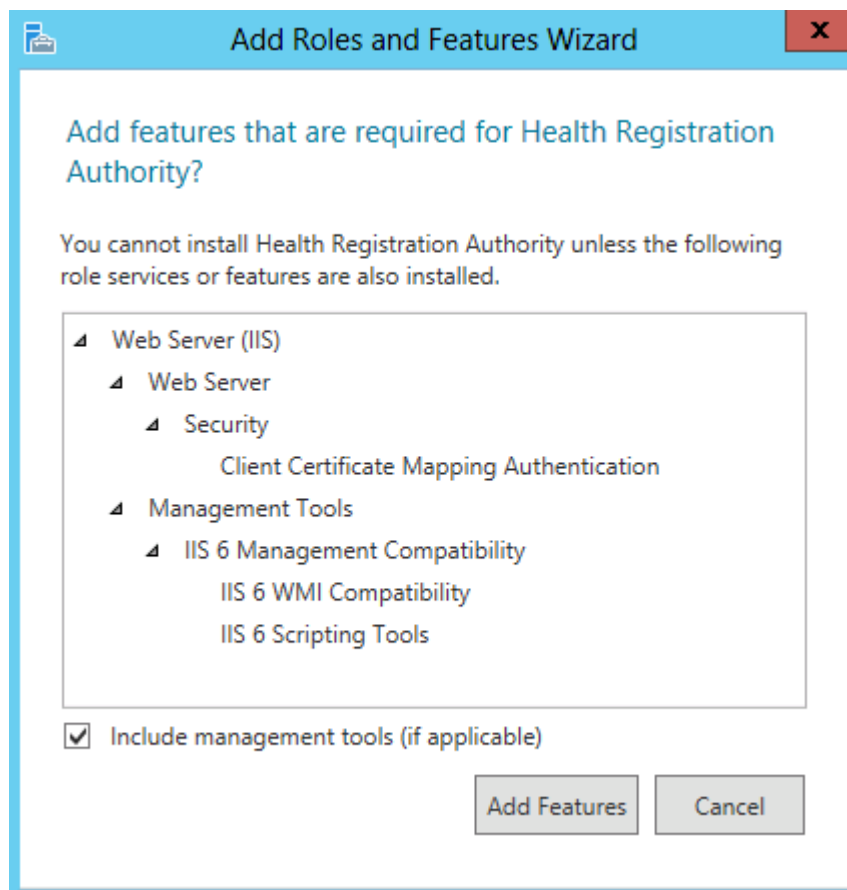
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous Next > Install Cancel

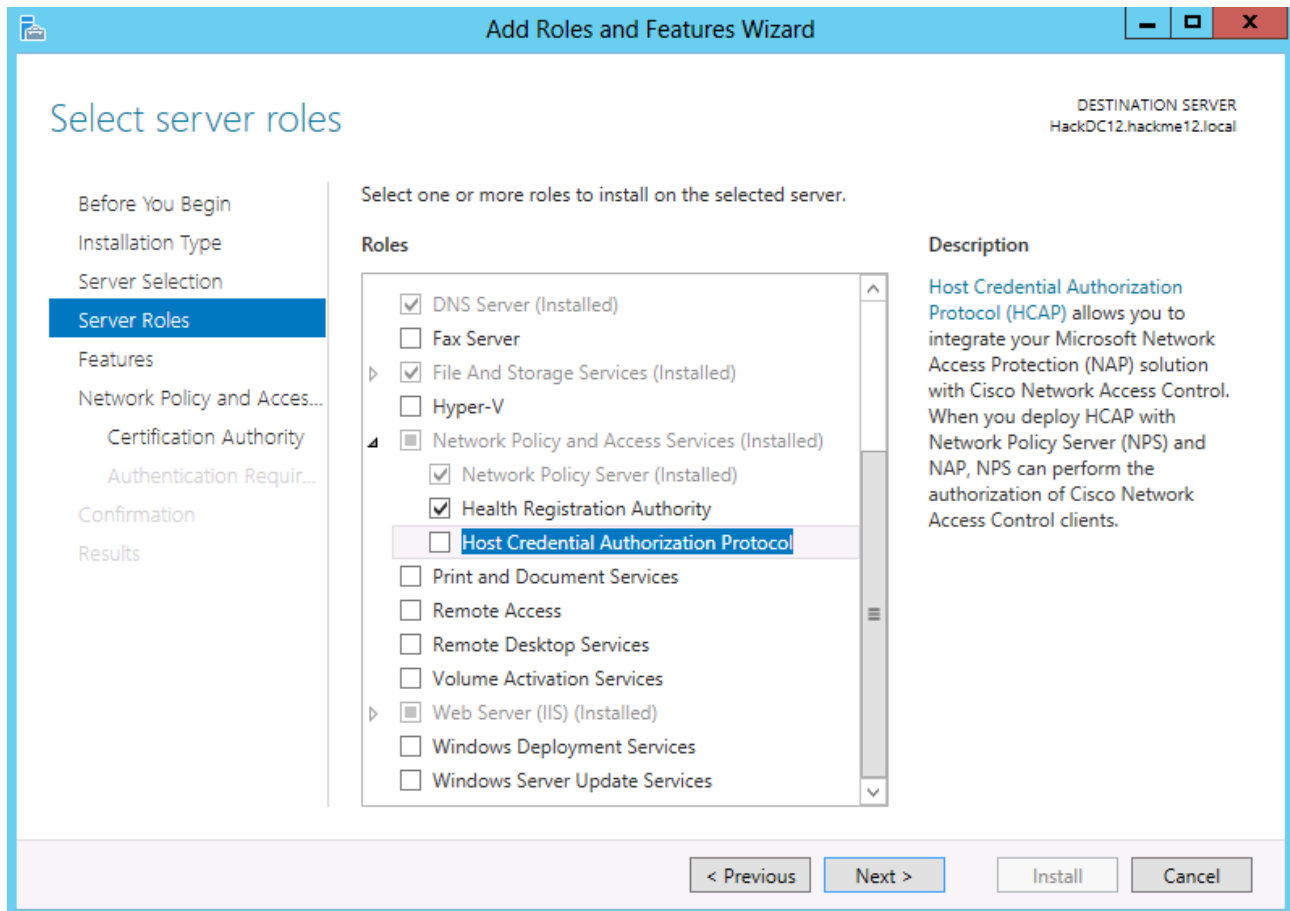
161 Check the “Health registration Authority”



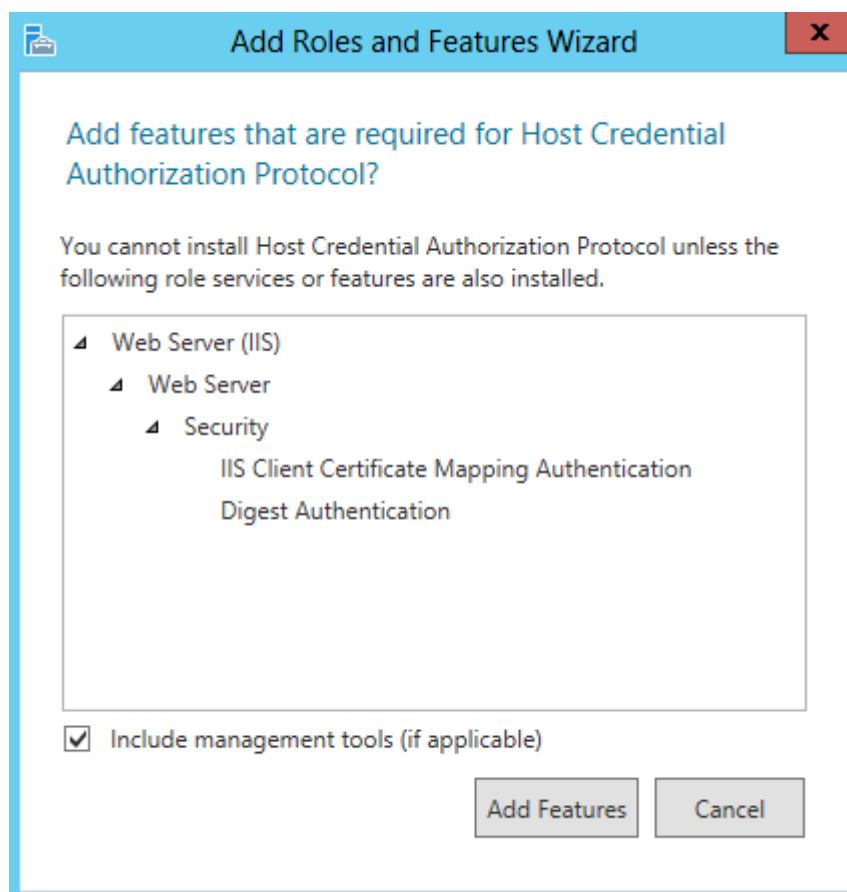
162 The computer states you should install some features as well. Just accept the recommendations by clicking the “Add Features” button.



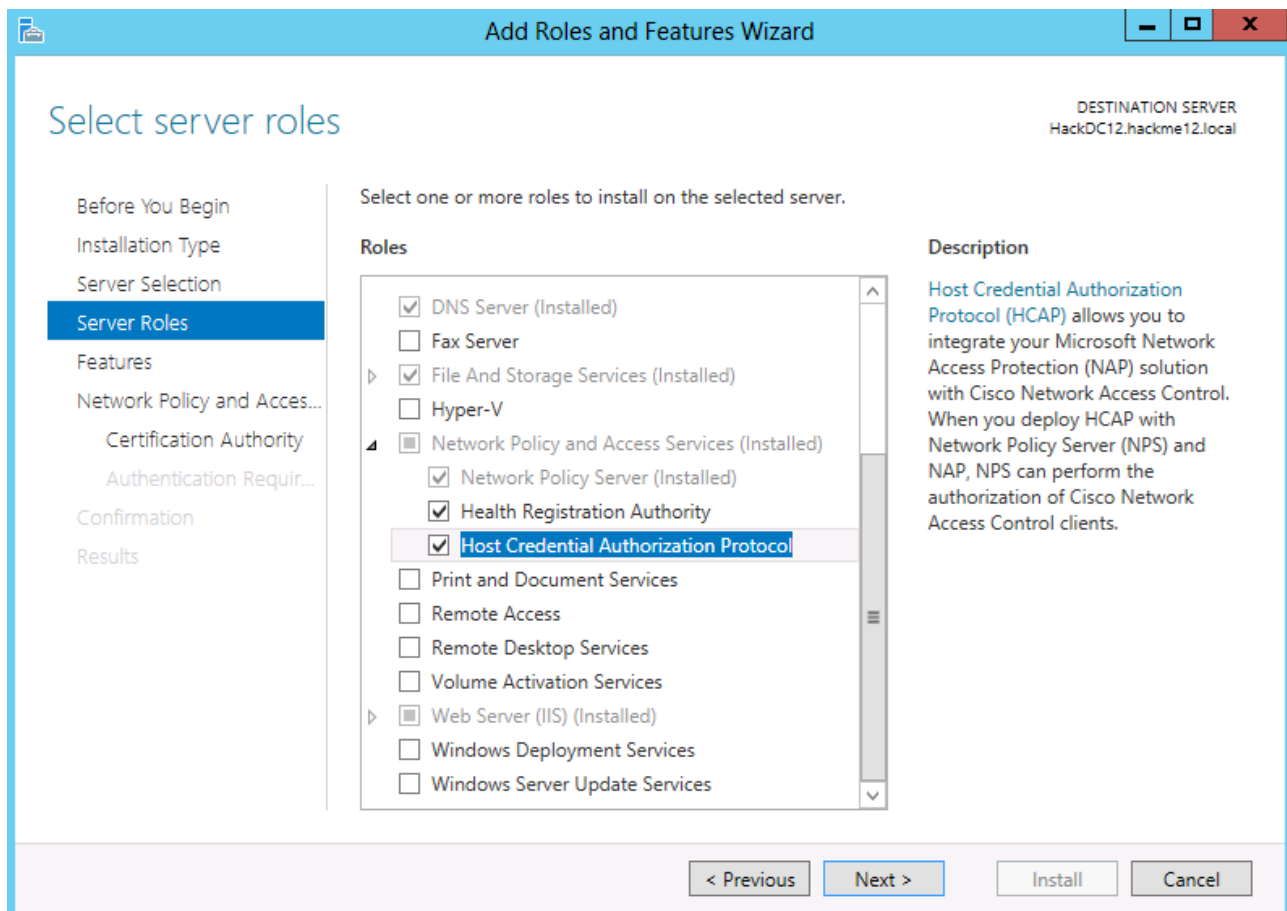
163 Put a check before the “Host Credential Authorization Protocol”



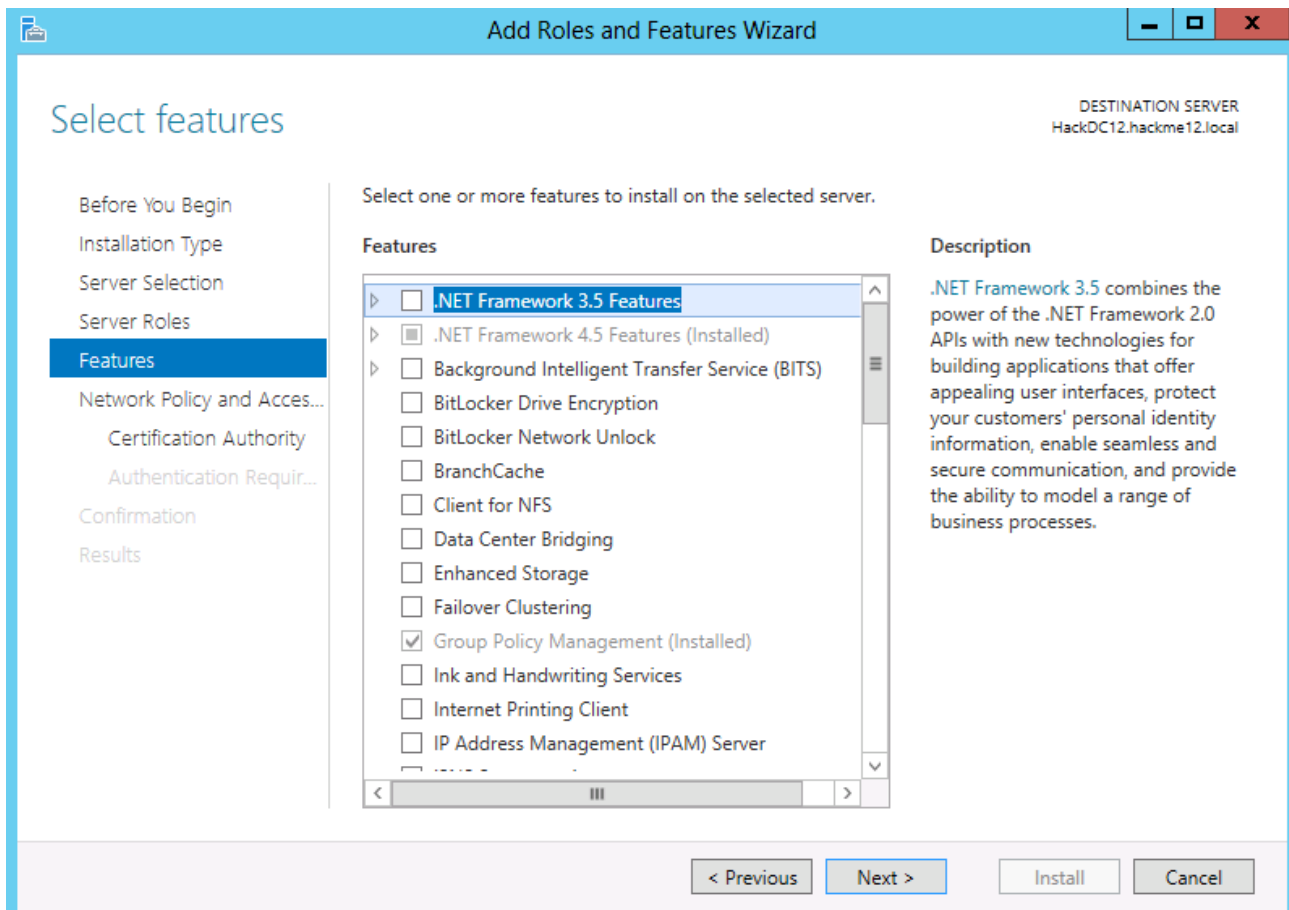
164 Again, to this role we must install some features, click to the “Add Features” button, to accept the recommendation of the computer.



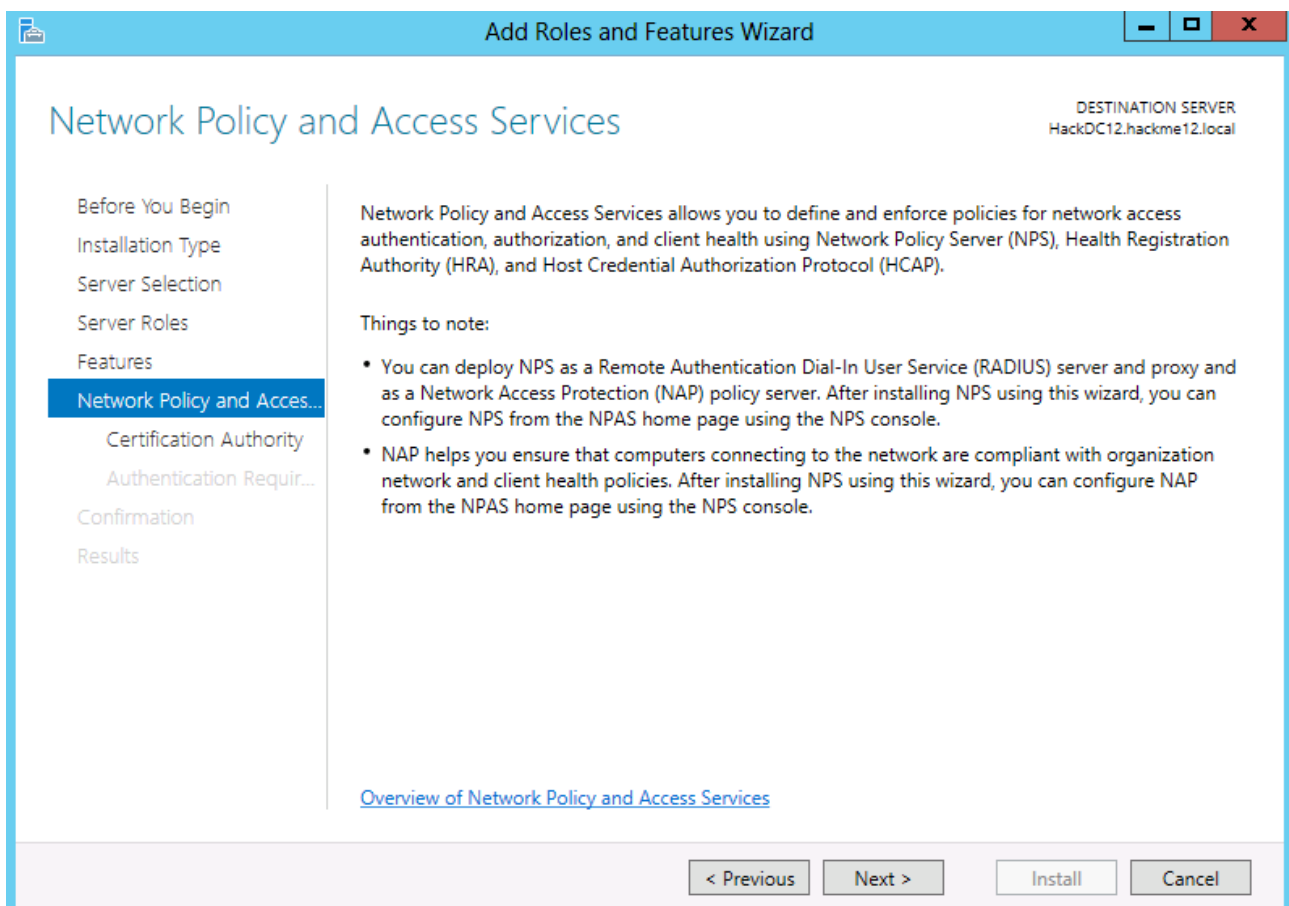
165 click to the next button



166 The required features were automatically selected, so just click to the next button again



167 click to the next button again



168 on the “Certification Authority” page select the “Use the local CA to issue health certificates for this HRA server” then click to the next button

DESTINATION SERVER
HackDC12.hackme12.local

Certification Authority


Before You Begin
Installation Type
Server Selection
Server Roles
Features
Network Policy and Acces...
Certification Authority
Authentication Requir...
Confirmation
Results

Health Registration Authority (HRA) requires that at least one Certification Authority (CA) be associated with it.

☒ Use the local CA to issue health certificates for this HRA server.
There is an existing CA on this computer. If you choose to use it, it will be dedicated to issuing health certificates.

☐ Use an existing remote CA.
If you choose to use an existing CA it should be one dedicated to issuing health certificates.

☐ Select a CA later using the HRA console.

 You will not be able to issue health certificates to NAP client computers until this CA is configured.

< Previous Next > Install Cancel

169 if you select yes only domain members will get health certificates, if you want to allow the communication of non domain member computers select the no.

Add Roles and Features Wizard

DESTINATION SERVER
HackDC12.hackme12.local

Authentication Requirements

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Network Policy and Acces...
Certification Authority
Authentication Requir...
Confirmation
Results

Health Registration Authority can be configured to ensure that only users authenticated to the domain can get health certificates.

Do you want to require that users be authenticated in order to get a health certificate?

☒ Yes, require requestors to be authenticated as members of a domain. (recommended)
This option is only available when the computer is joined to a domain.

☐ No, allow anonymous requests for health certificates.

< Previous Next > Install Cancel

170 click install, to start the installation

Add Roles and Features Wizard

DESTINATION SERVER
HackDC12.hackme12.local

Confirm installation selections

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Network Policy and Acces...
Certification Authority
Authentication Requir...
Confirmation
Results

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

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Network Policy and Access Services

Health Registration Authority

Host Credential Authorization Protocol

Web Server (IIS)

Management Tools

IIS 6 Management Compatibility

IIS 6 Scripting Tools

IIS 6 WMI Compatibility

Web Server

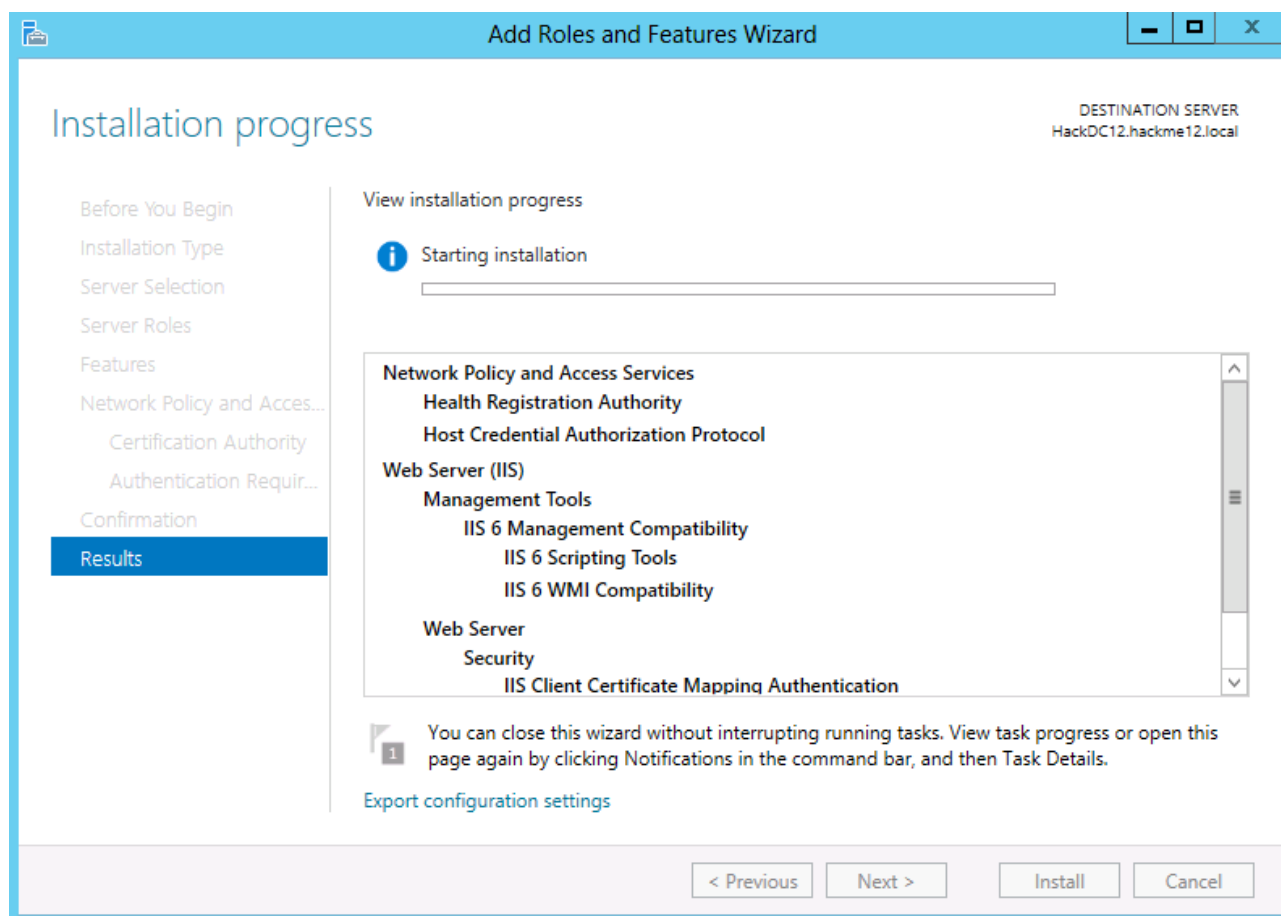
Security

IIS 6 Management and Monitoring Tools

[Export configuration settings](#)
[Specify an alternate source path](#)

< Previous Next > Install Cancel

171 wait patiently, until it finishes



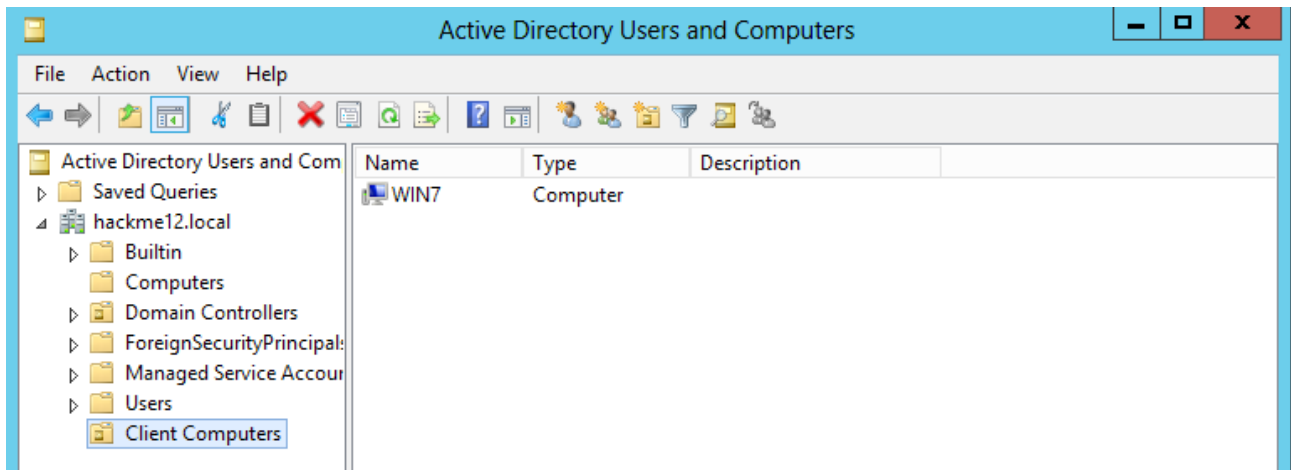
Group policy settings for DHCP and 802.1x enforce

In the group policy we should set up the “Network Access Protection Agent” service to auto start, and the “Wired AutoConfig” service to auto start.

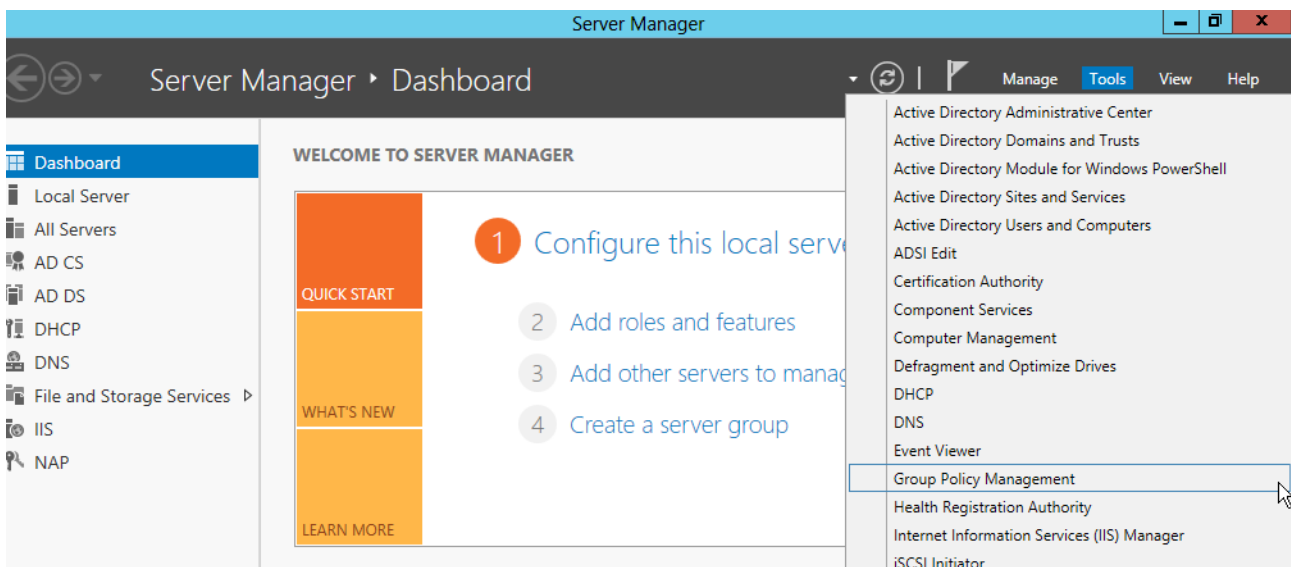
Enable the “DHCP Quarantine Enforcement Client”, and the “EAP Quarantine Enforcement Client” (later we will do the 802.1x enforce, so we enable both if we there).

Turn on security center for the client computers.

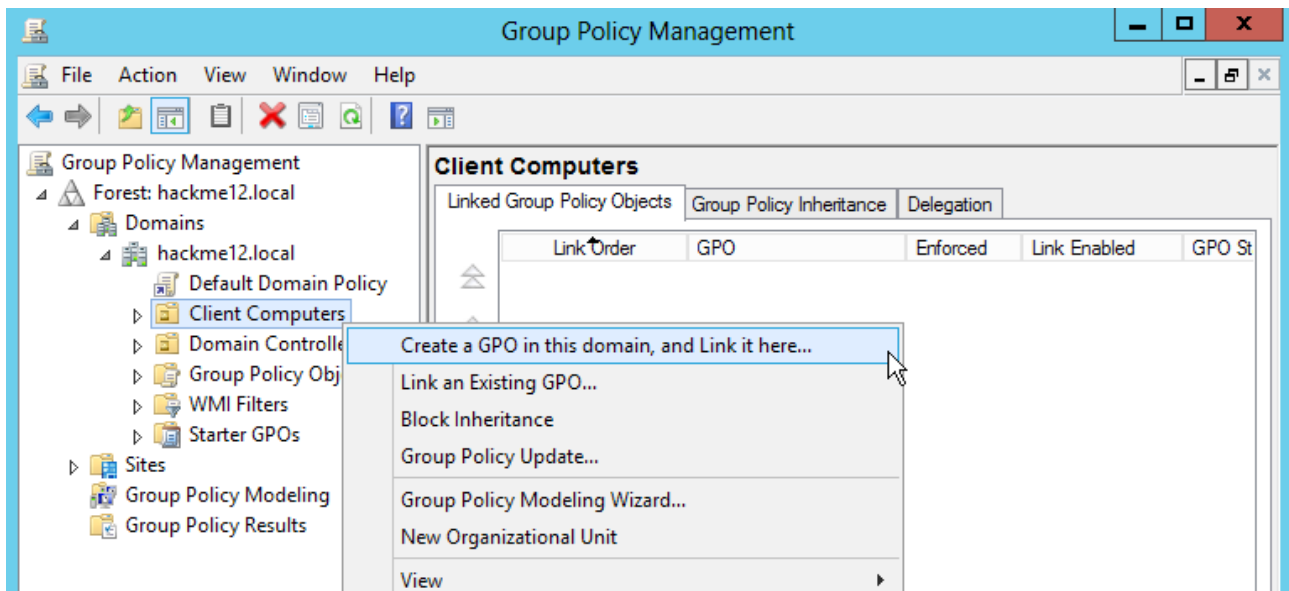
1. Open the Active Directory users and computers, and create an organization unit, and drop there the computer object of your windows 7 test machine



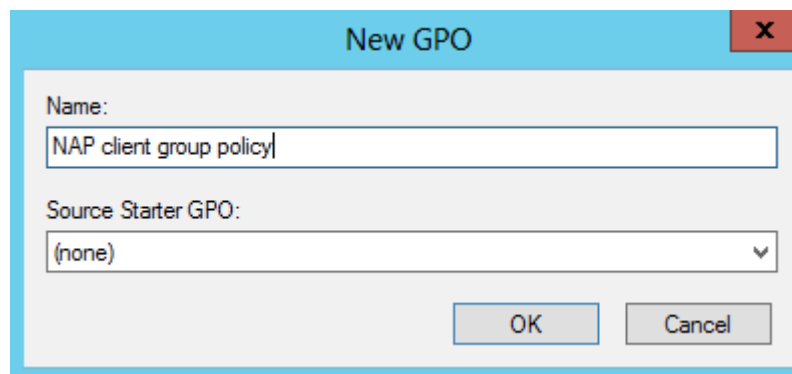
2 Start the group policy management console



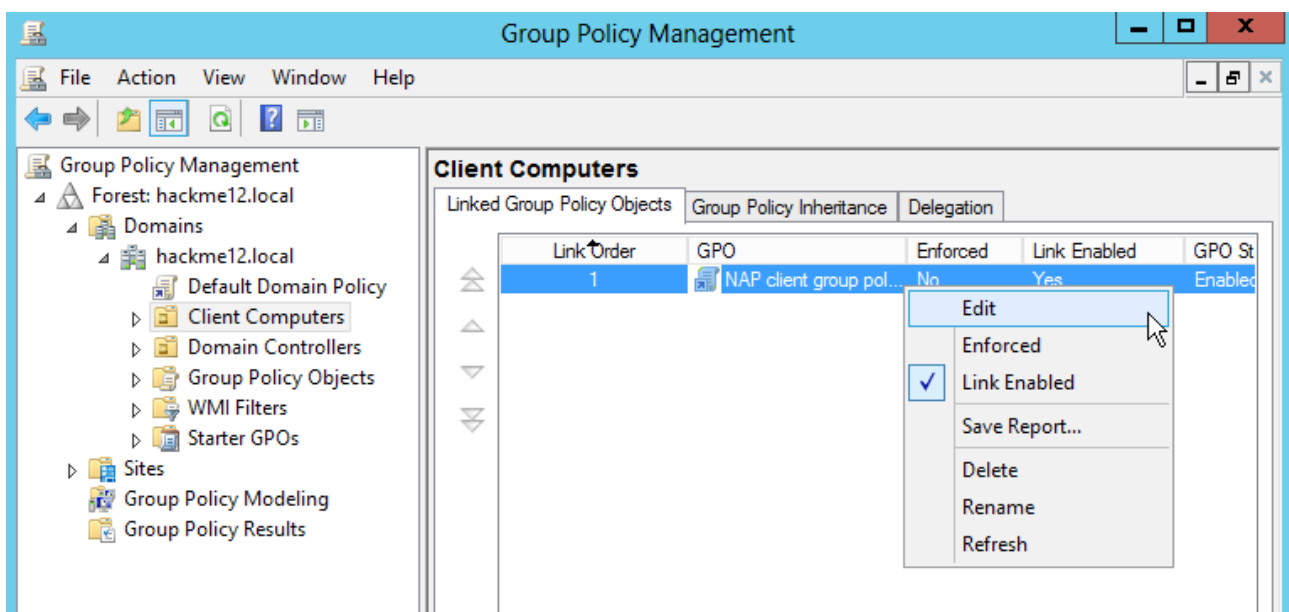
3 right click to the OU contains your windows 7 test machine, and from the popup menu select the “Create a GPO in this domain, and Link it here...”



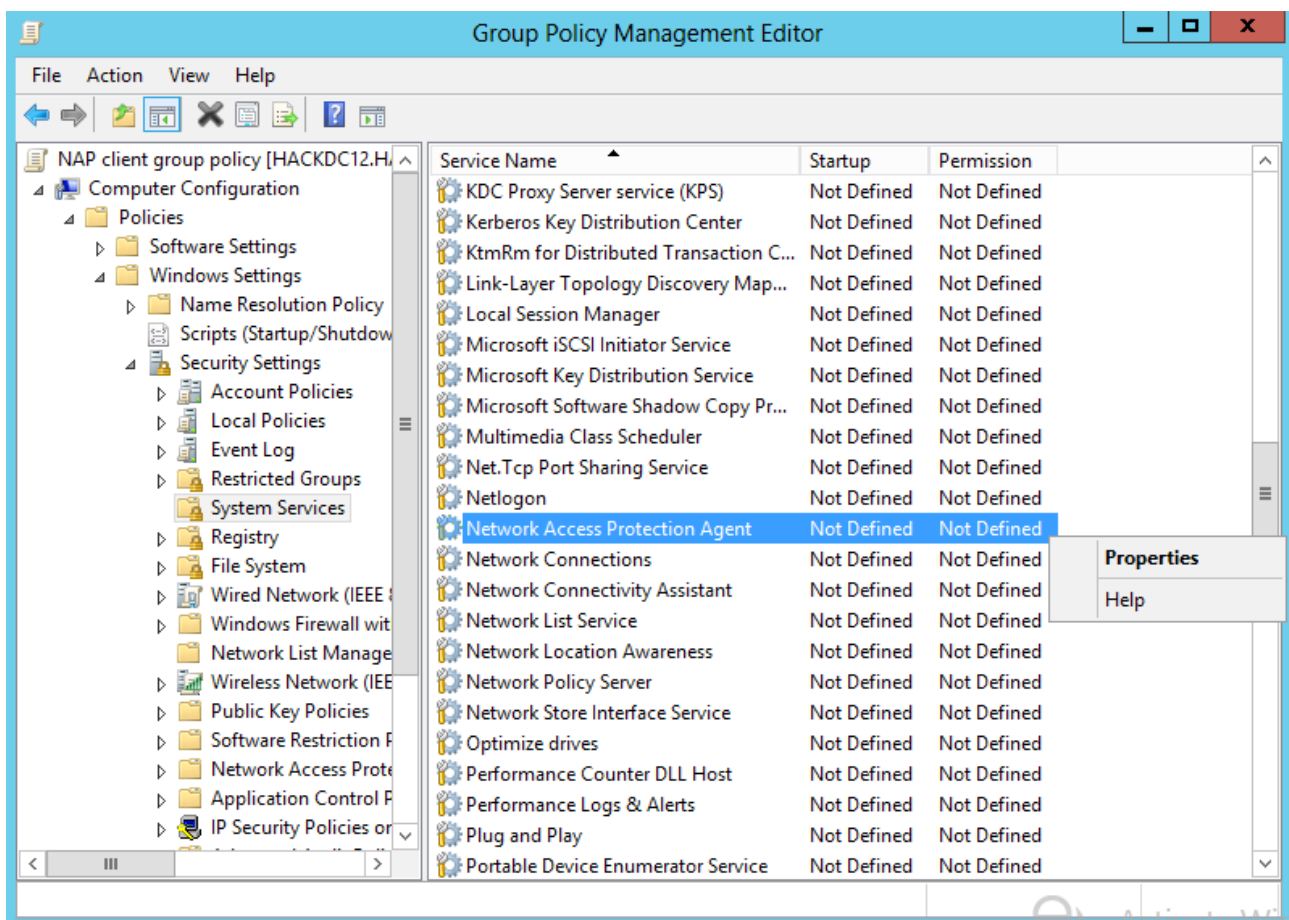
4 give it some name, and we do not need any starter GPO.



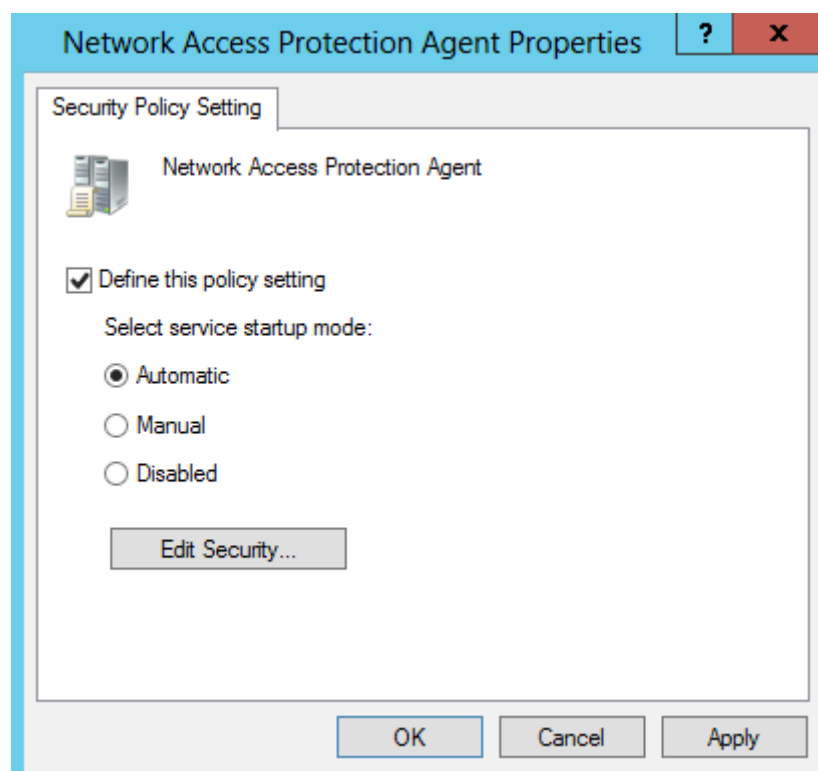
5 right click to this newly created policy, and from the popup menu select "Edit".



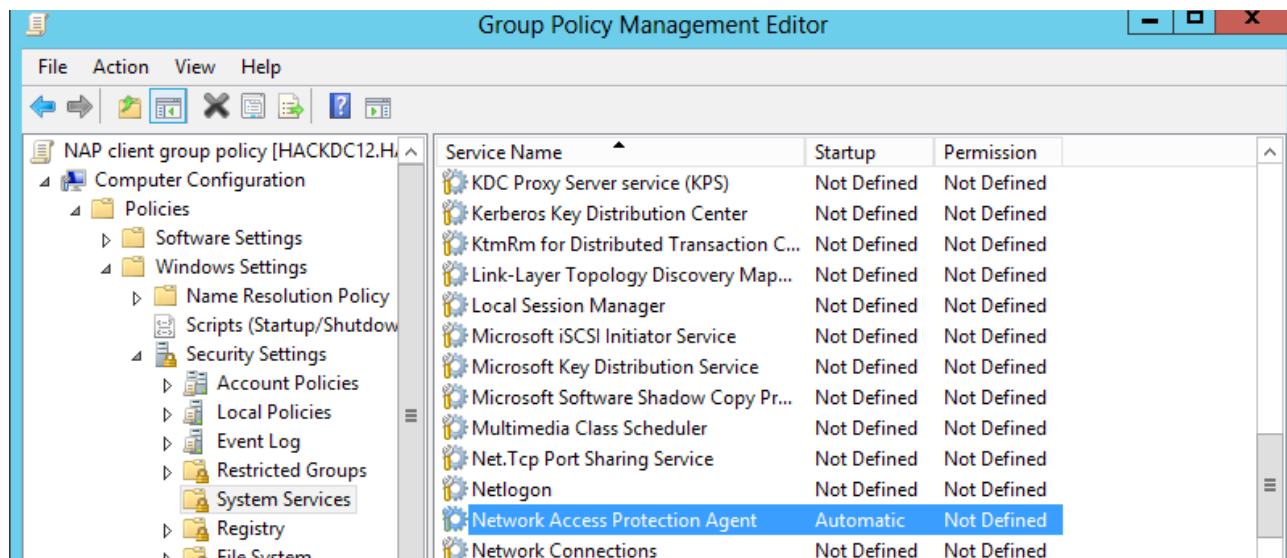
6. Navigate to: computer configuration / Policies / Windows settings / Secure Settings / System Services. Right click to the “Network Access Protection Agent”, and from the popup menu select “Properties”.



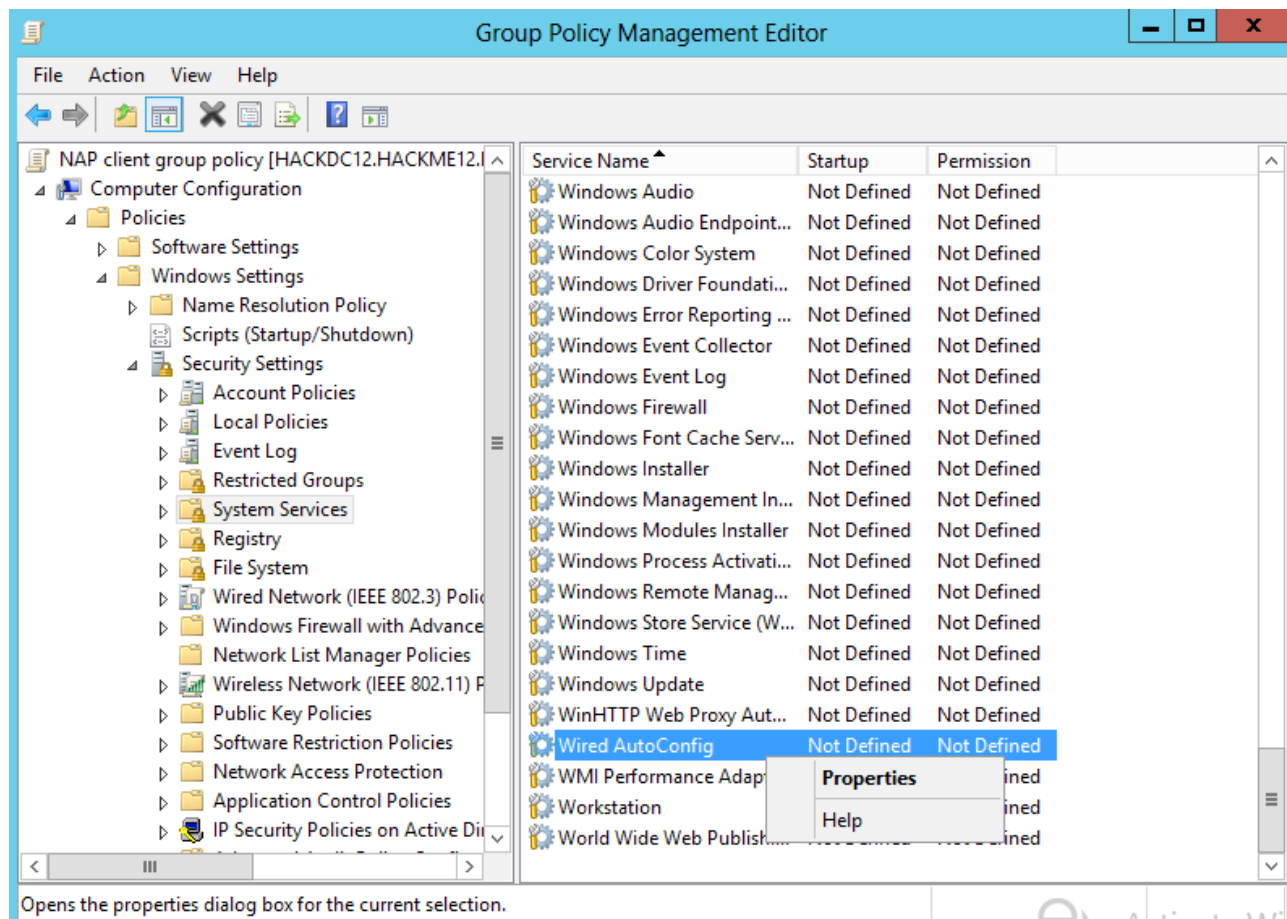
7 Set up the service to Automatic start



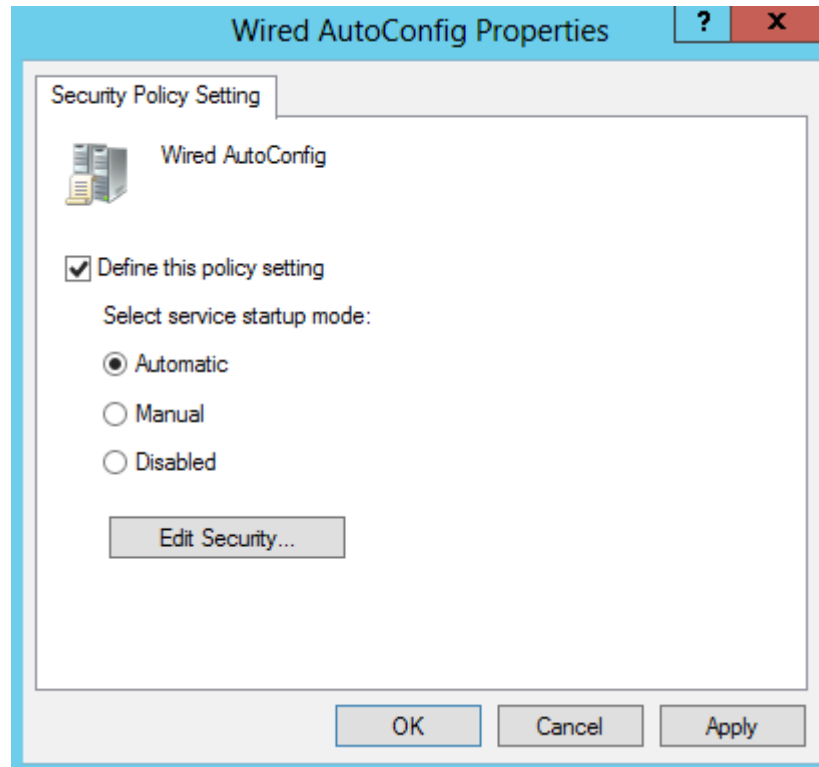
8 check if it really set to automatic



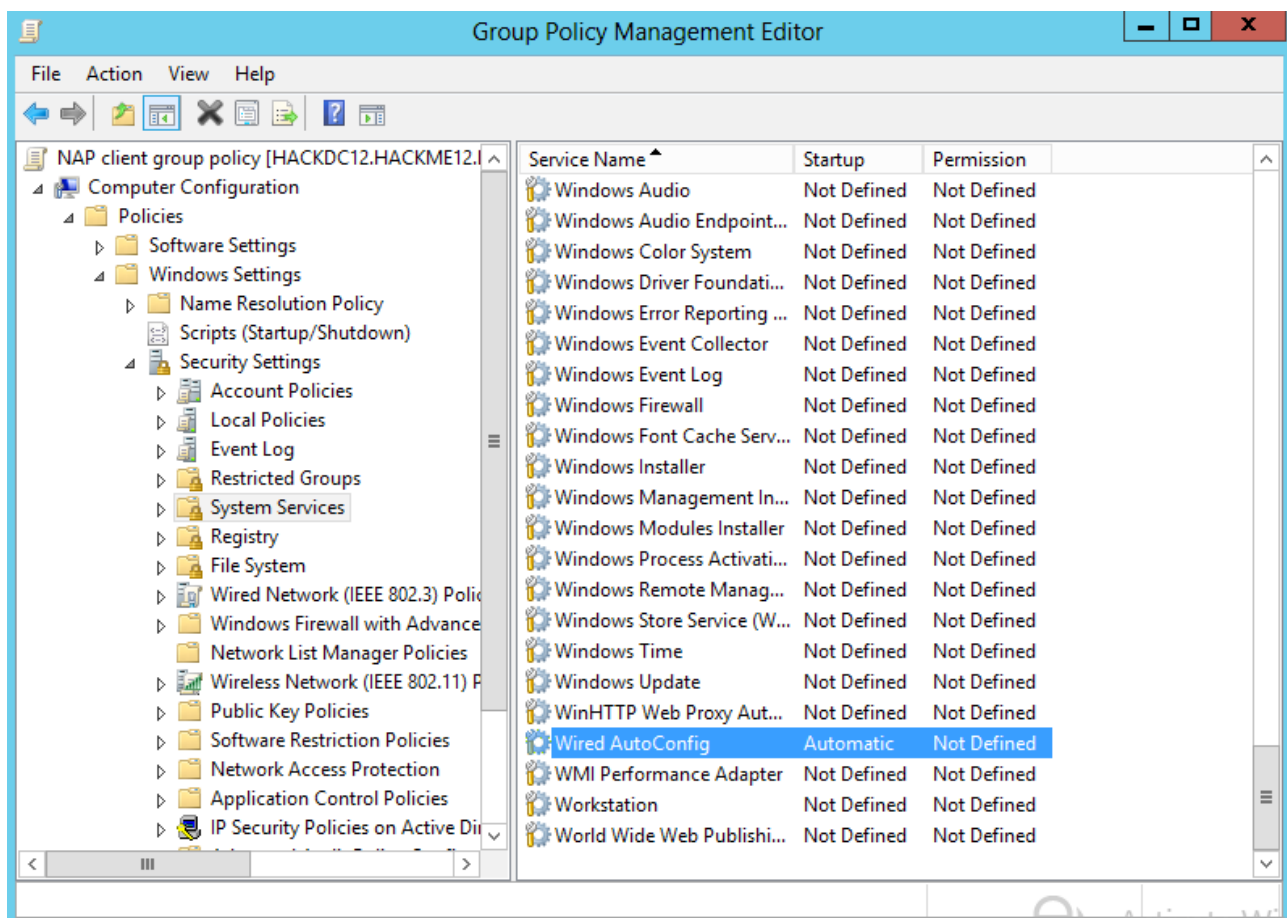
9 Right click to the “Wired AutoConfig”, and from the popup menu select “Properties”.



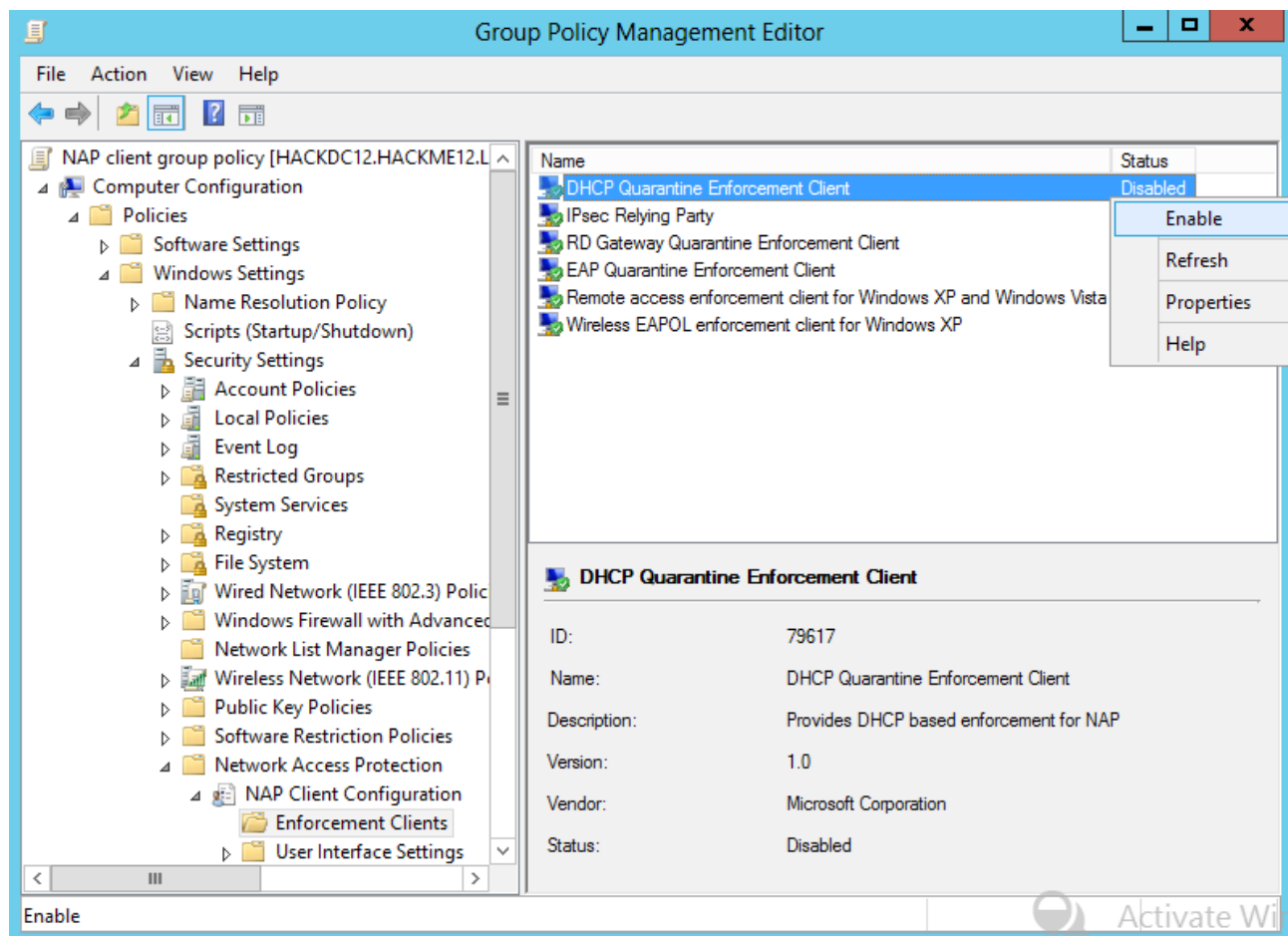
10 Set up the service to Automatic start



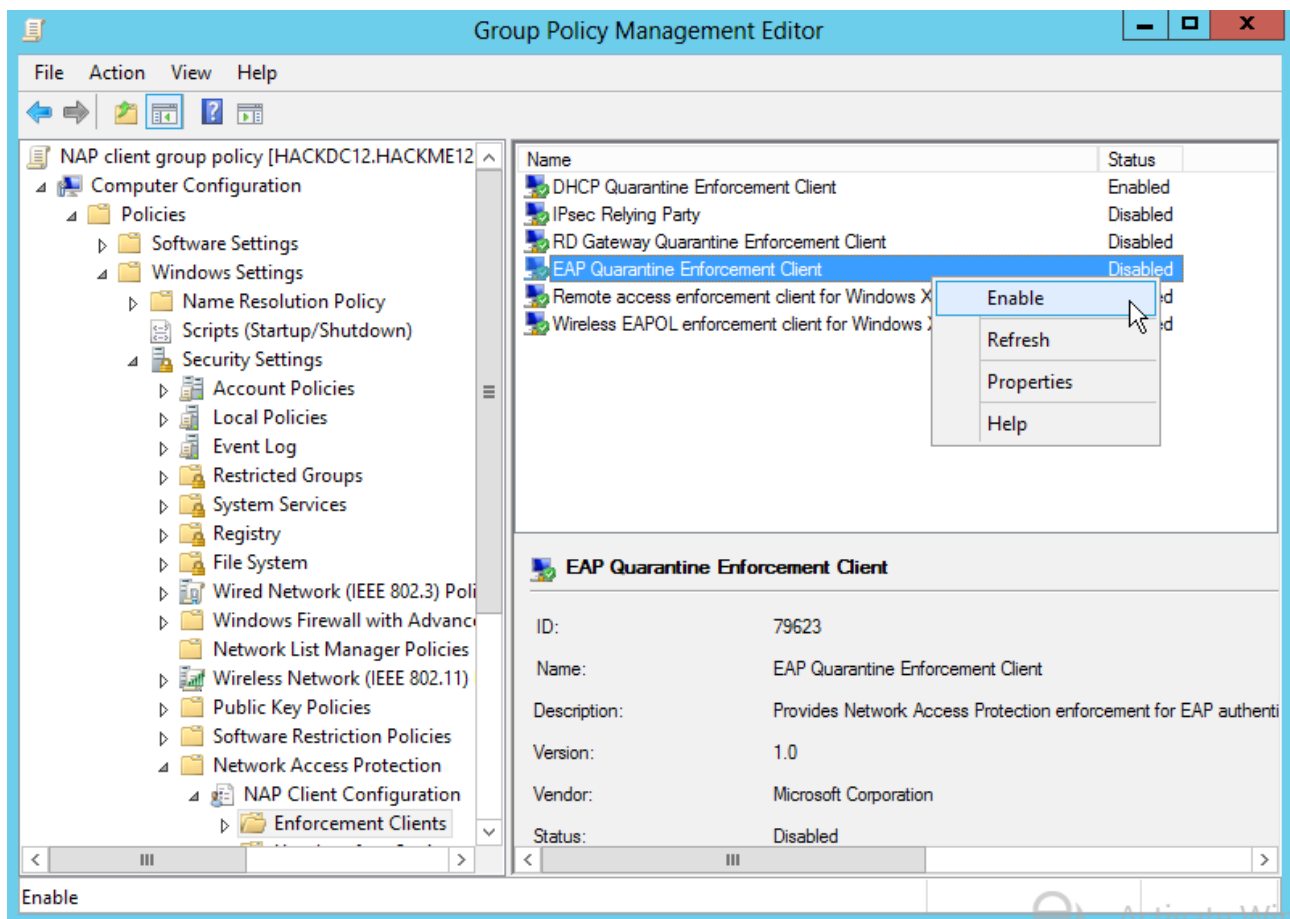
11 check if it really set to automatic



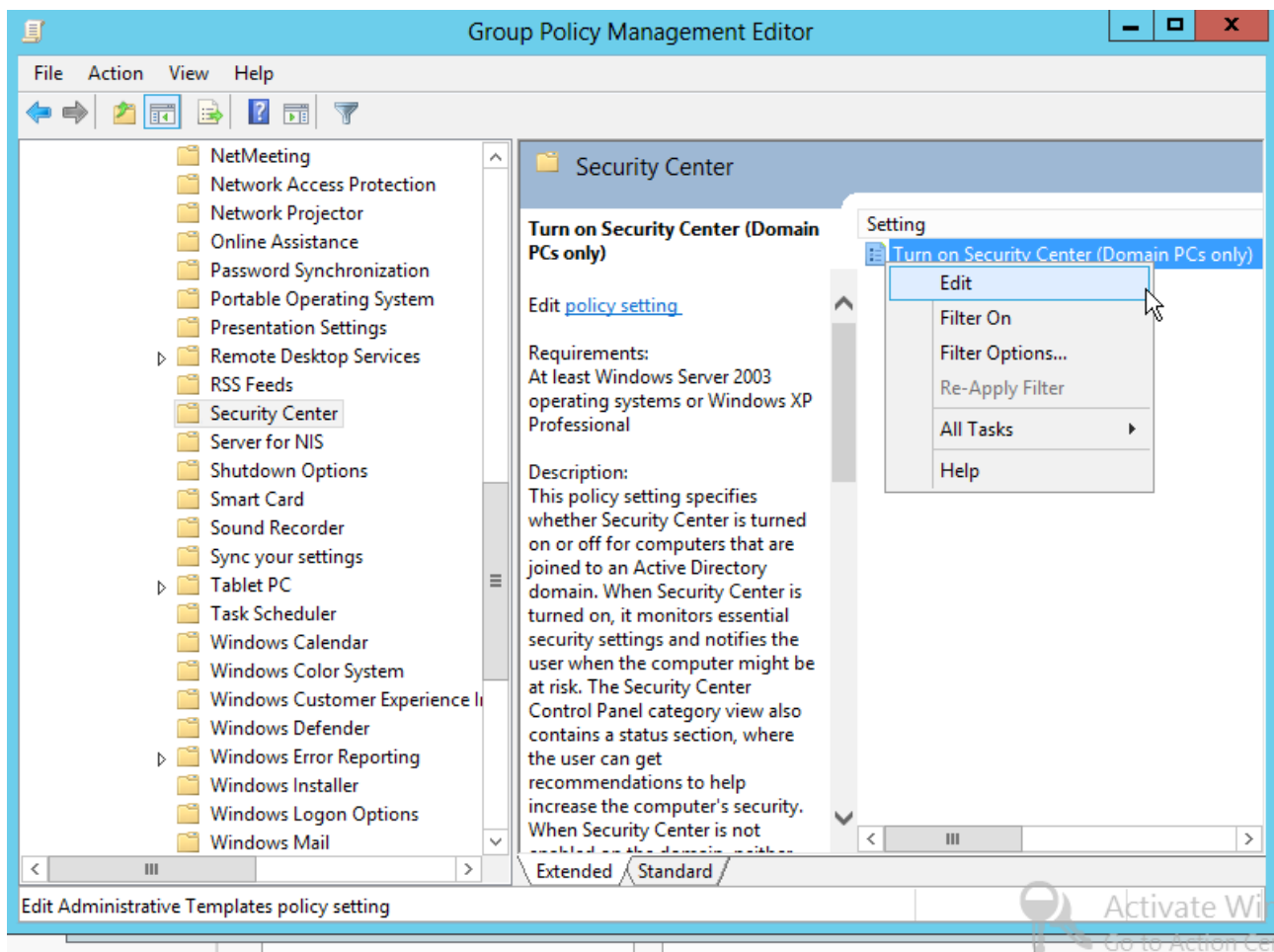
12 Navigate to: computer configuration / Policies / Windows settings / Secure Settings / Network Access Protection / Enforcement Clients. Right click to the “DHCP Quarantine Enforcement Client”, and from the popup menu select “Enable”.



13 Right click to the “EAP Quarantine Enforcement Client”, and from the popup menu select “Enable”. (Obviously this step does not need for the DHCP enforce, but we will do a 802.1x enforce later, and we set up this as well)



14 Navigate to: computer configuration / Policies / Administrative templates / Security Center. Right click to the “Turn on security center (Domain computers only)”, and from the popup menu select edit.



15 enable this policy, and click to the OK.

Turn on Security Center (Domain PCs only)

Turn on Security Center (Domain PCs only)

Previous SettingNext Setting

☐ Not Configured

☒ Enabled

☐ Disabled

Comment:

Supported on:

At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

This policy setting specifies whether Security Center is turned on or off for computers that are joined to an Active Directory domain. When Security Center is turned on, it monitors essential security settings and notifies the user when the computer might be at risk. The Security Center Control Panel category view also contains a status section, where the user can get recommendations to help increase the computer's security. When Security Center is not enabled on the domain, neither the notifications nor the Security Center status section are displayed.

Note that Security Center can only be turned off for computers that are joined to a Windows domain. When a computer is not joined to a Windows domain, the policy setting will have no effect.

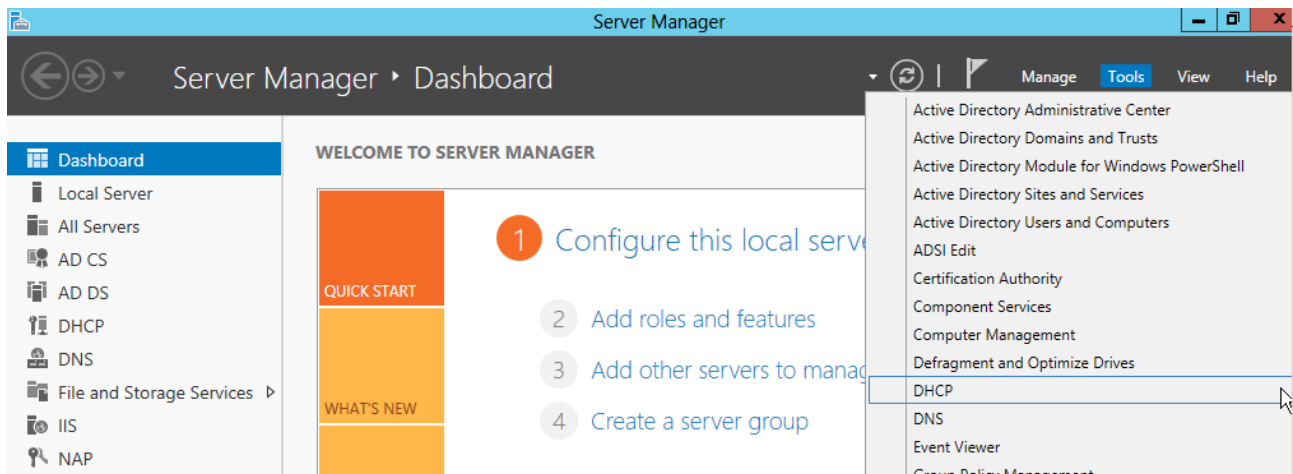
If you do not configure this policy setting, the Security Center is turned off for domain members.

If you enable this policy setting, Security Center is turned on for all users.

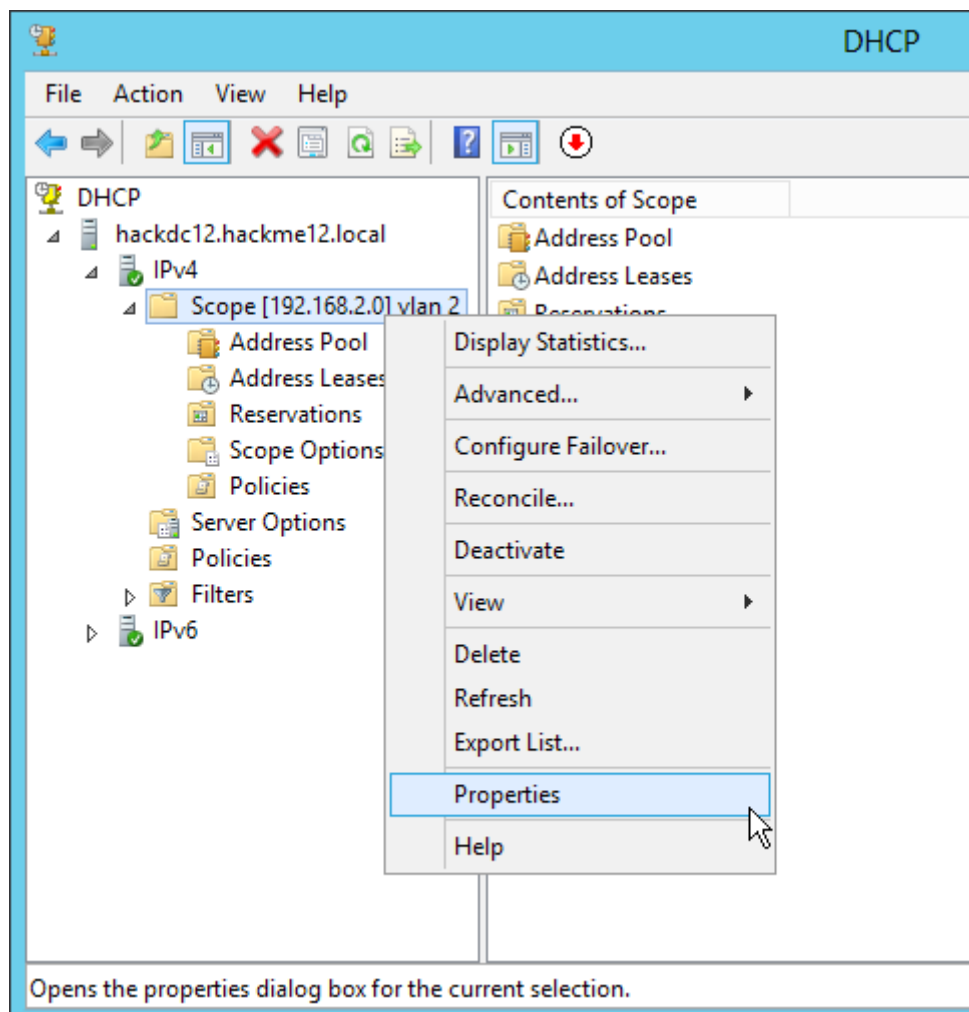
OKCancelApply

Set up the NAP capability on the DHCP

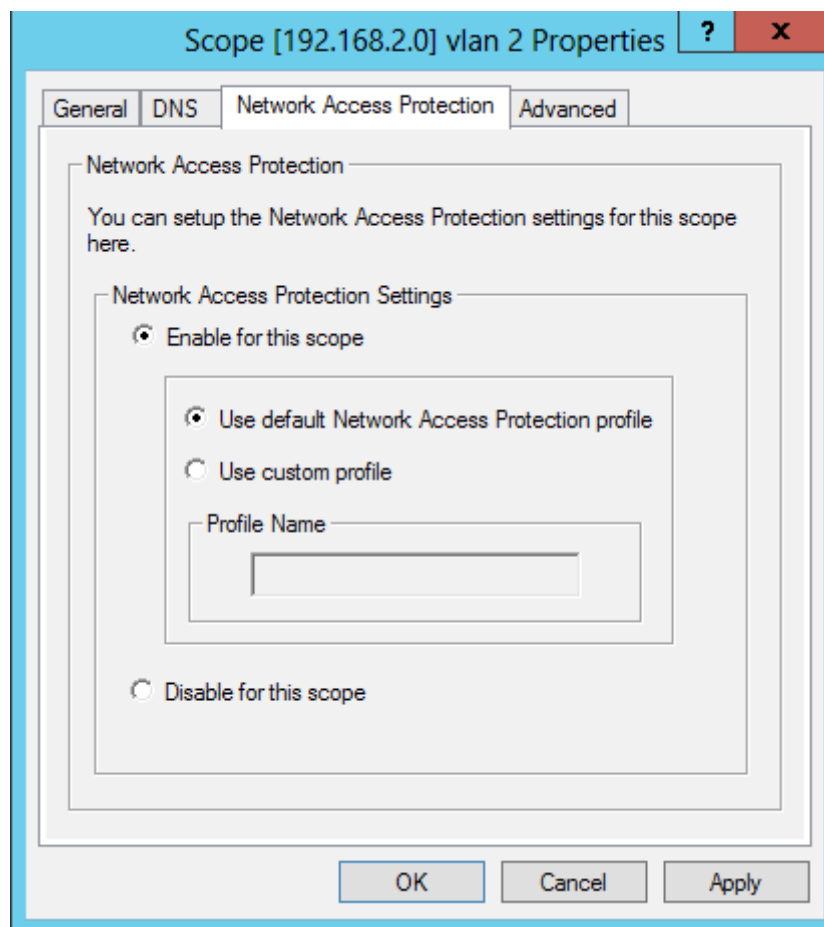
1 Start the DHCP management console



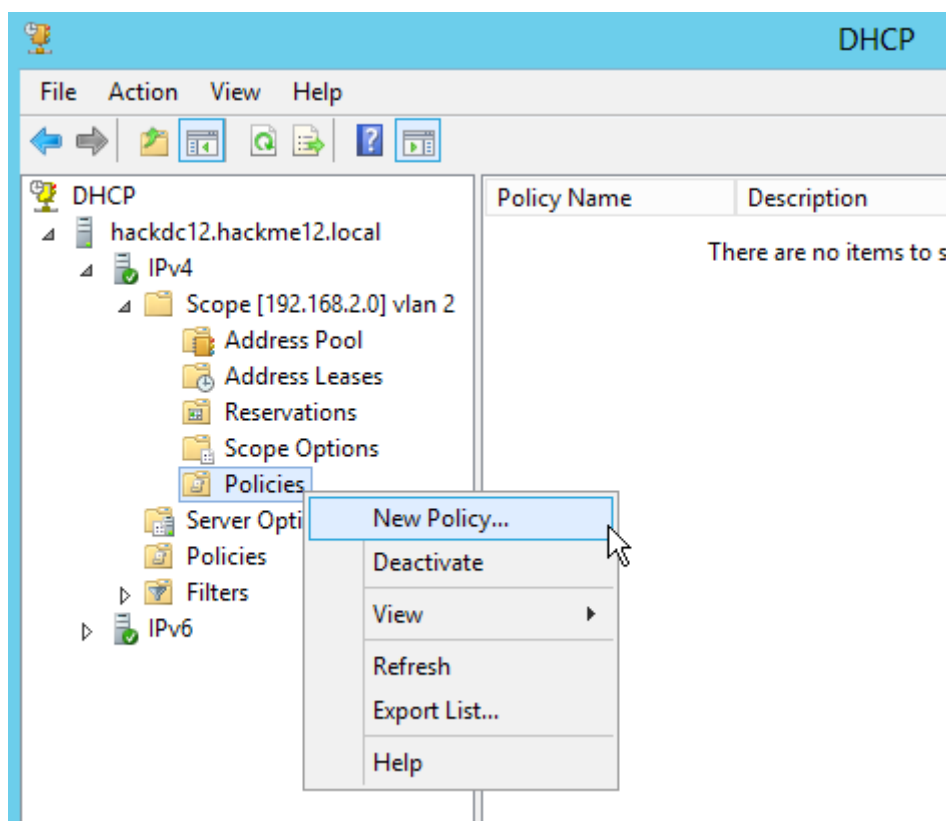
2 Right click to the scope, and from the popup menu select “Properties”



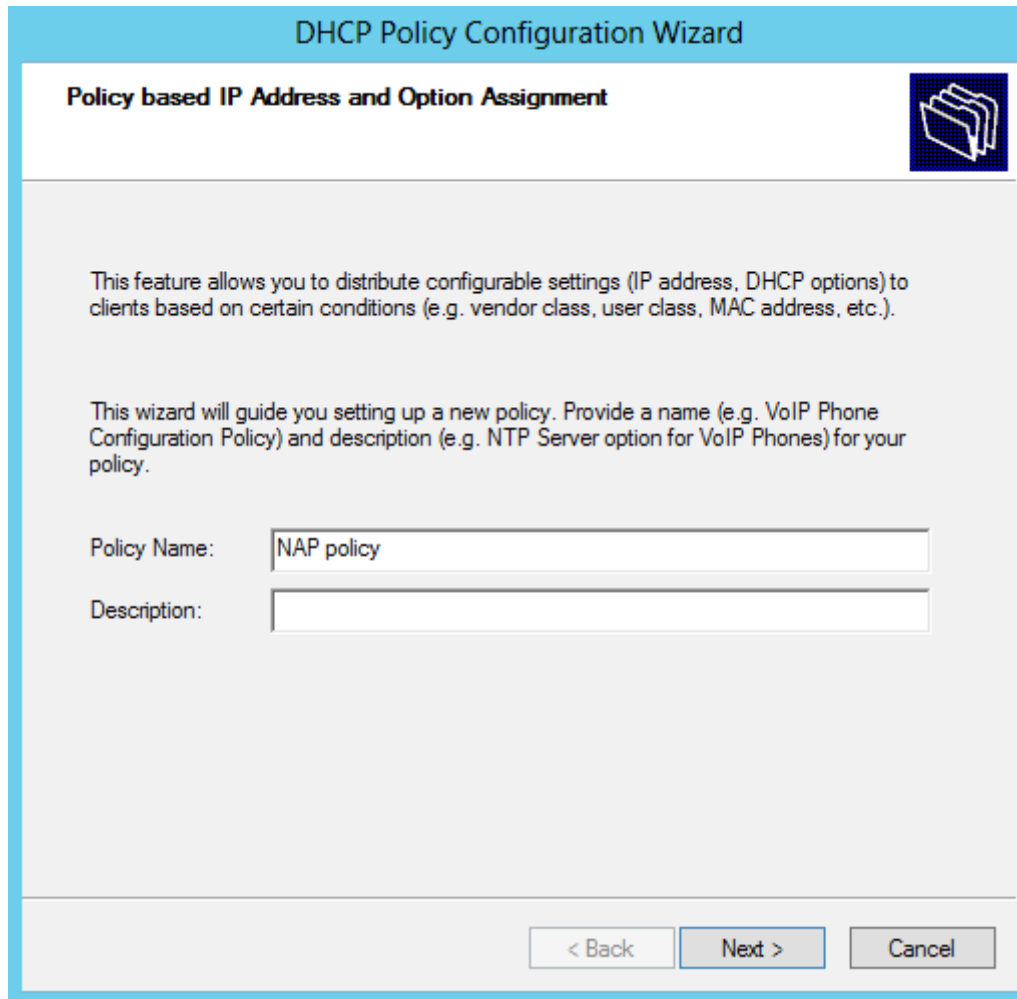
3 navigate to the “Network Access Protection” tab, and enable the NAP for this scope.



4 right click to the “Policies” container, and from the popup menu select the “New policy...” command.



5 give some name to the policy, then click to the “Next” button



The image shows a screenshot of the 'DHCP Policy Configuration Wizard' window. The title bar is blue and contains the text 'DHCP Policy Configuration Wizard'. Below the title bar, the window has a white header area with the text 'Policy based IP Address and Option Assignment' on the left and a blue folder icon on the right. The main content area is light gray and contains two paragraphs of text. The first paragraph states: 'This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).' The second paragraph states: 'This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.' Below the text, there are two input fields. The first is labeled 'Policy Name:' and contains the text 'NAP policy'. The second is labeled 'Description:' and is empty. At the bottom of the window, there is a gray bar containing three buttons: '< Back', 'Next >', and 'Cancel'.

DHCP Policy Configuration Wizard

Policy based IP Address and Option Assignment

This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name:


Description:

< Back Next > Cancel

6 Click to the “Add” button

DHCP Policy Configuration Wizard

Configure Conditions for the policy



A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

Conditions	Operator	Value

☐ AND
 ☒ OR

7 Select “User Class” for criteria, “Equals” as operator, and “Default Network Access Protection Class” as value:

Add/Edit Condition

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: User Class

Operator: Equals

Value(s)


Value: Default Network Access Protection Class

☐ Append wildcard(*)

Default Network Access Protection Class

8 Click to the next button

DHCP Policy Configuration Wizard

Configure Conditions for the policy 

A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

Conditions	Operator	Value
User Class	Equals	Default Network Access Protectio...


☐ AND ☒ OR

9 define a smaller IP range for the non compliant computers, just to be able to simply check it, then click to the next button.

DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.



A scope can be subdivided into multiple IP address ranges. Clients that match the conditions defined in a policy will be issued an IP Address from the specified range.

Configure the start and end IP address for the range. The start and end IP addresses for the range must be within the start and end IP addresses of the scope.

The current scope IP address range is 192.168.2.200 - 192.168.2.250

If an IP address range is not configured for the policy, policy clients will be issued an IP address from the scope range.

Do you want to configure an IP address range for the policy: ☒ Yes ☐ No

Start IP address:

End IP address:

Percentage of IP address range: 21.6

< Back

Next >


Cancel

10 Click next on the following window

DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.



Vendor class:

DHCP Standard Options

Available Options	Description	
<input type="checkbox"/> 002 Time Offset	UTC offset in seconds	^
<input type="checkbox"/> 003 Router	Array of router addresses order	
<input type="checkbox"/> 004 Time Server	Array of time server addresses	v
<		>

Data entry

Long:

0x0

< Back

Next >

Cancel

11 click finish to finish the configuration.

Cancel

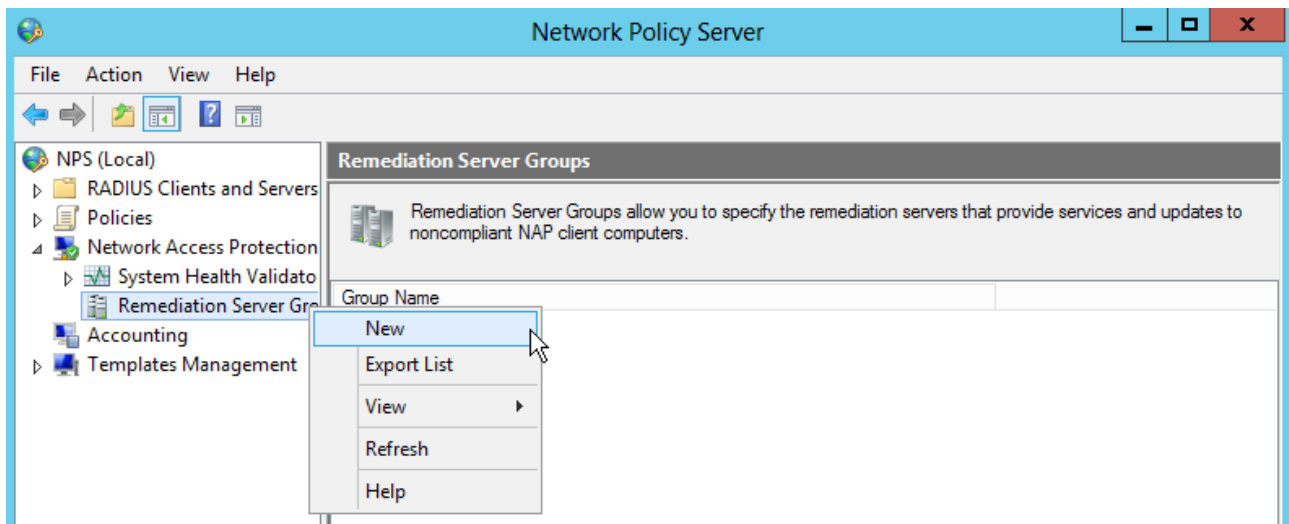
12 check if the policy is created

III

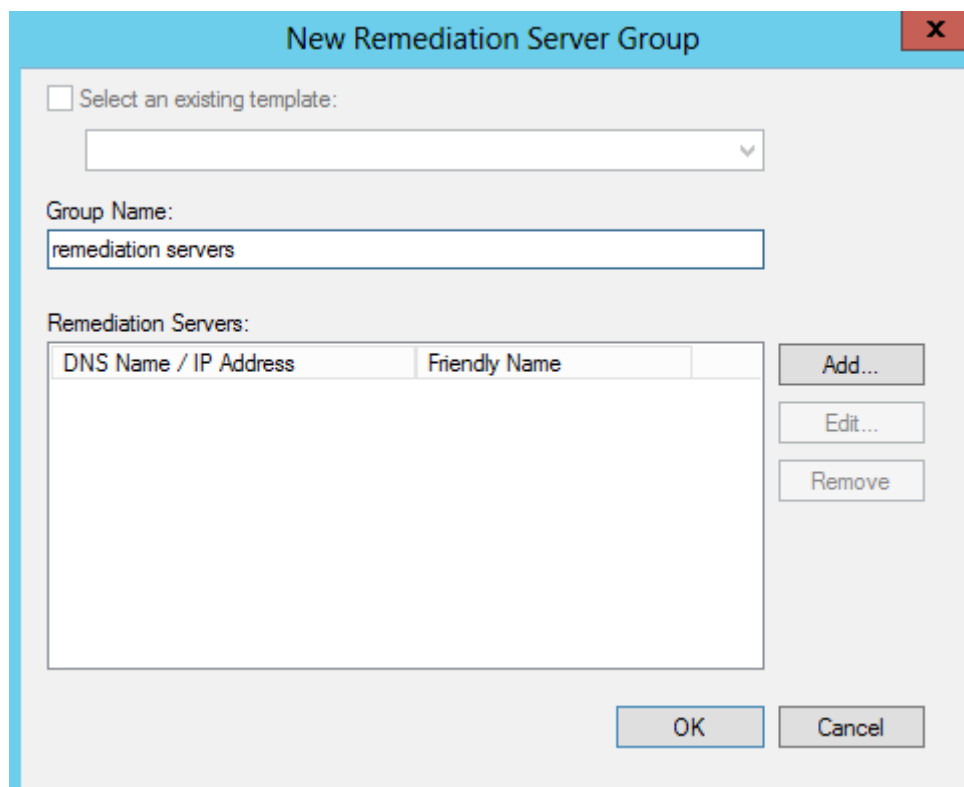
Set up the NAP on the NPS server

Create a Remediation Server Group

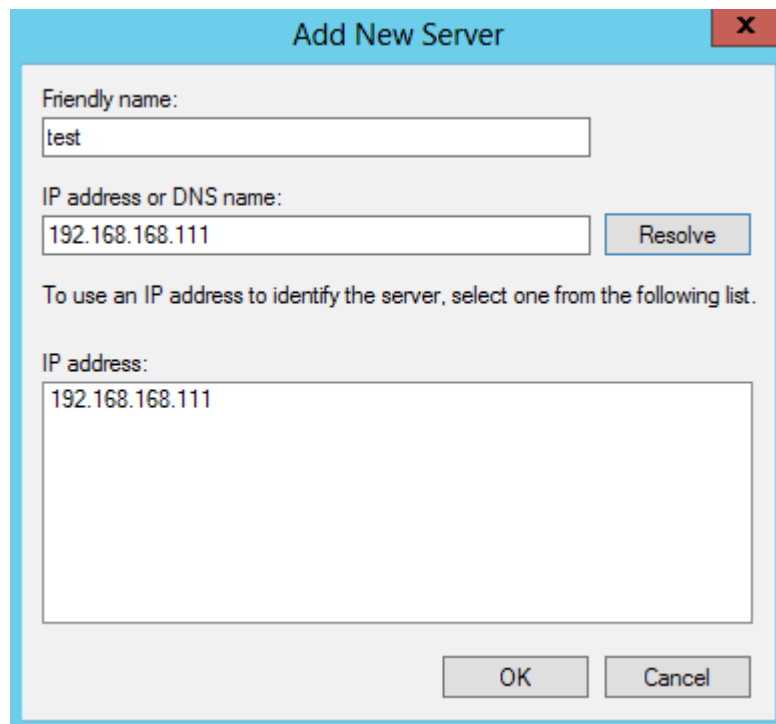
1 We create a remediation group, to be able to support the computers not bypass the health check. Start the “Network Policy Server” management console, then right click to the “Remediation Server Group”, and from the popup menu select New



2 give a name to the remediation server group, then click to the “Add...” buddon



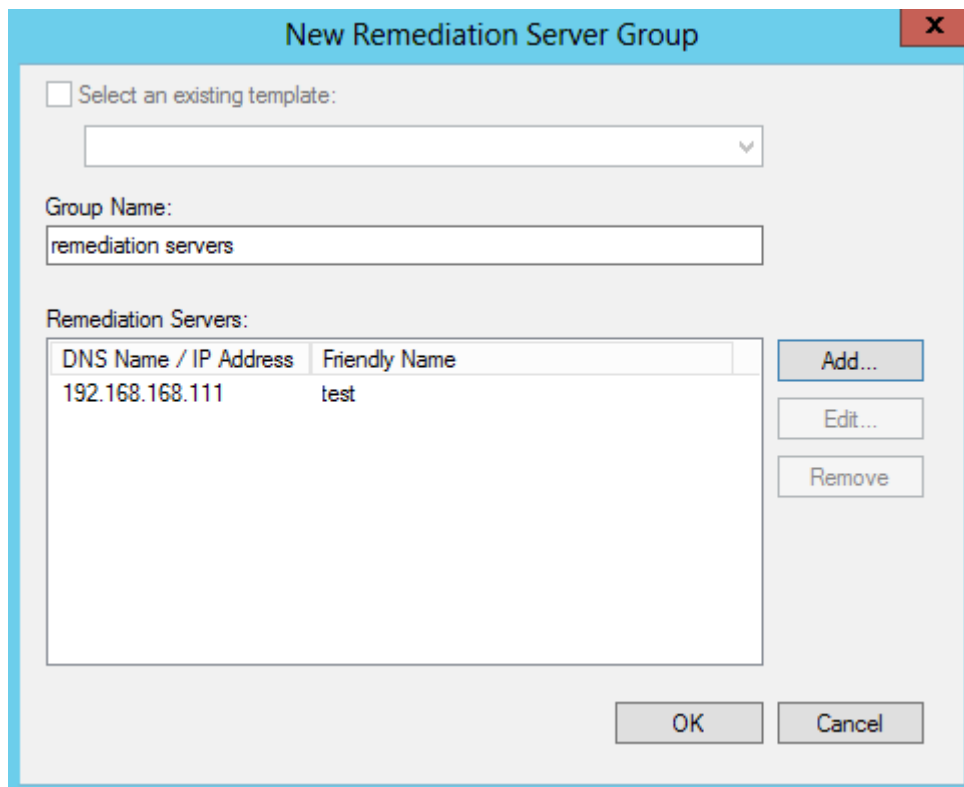
3 type the IP address or the name of the computer you want to use as remediation server, you can give it a friendly name, if you wish, but it not mandatory.



The "Add New Server" dialog box has a light blue title bar with a close button (X). It contains the following fields and controls:

- Friendly name:** A text input field containing "test".
- IP address or DNS name:** A text input field containing "192.168.168.111". To its right is a "Resolve" button.
- Instructions:** A line of text stating "To use an IP address to identify the server, select one from the following list."
- IP address:** A list box containing "192.168.168.111".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

4 if you want to add more computers use the “Add...” button. For me this one is enough, so I just click to the “OK” button.



The "New Remediation Server Group" dialog box has a light blue title bar with a close button (X). It contains the following fields and controls:

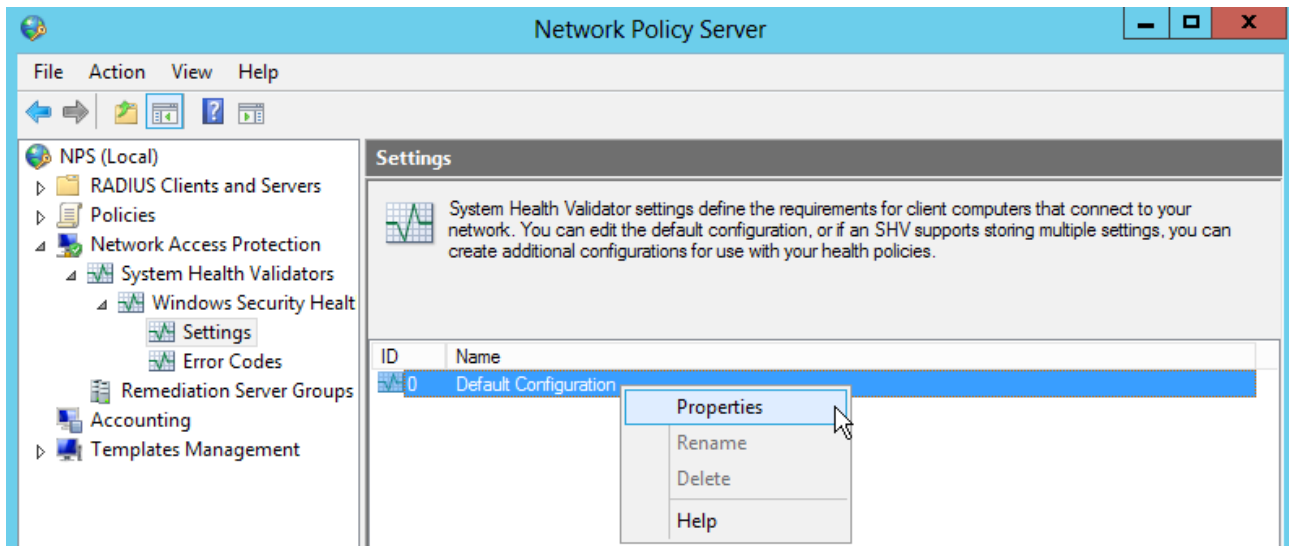
- Select an existing template:** An unchecked checkbox above a dropdown menu.
- Group Name:** A text input field containing "remediation servers".
- Remediation Servers:** A table with two columns: "DNS Name / IP Address" and "Friendly Name".

DNS Name / IP Address	Friendly Name
192.168.168.111	test
- Buttons:** "Add...", "Edit...", and "Remove" buttons are located to the right of the table. "OK" and "Cancel" buttons are at the bottom right.

Set up windows security health

After we set up the remediation server group the next step is to define what kind of tests we want to run on the computers.

1 find the “Network Access Protection” / System Health Validators / Windows Security Health / Settings. Right click to the “Default Configuration”, and from the popup menu select the Properties command.



2 Select what kind of test you want to execute, now I want test only if the firewall is enabled, because it is easy to test in this way. Then click to the OK button.

Windows Security Health Validator

Windows 8/Windows 7/Win
Windows XP



Choose policy settings for Windows Security Health Validator

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

[How do I configure a security health policy?](#)

Firewall Settings

☒ A firewall is enabled for all network connections

Antivirus Settings

☐ An antivirus application is on

☐ Antivirus is up to date

Spyware Protection Settings

☐ An antispyware application is on

☐ Antispyware is up to date

Automatic Updates Settings

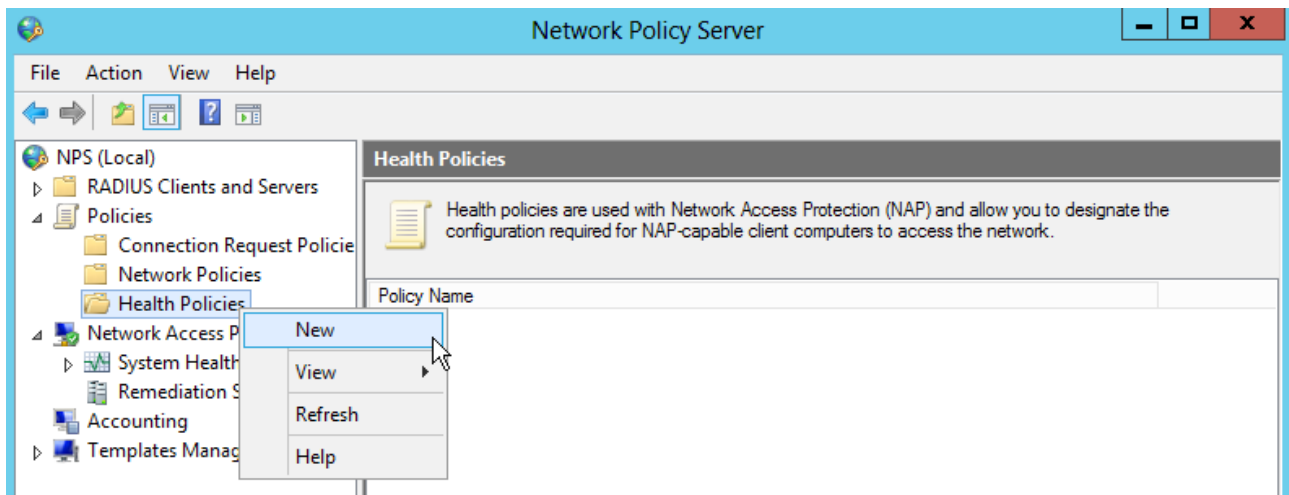
OK

Cancel

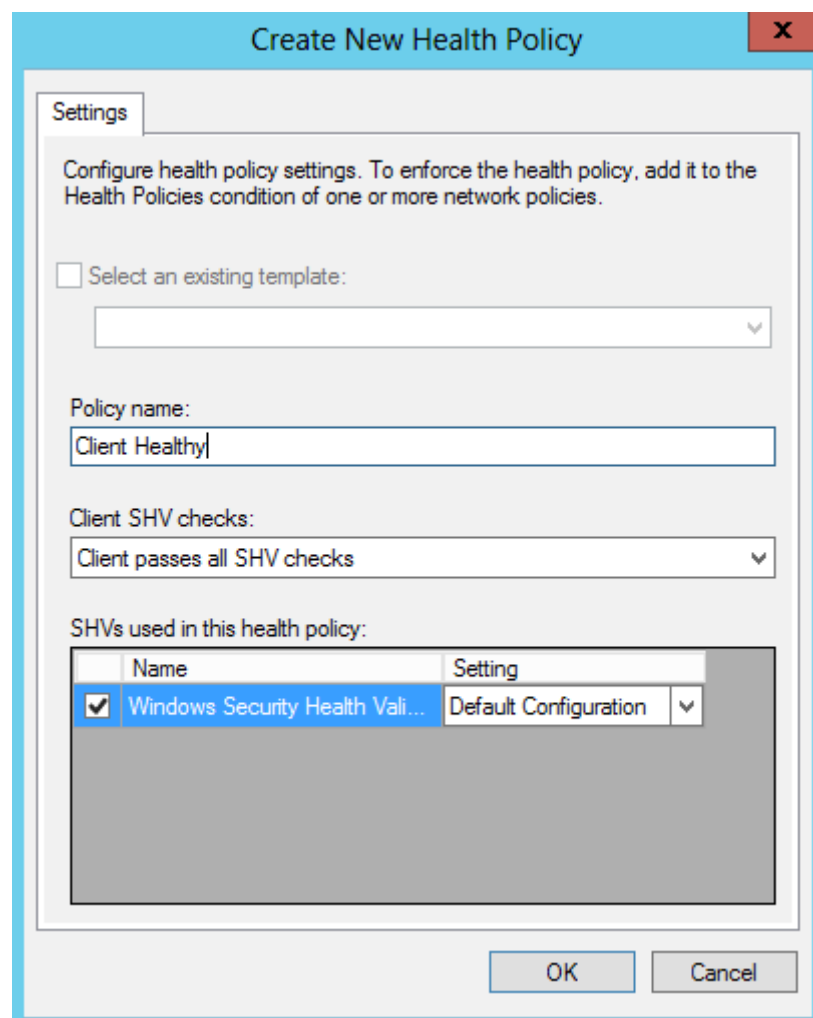
Create Health policy

Now we should create two health policies, one which define how we identify the compliant computers, and the non compliant computers.

1 right click to the policies / Health Policies and from the popup menu select “New”



2 create a new policy for the healthy computers. Give it some name, and from the “Client SHV checks” select the “Client passes all SHV checks”. So this policy will evaluates to true, if the client pass every check. Then click to the OK button



3 right click again to the policies / Health Policies and from the popup menu select “New”. Create a new policy for the non healthy computers. Give it some name, and from the “Client SHV checks” select the “Client fails one or more SHV checks”. So this policy will evaluates to true, if the client fails on at least one check. Then click to the OK button

Create New Health Policy

Settings

Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.

☐ Select an existing template:

Policy name:
Client NOT Healthy

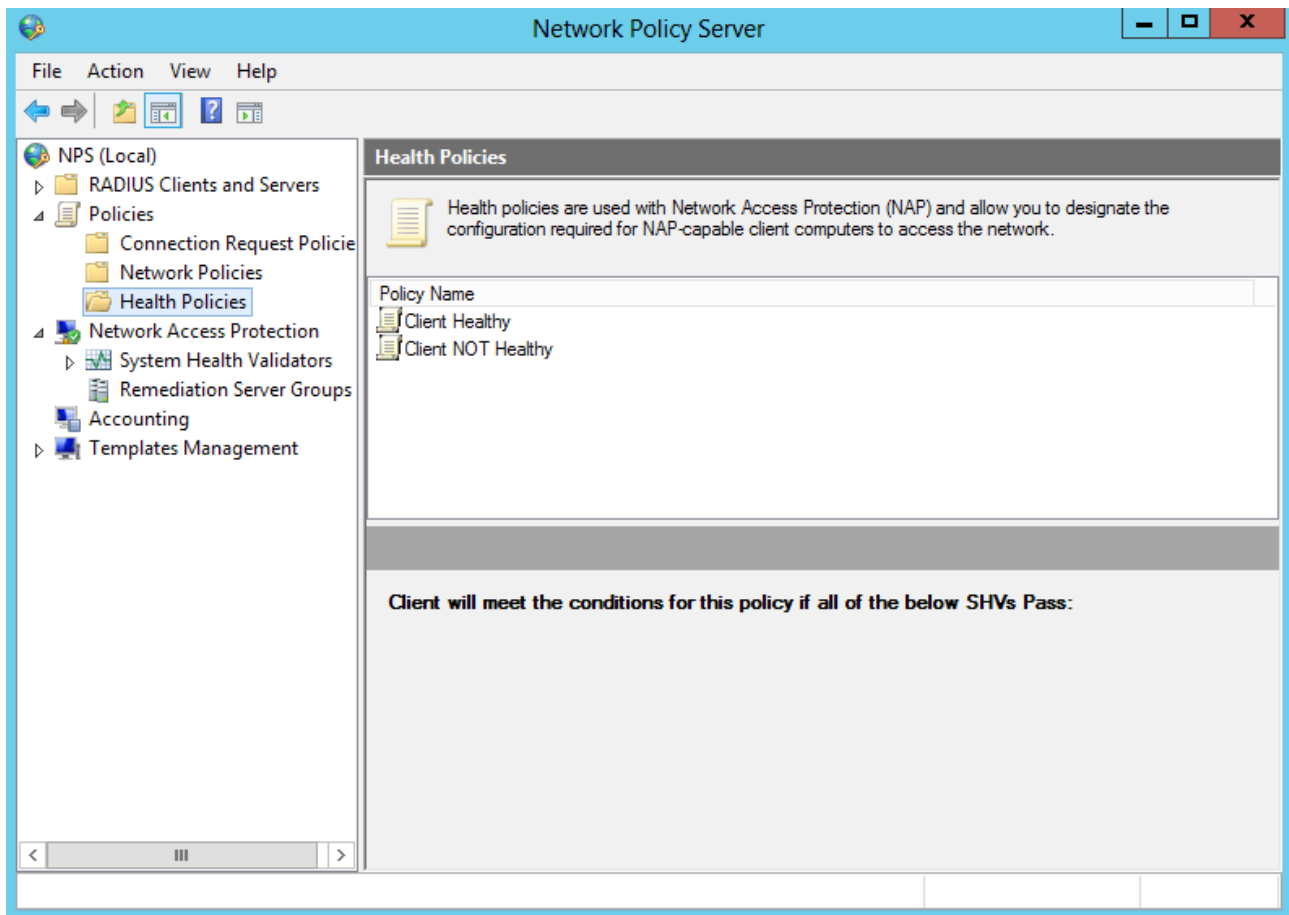
Client SHV checks:
Client fails one or more SHV checks

SHVs used in this health policy:

	Name	Setting
<input checked="" type="checkbox"/>	Windows Security Health Vali...	Default Configuration

OK Cancel

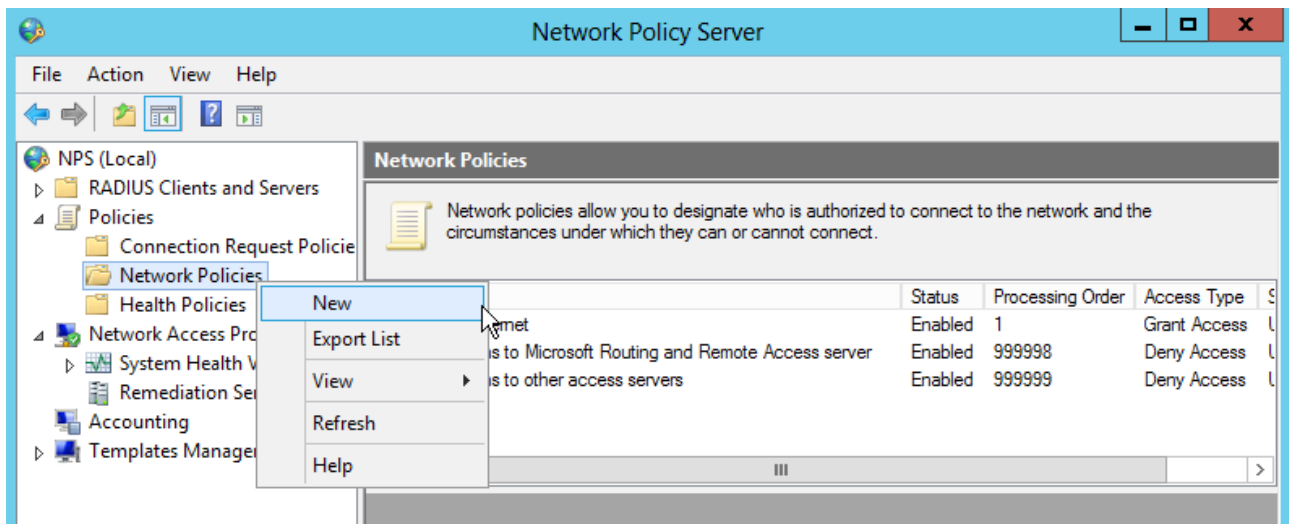
4 Check if both the health policies are created.



Create Network Policy


The next step is to create two network policies. The first is to enable full network access for the compliant client computers, and a second, to enable access to only the remediation computers for the non compliant computers.

1 right click to the Policies / Network Policies, and from the popup menu select “New”



2 Give some name to the policy, and select “DHCP Server” as “Type of network access server”, then click to the “Next” button.

New Network Policy



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

Healthy\clients get network access

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, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

DHCP Server

▼

☐ Vendor specific:

10

^
▼

Previous

Next

Finish

Cancel

3 on the specify condition window click to the “Add...” button

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
-----------	-------

Condition description:

Add... Edit... Remove

Previous Next Finish Cancel

4 Select "Health Policies" as condition type then click to the "Add..." button

Select condition

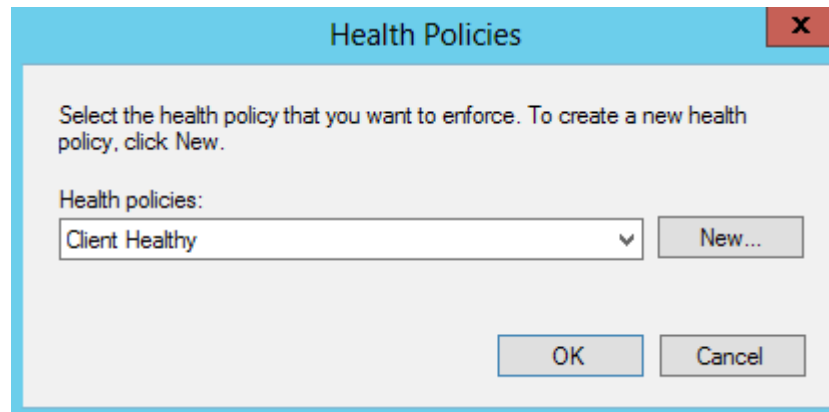
Select a condition, and then click Add.

Network Access Protection

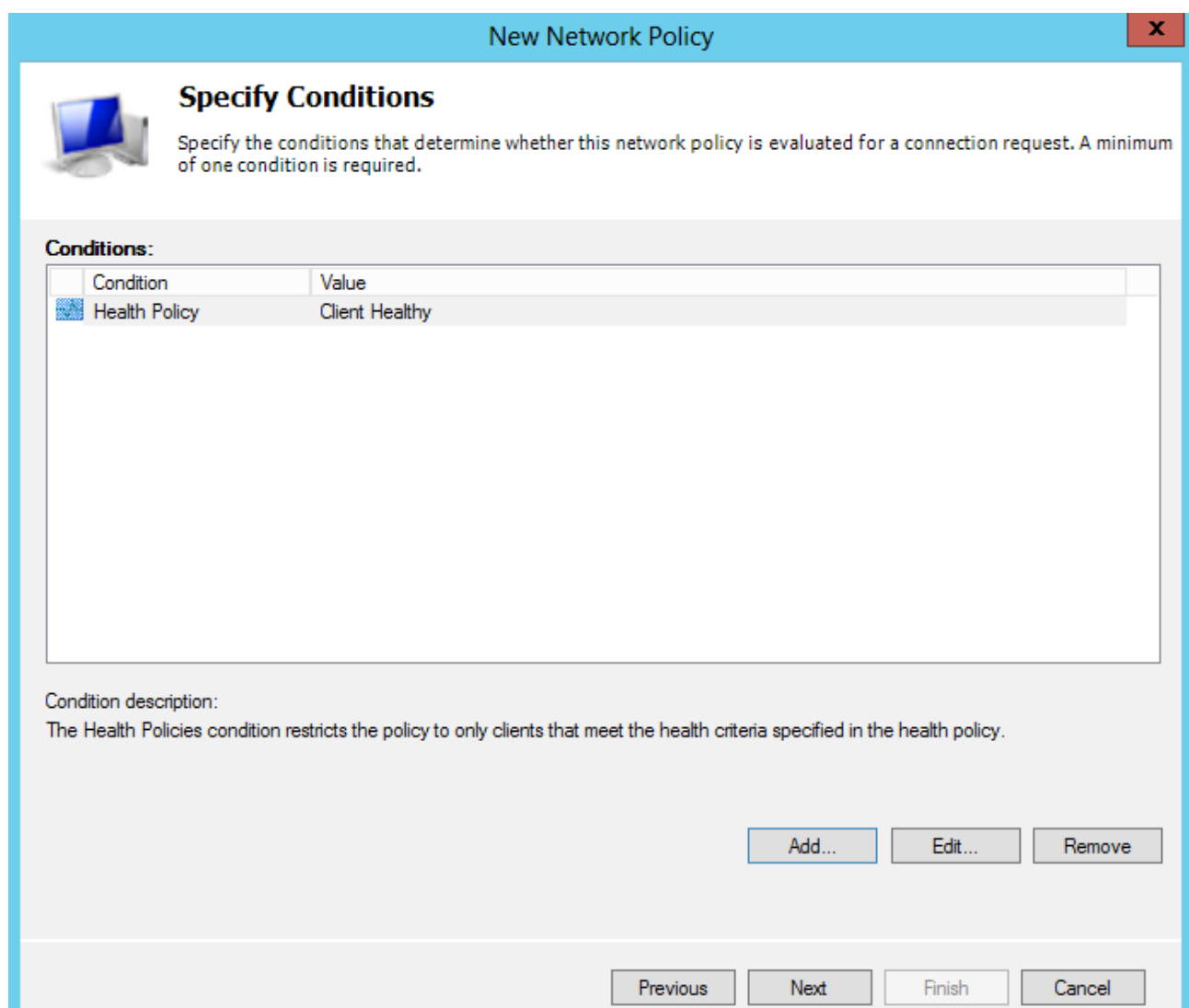
- Identity Type**
The Identity Type condition restricts the policy to only clients that can be identified through the specified mechanism, such as NAP statement of health (SoH).
- MS-Service Class**
The MS-Service Class condition specifies that the connecting computer must have an IP address lease from a DHCP scope that matches the selected profile name.
- Health Policies**
The Health Policies condition restricts the policy to only clients that meet the health criteria specified in the health policy.
- NAP-Capable Computers**
The NAP-Capable Computers condition specifies that connecting computers either are or are not capable of participating in NAP. This capability is determined by whether the client computer sends a statement of health to NPS.

Add... Cancel

5 Select the “Client Healthy” policy, then click to the OK button




6 We do not have any other condition so click to the Next button.



7 Specify “Access granted” as permission, then click to the next button

New Network Policy X



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous


Next

Finish

Cancel

8 On the “Configure Authentication Methods” window select “Perform machine health check only”, then click to the next button

New Network Policy



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

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

Previous


Next

Finish

Cancel

9 On the “Configure constraints” window click to the next button

New Network Policy




Configure Constraints


Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.


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


Constraints:


Constraints

 Idle Timeout

 Session Timeout

 Called Station ID

 Day and time restrictions

 NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

^

v

Previous


Next

Finish

Cancel

10 On the “Configure Settings” window select “Nap enforcement”, and there the “Allow full network access”, then click to the next button.

New Network Policy




Configure Settings


NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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


Settings:


RADIUS Attributes

 Standard


 Vendor Specific


Network Access Protection


 NAP Enforcement


 Extended State

Routing and Remote Access

 Multilink and Bandwidth Allocation Protocol (BAP)

 IP Filters

 Encryption

 IP Settings

Specify whether you want to enforce Network Access Protection for this policy.

☒ Allow full network access

Allows unrestricted network access for clients when the connection request matches the policy. Use this option for reporting mode.

☐ Allow full network access for a limited time

Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date: Time:

☐ Allow limited access

Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL

To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

Previous

Next

Finish

Cancel

11 On the completing window click to the finish button



Completing New Network Policy

You have successfully created the following network policy:

Healthy clients get network access

Policy conditions:

Condition	Value
Health Policy	Client Healthy

Policy settings:

Condition	Value
Authentication Method	Perform Machine Health Check Only
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous

Next

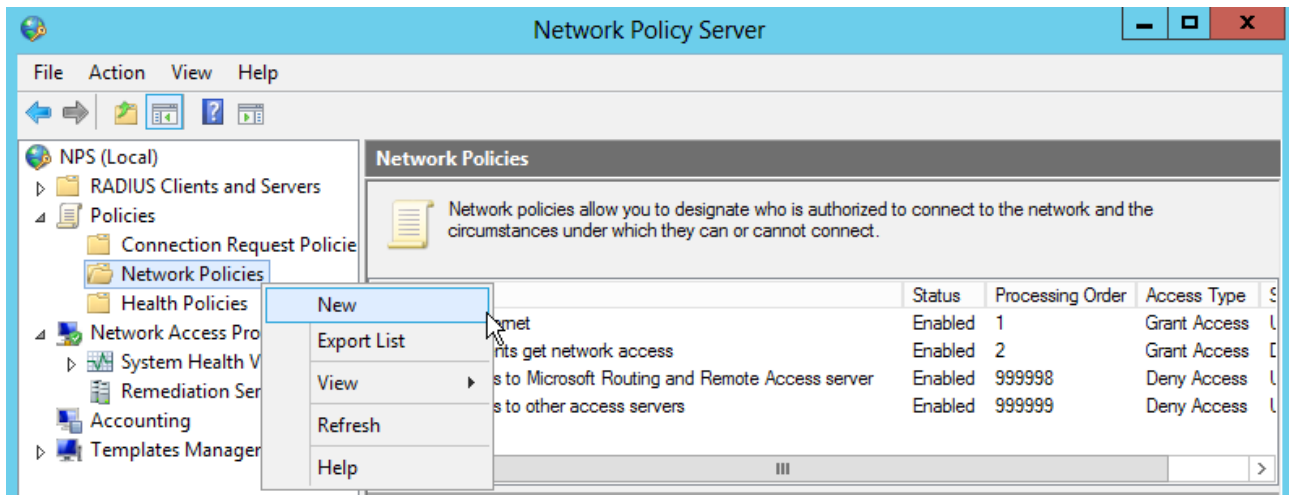
Finish

Cancel

Create the second Network policy for non compliant machines

Now very similarly we create another policy for those computers which fail on the health check. The difference will be only that we allow these computers to communicate only to the remediation servers.


1 right click to the Policies / Network Policies, and from the popup menu select “New”



2 Give some name to the policy, and select “DHCP Server” as “Type of network access server”, then click to the “Next” button.

New Network Policy

X



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

NOT healthy clients get LIMITED access

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, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

DHCP Server

☐ Vendor specific:

10

Previous


Next

Finish

Cancel

3 on the specify condition window click to the “Add...” button

New Network Policy



Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value

Condition description:

Add...
Edit...
Remove


Previous
Next
Finish
Cancel

4 Select “Health Policies” as condition type then click to the “Add...” button

Select condition


Select a condition, and then click Add.

Network Access Protection




Identity Type

The Identity Type condition restricts the policy to only clients that can be identified through the specified mechanism, such as NAP statement of health (SoH).




MS-Service Class

The MS-Service Class condition specifies that the connecting computer must have an IP address lease from a DHCP scope that matches the selected profile name.



Health Policies

The Health Policies condition restricts the policy to only clients that meet the health criteria specified in the health policy.

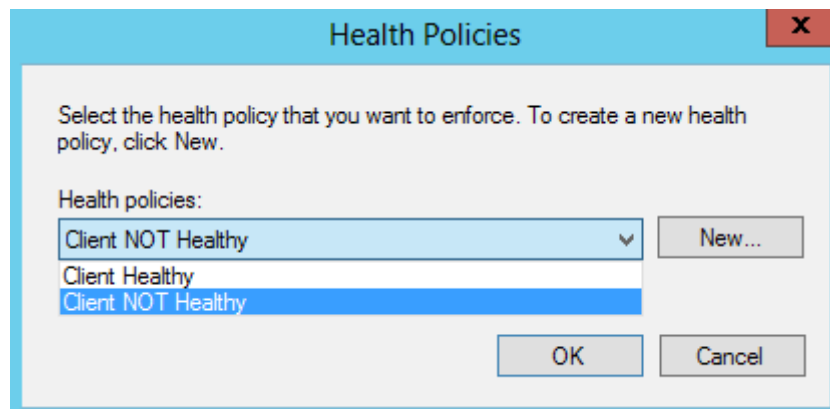


NAP-Capable Computers

The NAP-Capable Computers condition specifies that connecting computers either are or are not capable of participating in NAP. This capability is determined by whether the client computer sends a statement of health to NPS.

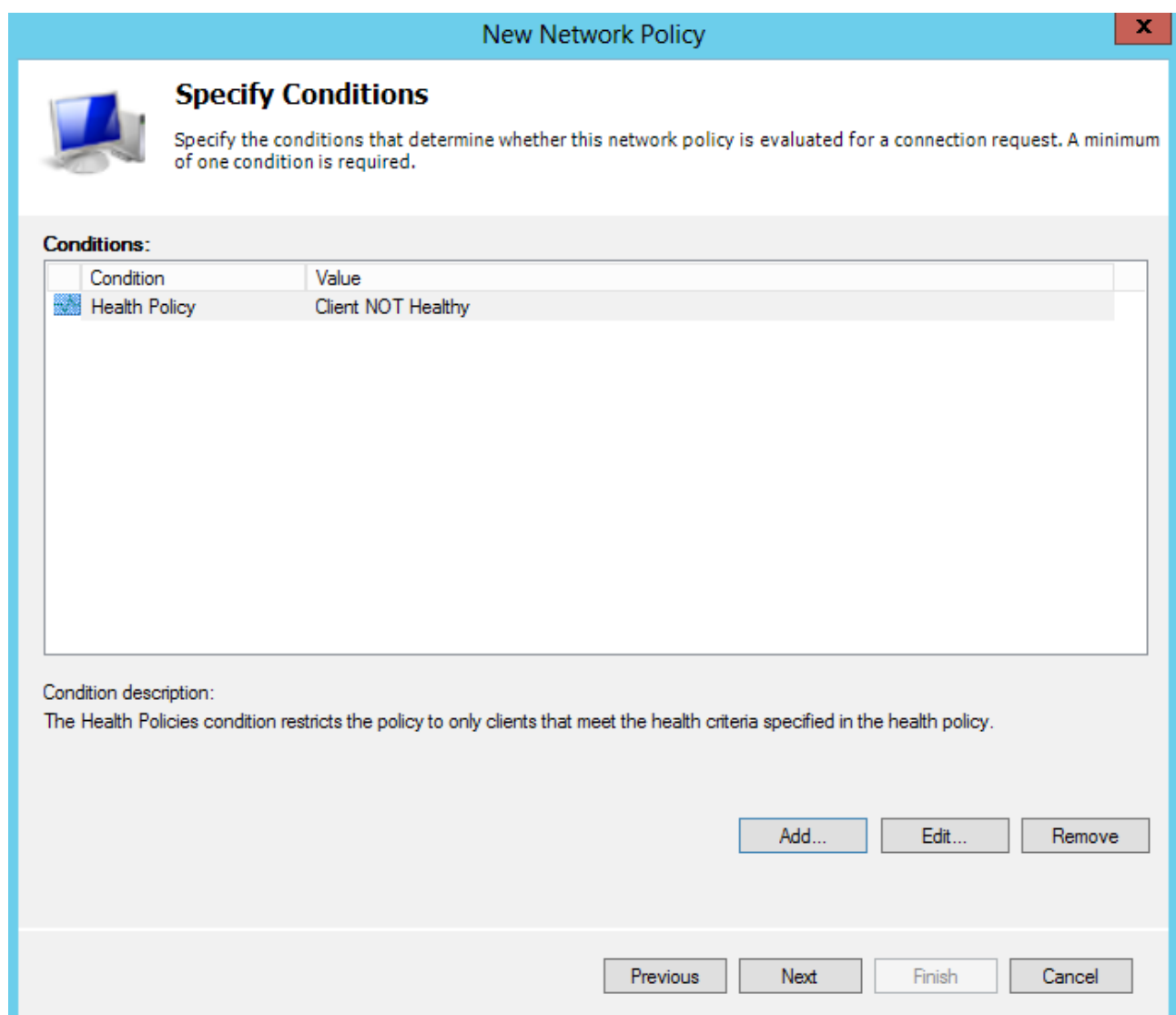
Add...
Cancel

5 Select the “Client NOT Healthy” policy, then click to the OK button



The "Health Policies" dialog box has a title bar with a close button (X). The main area contains the text: "Select the health policy that you want to enforce. To create a new health policy, click New." Below this, there is a label "Health policies:" followed by a dropdown menu. The dropdown menu is open, showing three options: "Client NOT Healthy" (selected), "Client Healthy", and "Client NOT Healthy". To the right of the dropdown is a "New..." button. At the bottom right are "OK" and "Cancel" buttons.

6 We do not have any other condition so click to the Next button.




The "New Network Policy" dialog box has a title bar with a close button (X). The main area has a sub-header "Specify Conditions" with a computer icon. Below the icon is the text: "Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required." Below this is a section labeled "Conditions:" containing a table.

Condition	Value
Health Policy	Client NOT Healthy

Below the table is a "Condition description:" section with the text: "The Health Policies condition restricts the policy to only clients that meet the health criteria specified in the health policy." At the bottom right are three buttons: "Add...", "Edit...", and "Remove". At the very bottom are four buttons: "Previous", "Next", "Finish", and "Cancel".

7 Specify “Access granted” as permission, then click to the next button

New Network Policy ✕



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.


☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

8 On the “Configure Authentication Methods” window select “Perform machine health check only”, then click to the next button

New Network Policy



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Move Up

Move Down

Add...Edit...Remove

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

Previous


Next

Finish

Cancel

9 On the “Configure constraints” window click to the next button

New Network Policy




Configure Constraints


Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.


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


Constraints:


Constraints

 Idle Timeout

 Session Timeout

 Called Station ID

 Day and time restrictions

 NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

^

v

Previous

Next

Finish

Cancel

10 On the “Configure Settings” window select “Nap enforcement”, and there the “Allow limited access”, then click to the configure button.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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

Settings:

RADIUS Attributes

- Standard
- ☒ Vendor Specific

Network Access Protection

- NAP Enforcement**
- ☒ Extended State

Routing and Remote Access

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- ☒ IP Settings

☐ Allow full network access for a limited time

Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date:

Time:

☒ Allow limited access

Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL

To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

[Configure...](#)

Auto remediation

☐ Enable auto-remediation of client computers

Automatically remediate computers that do not meet health requirements defined in this policy.

[Previous](#)
[Next](#)
[Finish](#)
[Cancel](#)

11 Select the Remediation server group, because we want these computers to be reached by the non compliant computers.

Remediation Servers and Troubleshooting URL

Remediation Server Group

Select the remediation servers that you would like to provide to computers with limited network access.

▼

[New Group...](#)

Troubleshooting URL

Specify a Web page address Uniform Resource Locator (URL) that provides instructions to users on how to bring computers and devices into compliance with your network access policy.

[OK](#)
[Cancel](#)

12 On the completing window click to the finish button

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

NOT healthy clients get LIMITED access

Policy conditions:

Condition	Value
Health Policy	Client NOT Healthy

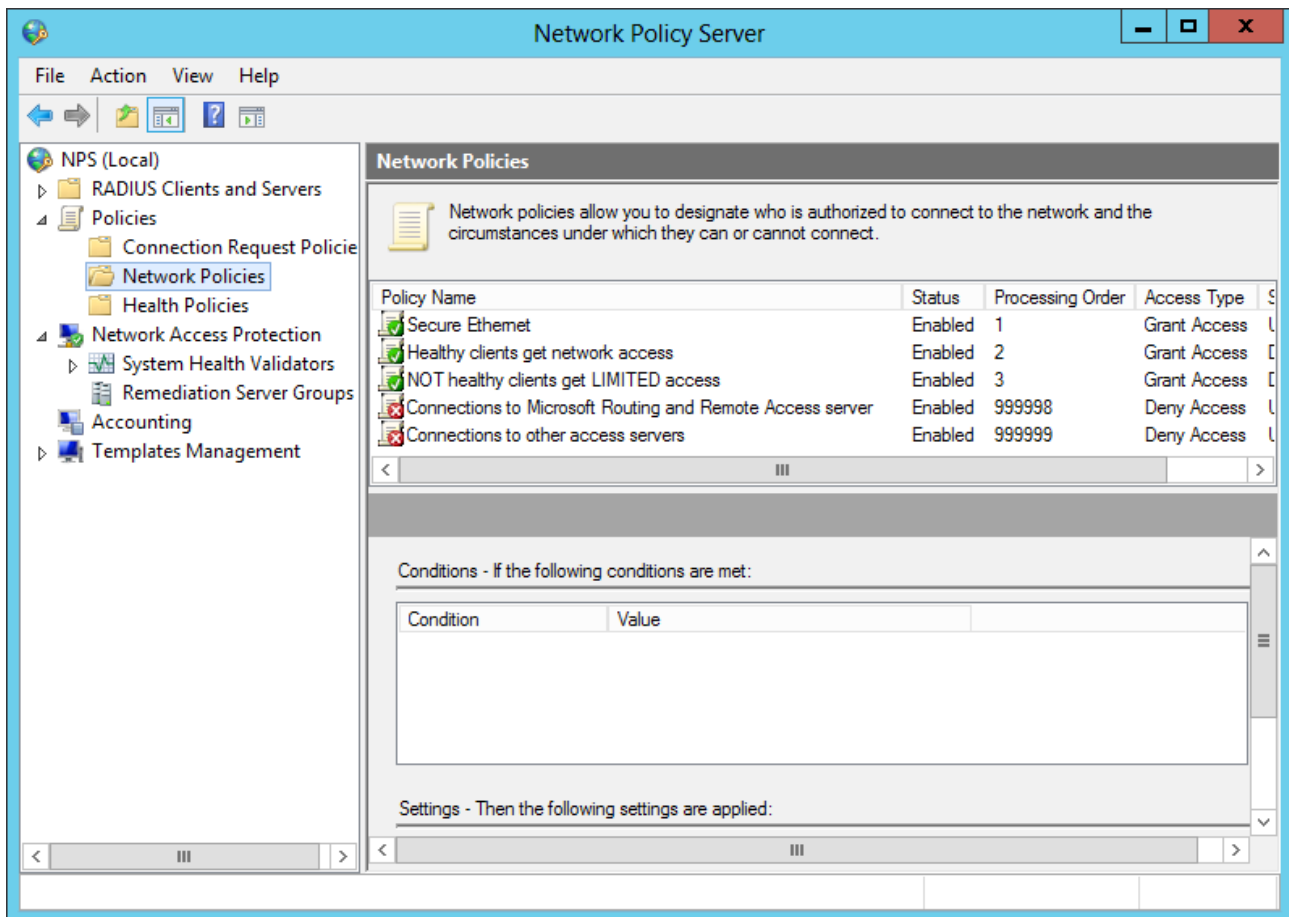
Policy settings:

Condition	Value
Authentication Method	Perform Machine Health Check Only
Access Permission	Grant Access
Update Noncompliant Clients	False
NAP Enforcement	Allow limited network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous Next Finish Cancel

13 Check the two newly created policies



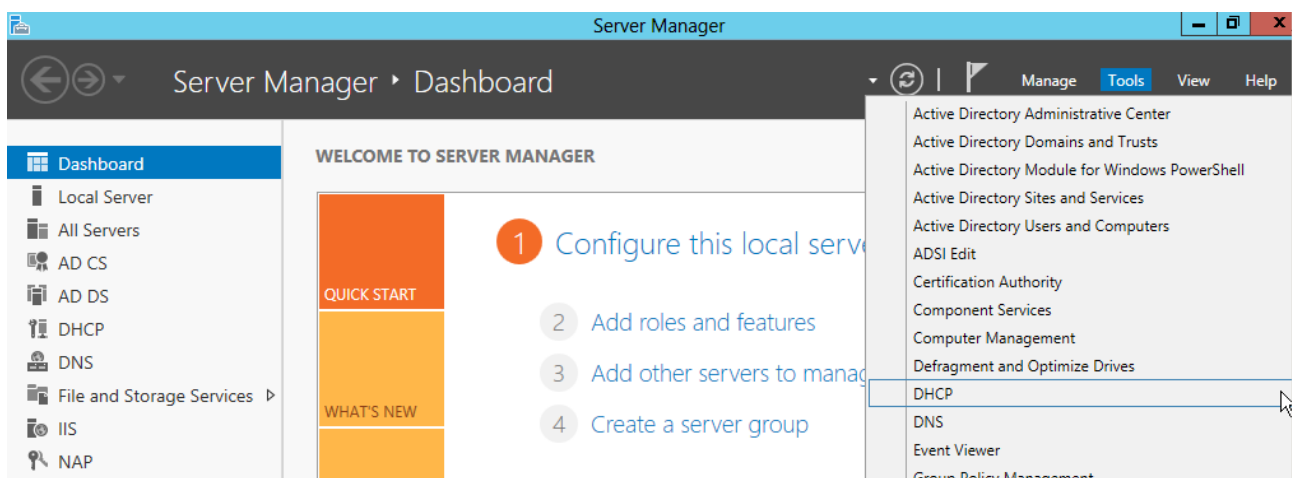
NAP with 802.1x enforce

Previously we created a NAP enforcement with DHCP. It is good for testing purposes, because easy to configure, and used to work fine, but from security point of view it is nothing. It can be easily bypassed by setting up a static IP address to our computers. So in real environment some better enforcement are required. One can be the 802.1x enforcement. Let us see how it can be configured

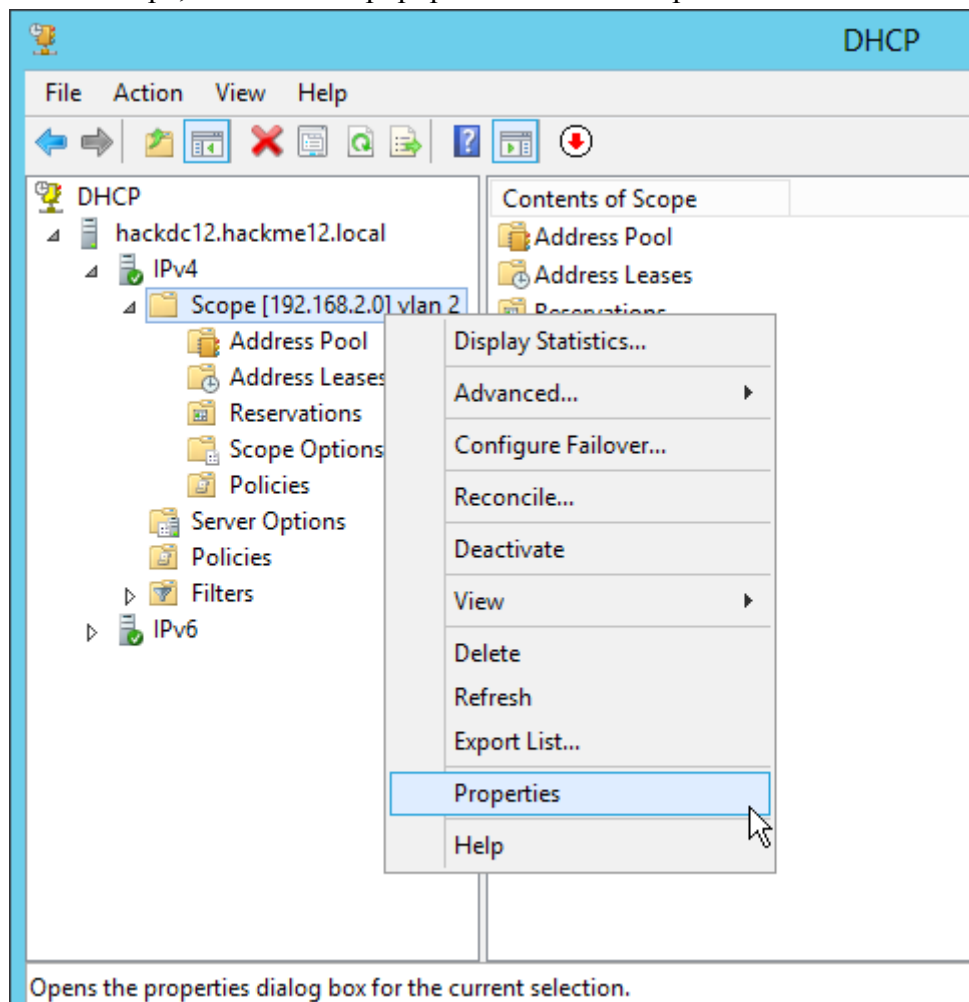
Turn off the NAP on the DHCP scope

First turn off the previously created DHCP enforcement, just to do not have any side effect.

1 Start the DHCP management console



2 Right click to the scope, and from the popup menu select “Properties”



3 navigate to the “Network Access Protection” tab, and disable the NAP for this scope.

The screenshot shows a Windows-style dialog box titled "Scope [192.168.2.0] vlan 2 Properties". It has four tabs: "General", "DNS", "Network Access Protection" (which is selected), and "Advanced". The "Network Access Protection" tab contains a section titled "Network Access Protection" with the text "You can setup the Network Access Protection settings for this scope here." Below this is a "Network Access Protection Settings" section. It has two radio buttons: "Enable for this scope" (which is unselected) and "Disable for this scope" (which is selected). Under the "Enable for this scope" option, there are two sub-options: "Use default Network Access Protection profile" (selected) and "Use custom profile" (unselected). Below these is a "Profile Name" label and an empty text input field. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Scope [192.168.2.0] vlan 2 Properties

General DNS Network Access Protection Advanced

Network Access Protection

You can setup the Network Access Protection settings for this scope here.

Network Access Protection Settings

☐ Enable for this scope

☒ Use default Network Access Protection profile

☐ Use custom profile

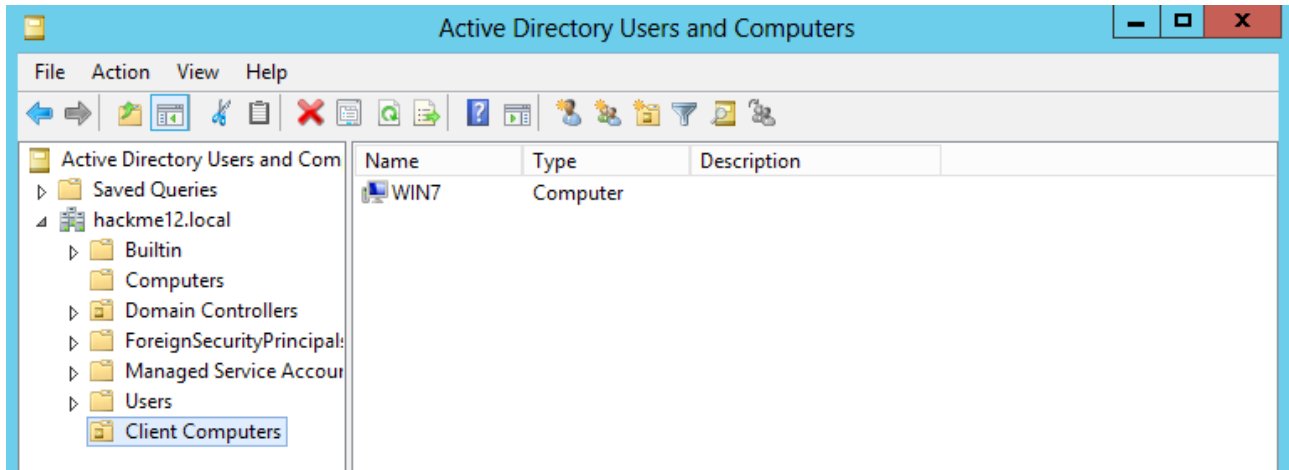
Profile Name

☒ Disable for this scope

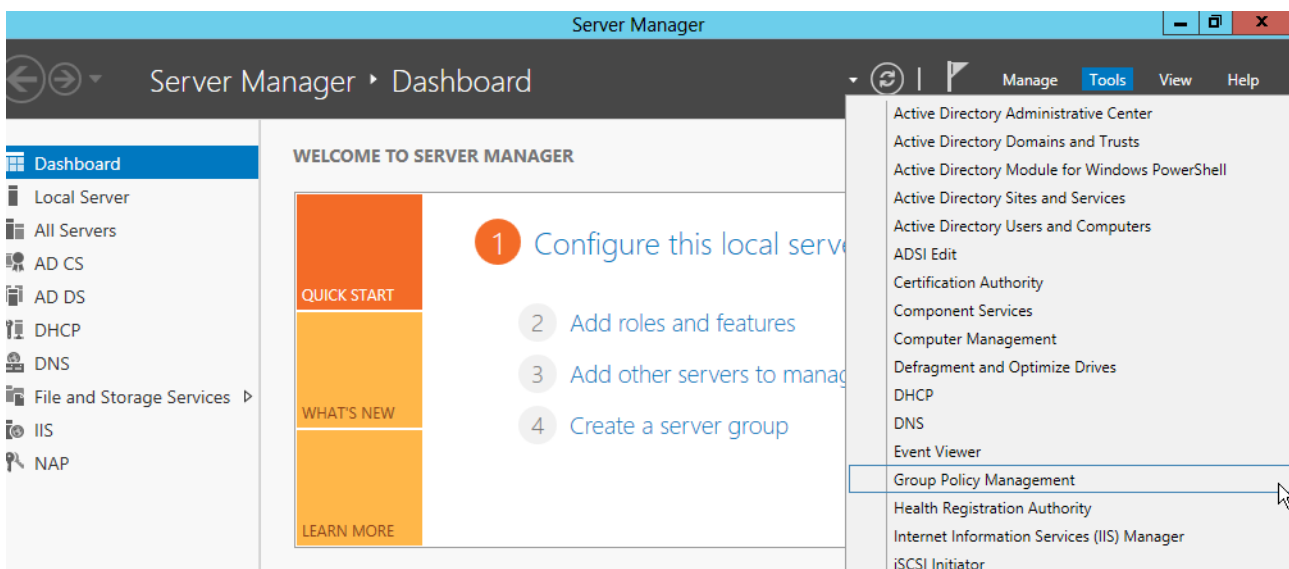
OK Cancel Apply

Enable the EAP Quarantine enforcement client by group policy

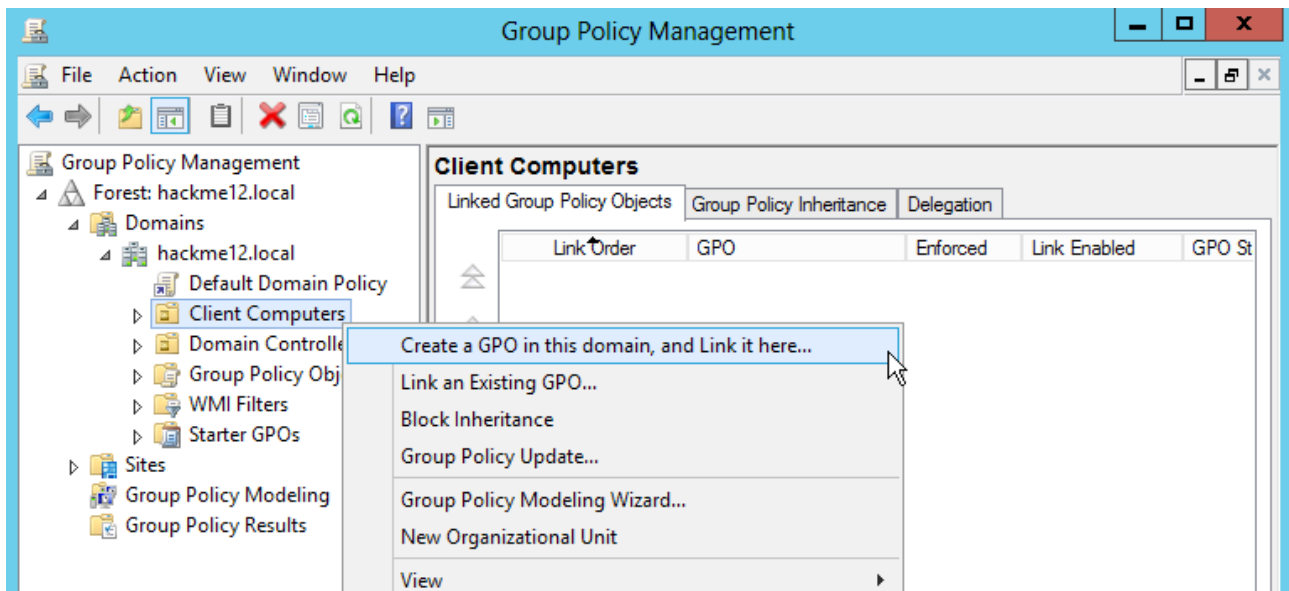
1 Open the “active directory users and computers” console, and create an organization unit for the test computers, then move there the windows 7 machine.



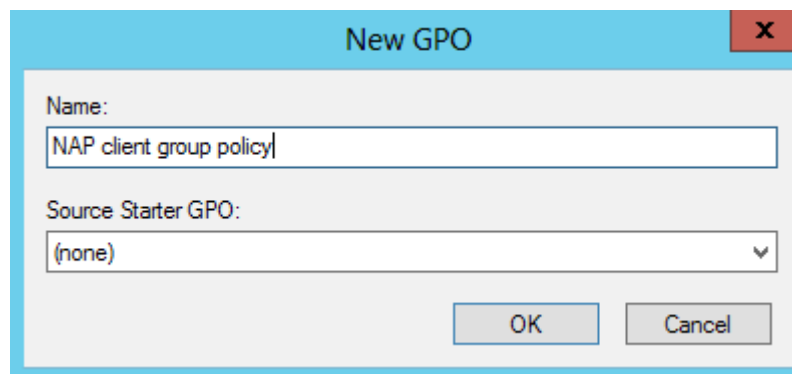
2 start the server manager, and from the tools start the “Group Policy Management Console”



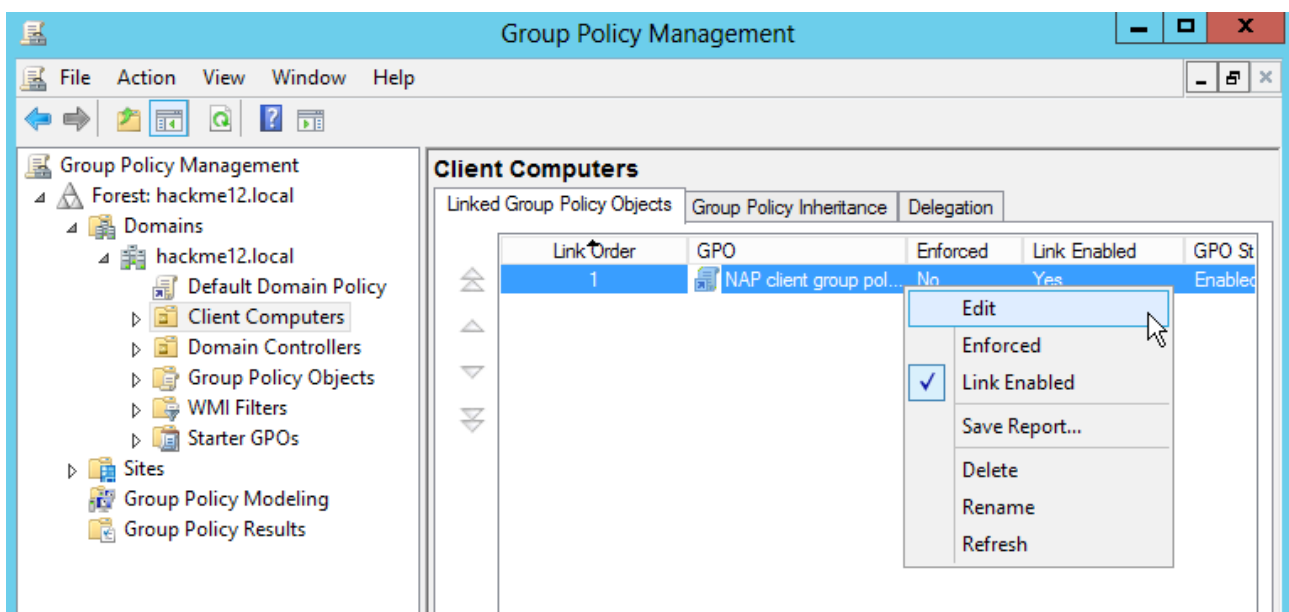
3 find the organization unit contains your test computer. Right click to it, and from the popup menu select the “Create a GPO in this domain, and Link it here...”



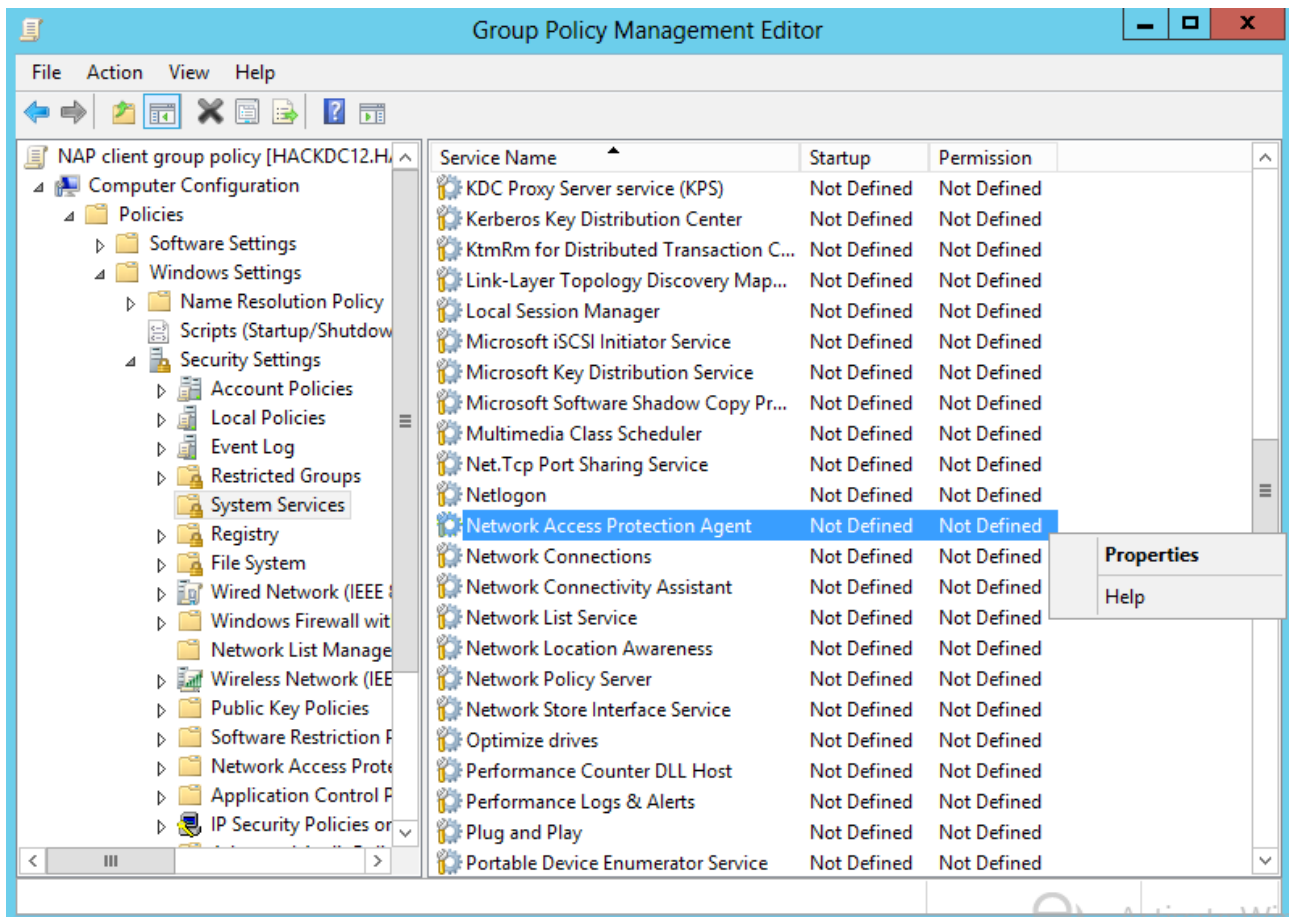
4 Give a name to this group policy, and click to the OK button (we do not use any starter GPO)



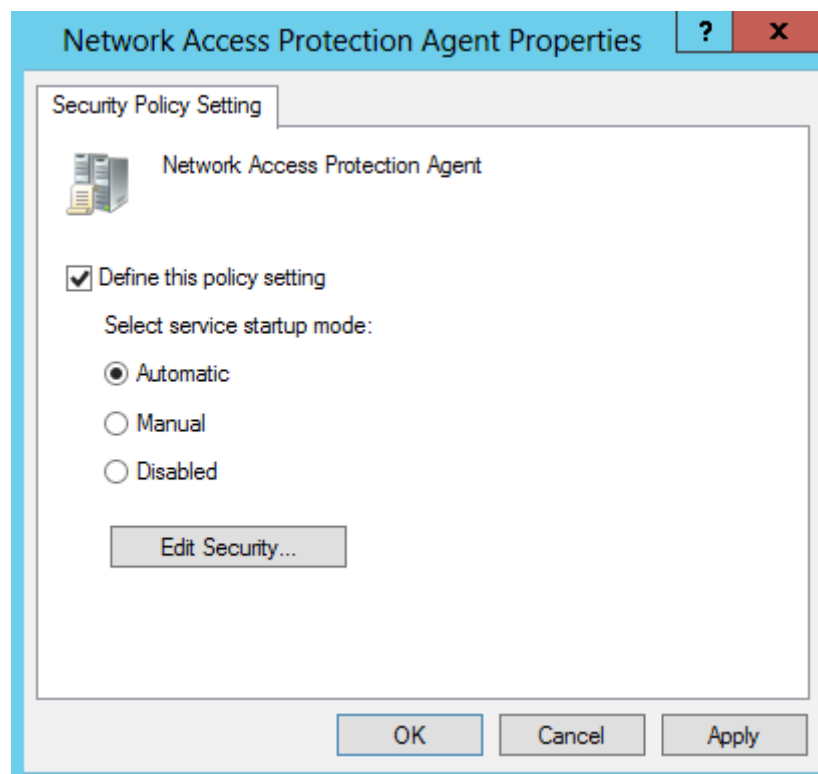
5 Right click to the newly created group policy, and from the popup menu select the Edit command



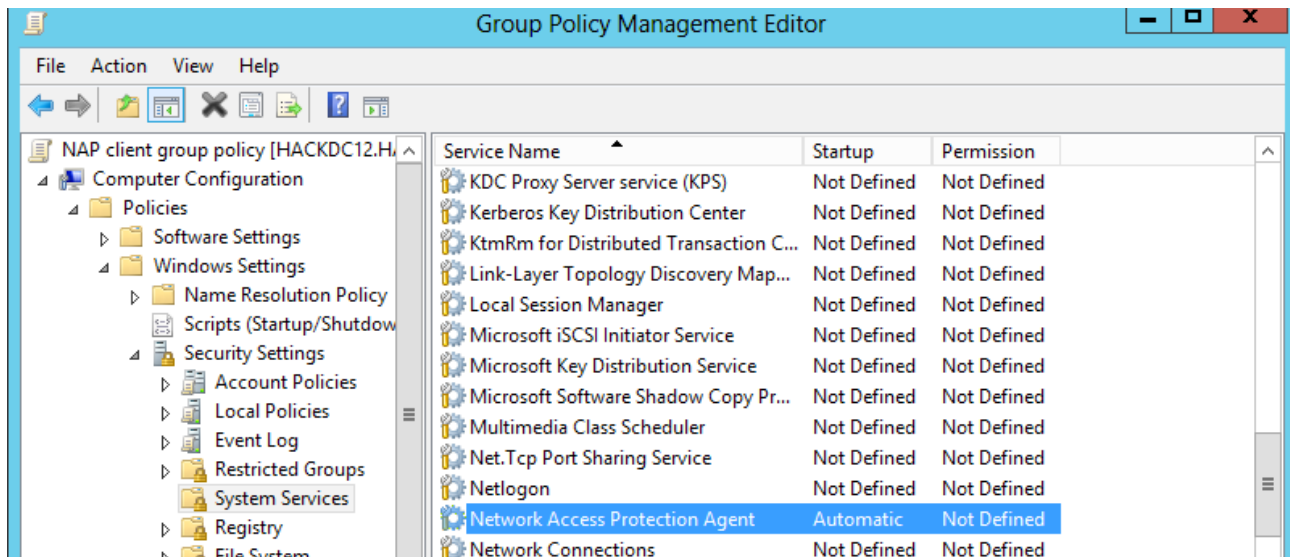
6. Navigate to: computer configuration / Policies / Windows settings / Secure Settings / System Services. Right click to the “Network Access Protection Agent”, and from the popup menu select “Properties”.



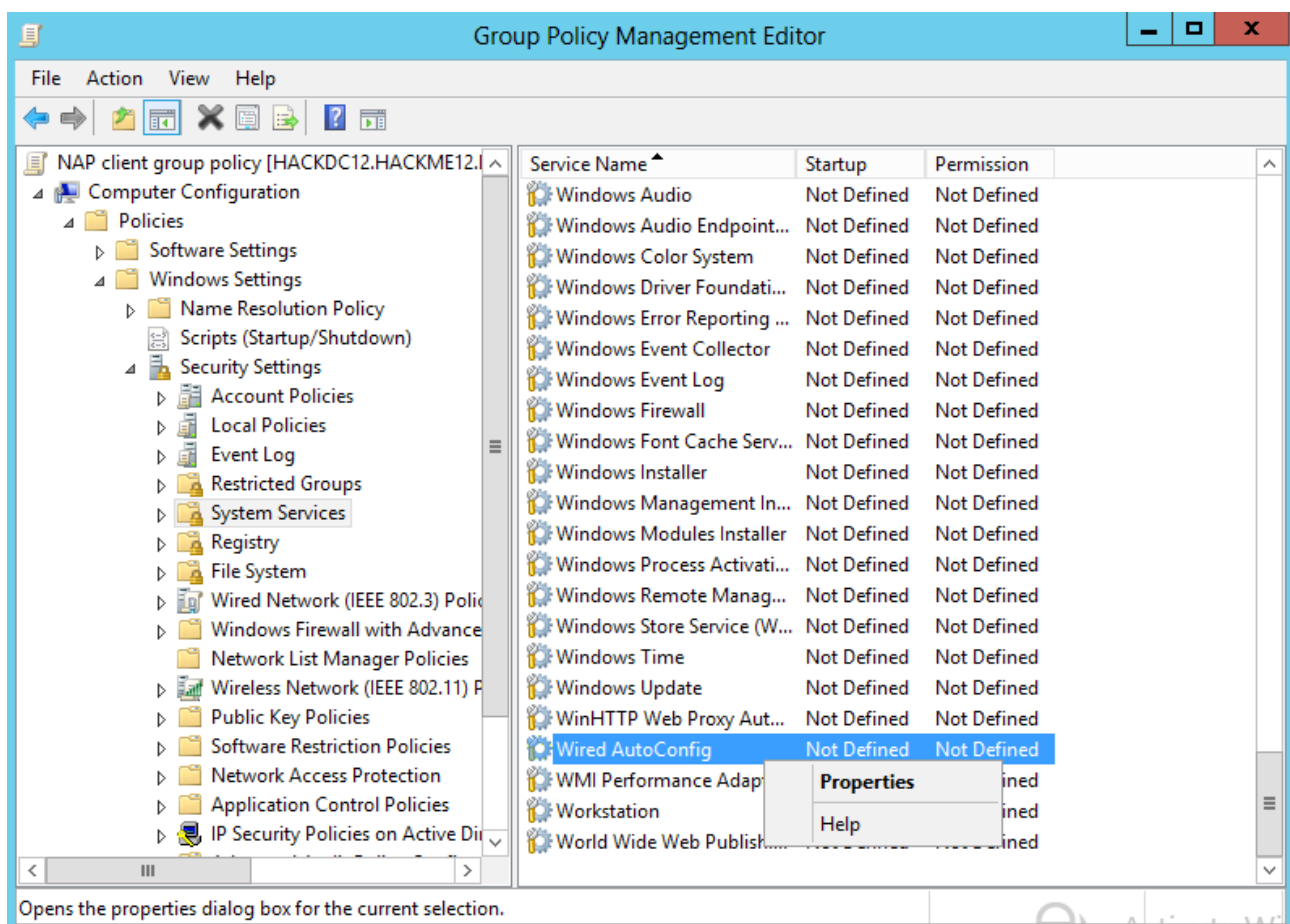
7 Set up the service to Automatic start



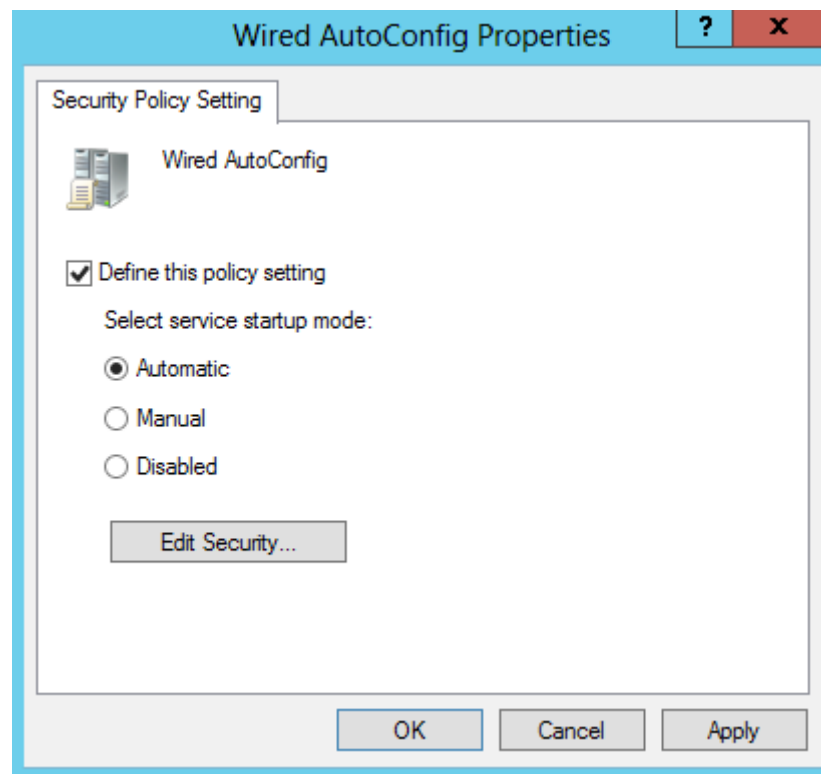
8 check if it really set to automatic



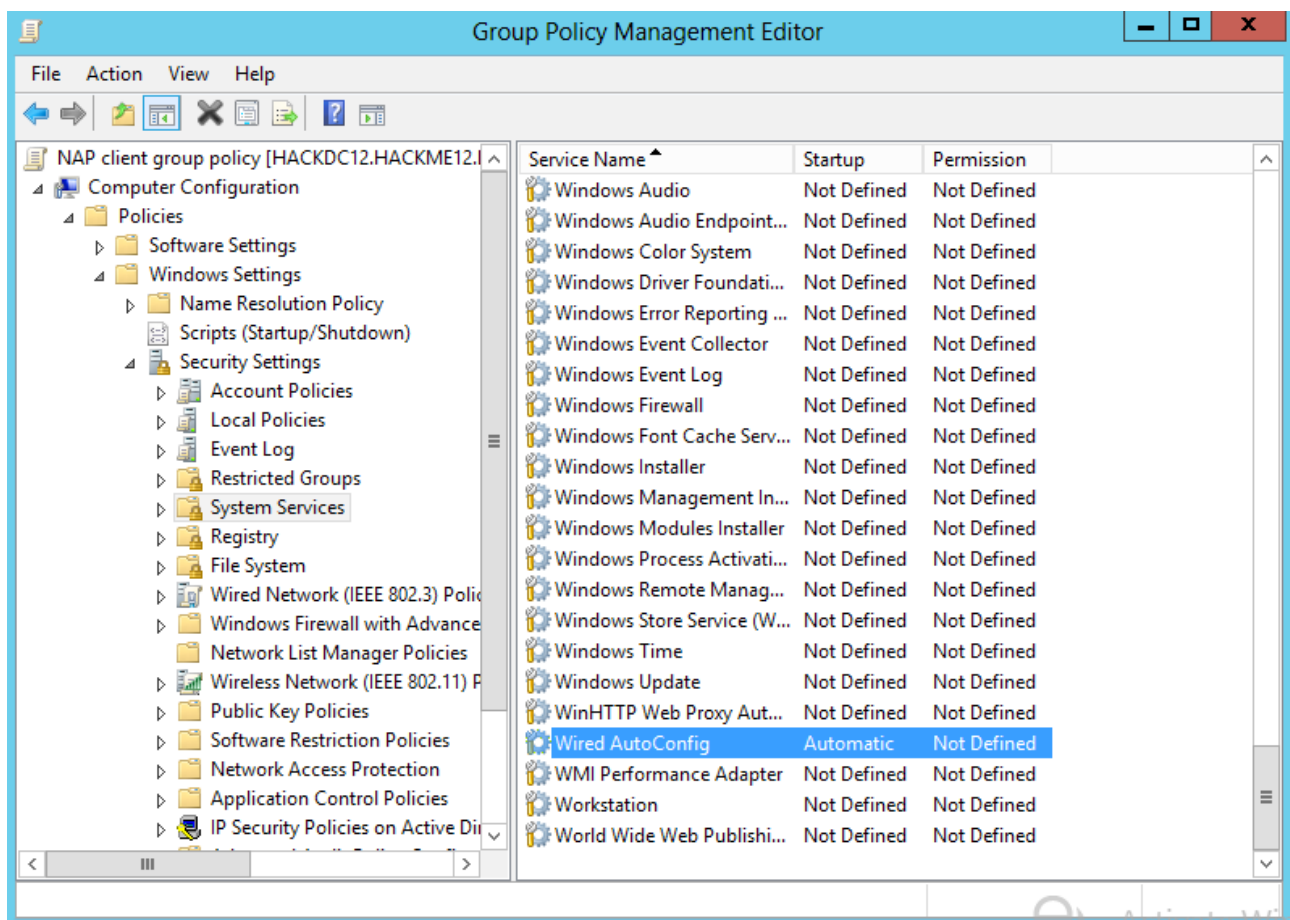
9 Right click to the “Wired AutoConfig”, and from the popup menu select “Properties”.



10 Set up the service to Automatic start

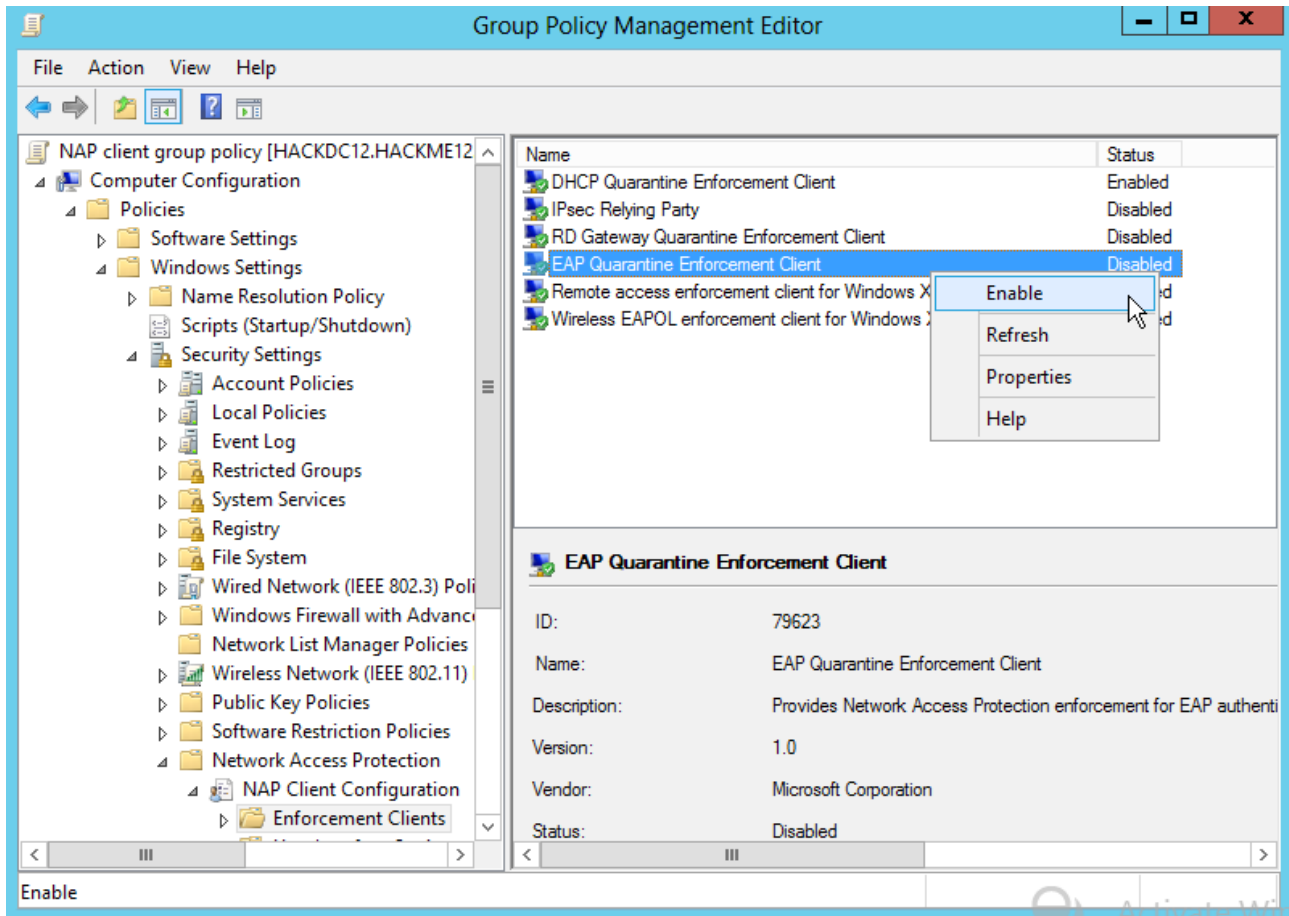


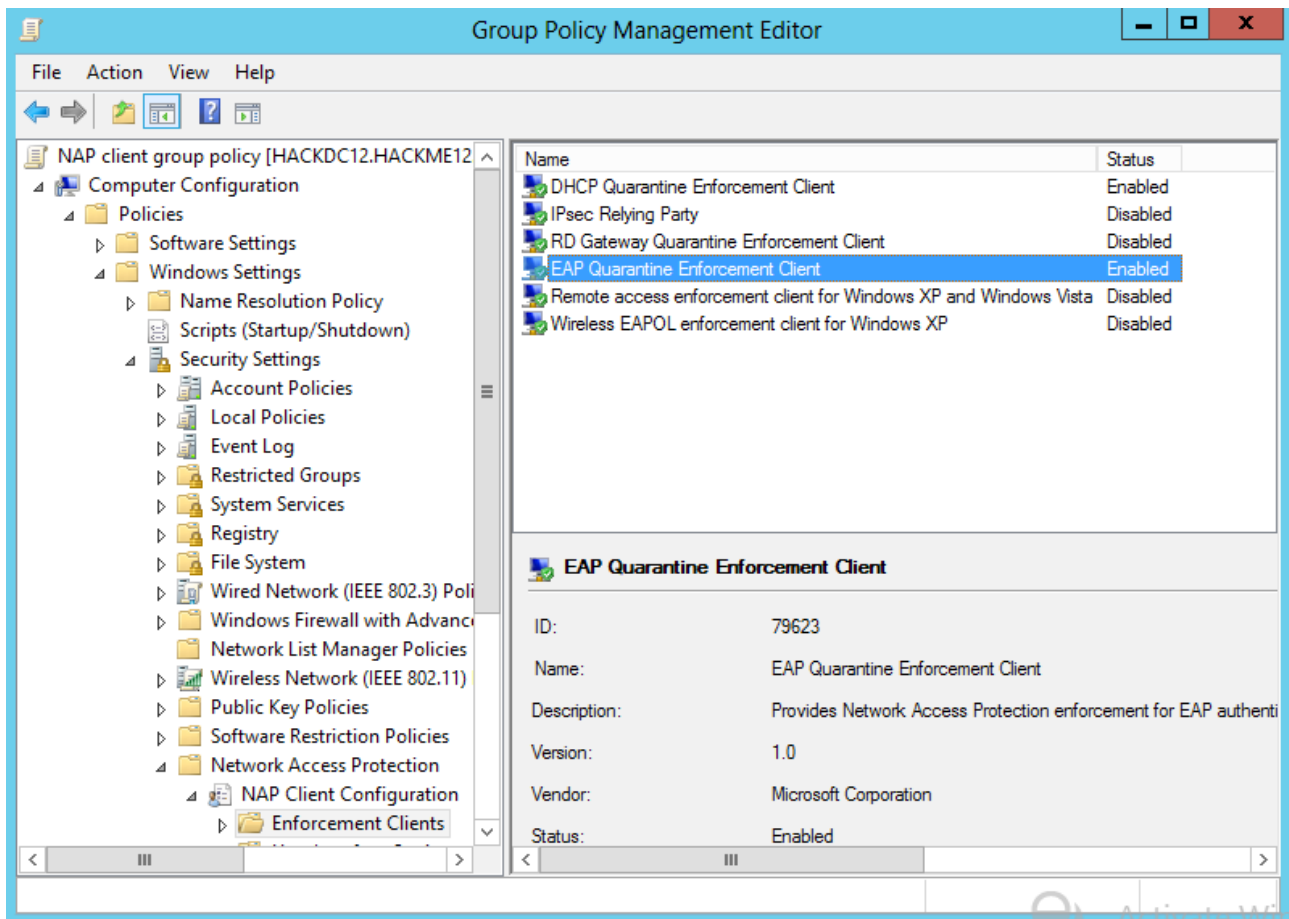
11 check if it really set to automatic



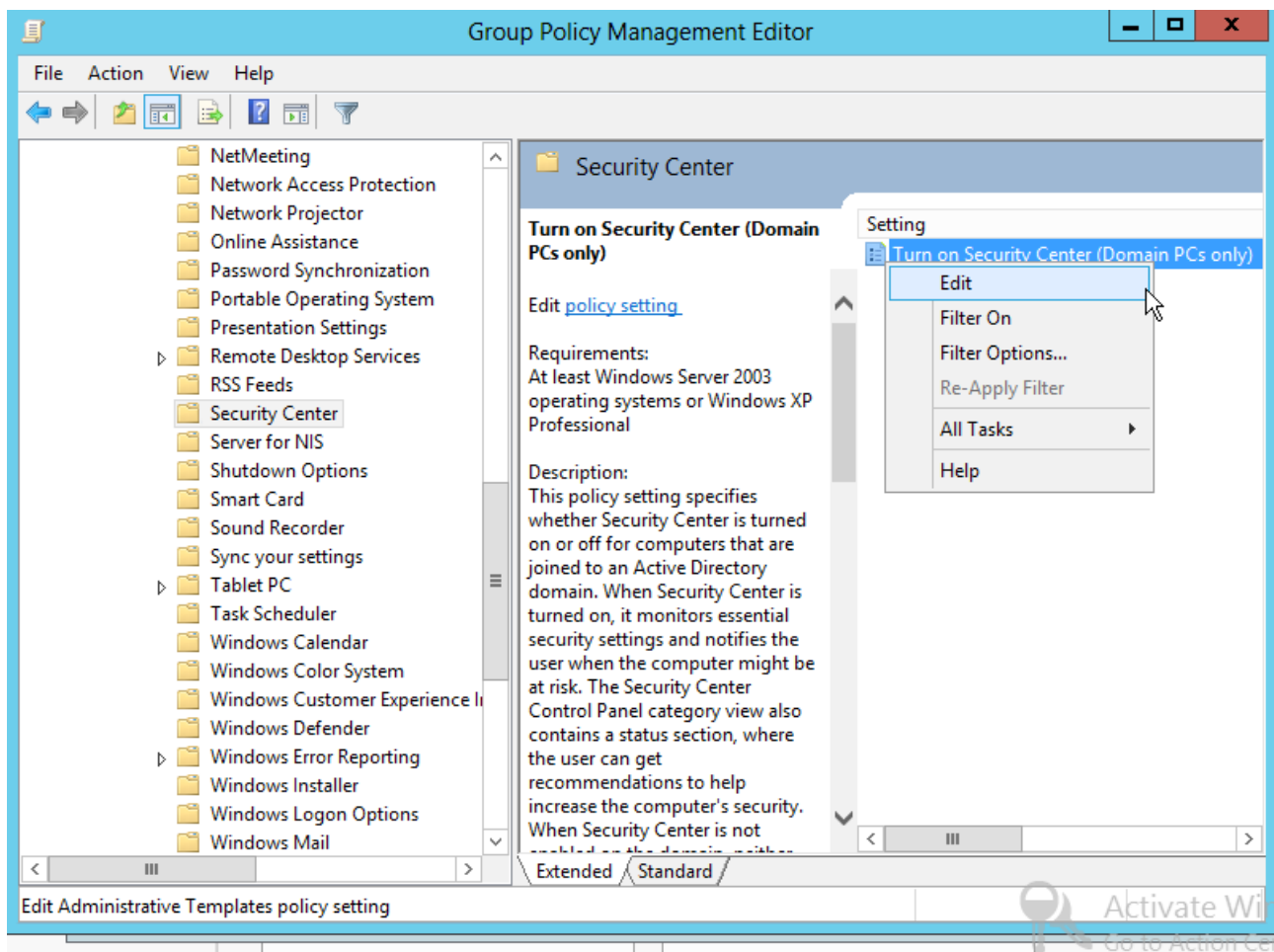
12 Navigate to: computer configuration / Policies / Windows settings / Secure Settings / Network Access Protection / Enforcement Clients. Right click to the “EAP Quarantine Enforcement Client”,

and from the popup menu select “Enable”.





14 Navigate to: computer configuration / Policies / Administrative templates / Security Center. Right click to the “Turn on security center (Domain computers only)”, and from the popup menu select edit.



15 enable this policy, and click to the OK.

Turn on Security Center (Domain PCs only)

Turn on Security Center (Domain PCs only)

Previous SettingNext Setting

☐ Not Configured

☒ Enabled

☐ Disabled

Comment:

Supported on:

At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

This policy setting specifies whether Security Center is turned on or off for computers that are joined to an Active Directory domain. When Security Center is turned on, it monitors essential security settings and notifies the user when the computer might be at risk. The Security Center Control Panel category view also contains a status section, where the user can get recommendations to help increase the computer's security. When Security Center is not enabled on the domain, neither the notifications nor the Security Center status section are displayed.

Note that Security Center can only be turned off for computers that are joined to a Windows domain. When a computer is not joined to a Windows domain, the policy setting will have no effect.

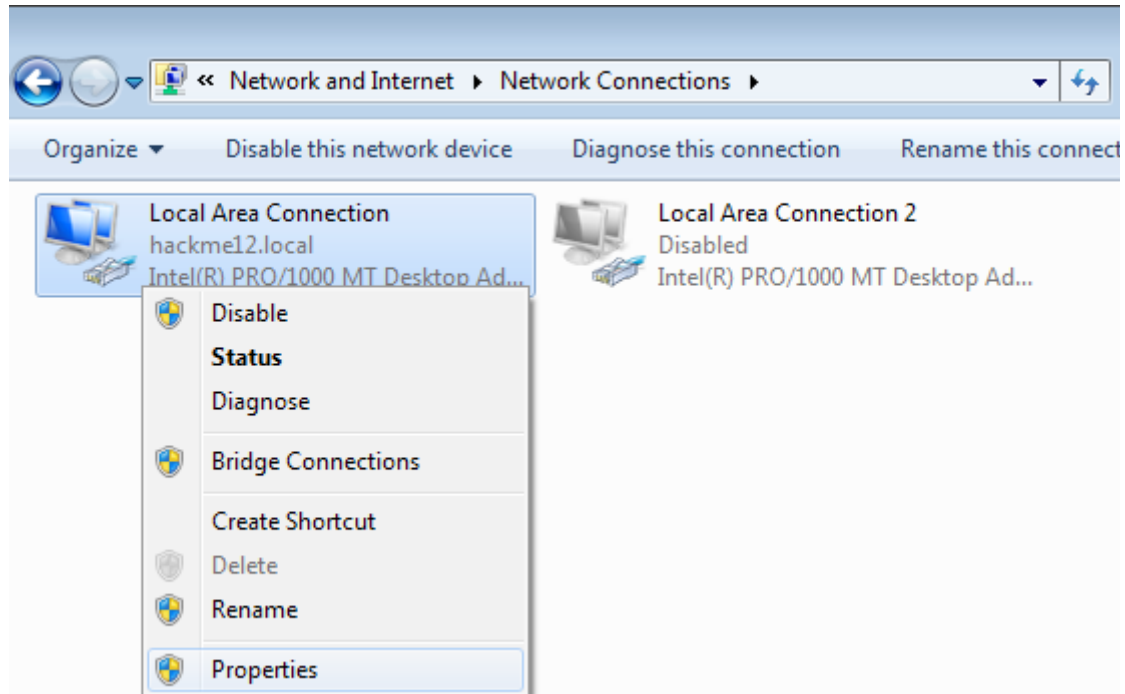
If you do not configure this policy setting, the Security Center is turned off for domain members.

If you enable this policy setting, Security Center is turned on for all users.

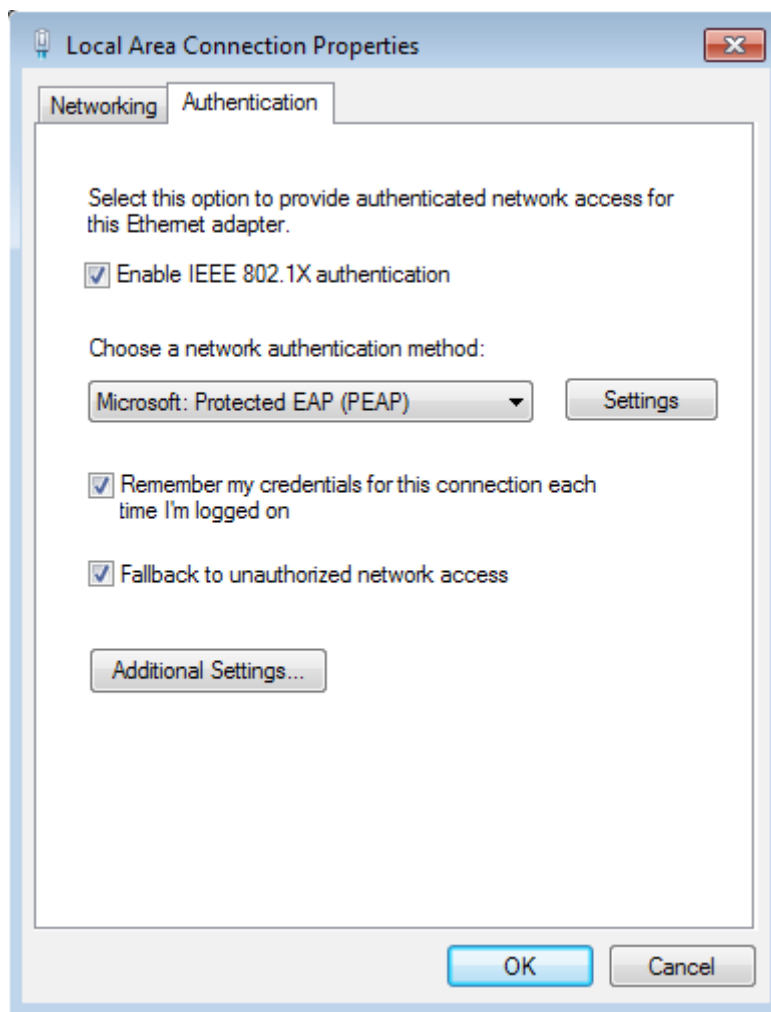
OKCancelApply

Enable the NAP capability on the client computers network card

1 On the client computer navigate to the network connections. Right click to the network card you want to use, and from the popup menu select the properties command



2 go to the authentication tab (if you do not find it then the “Wired AutoConfig” service does not run, we set it up as automatic in the previous group policy part so use a `gpupdate /force` command, reboot the machine, or wait until it applies. Or of course you can start the service by the services snapin in the administrative tools). Put a checkmark to the “Enable IEEE 802.1x authentication”, then click to the settings button next to the “Microsoft: Protected EAP (PEAP)”



3 put a check before the “Enforce Network Access Protection”, then click to the OK.

Protected EAP Properties

When connecting:

☒ Validate server certificate

☒ Connect to these servers:

hackdc12.hackme12.local

Trusted Root Certification Authorities:

☐ Class 3 Public Primary Certification Authority

☐ GeoTrust Global CA

☐ GTE CyberTrust Global Root

☒ hackme12-HACKDC12-CA

☐ Microsoft Root Authority

☐ Microsoft Root Certificate Authority

☐ Thawte Timestamping CA

☐ UTN-USERFirst-Object

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

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

☐ Enable Fast Reconnect

☒ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

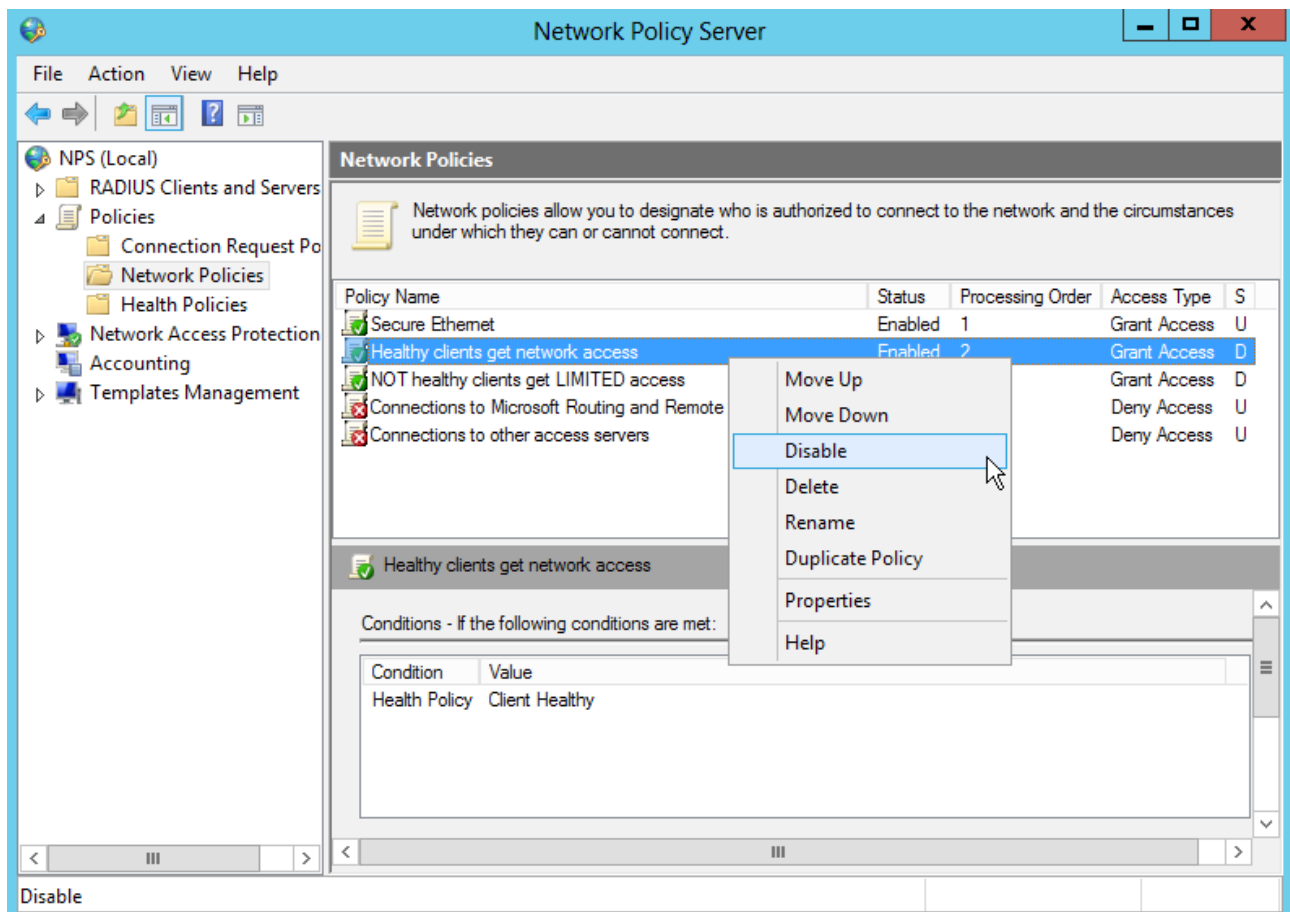
OK Cancel

Set up the NPS server manually

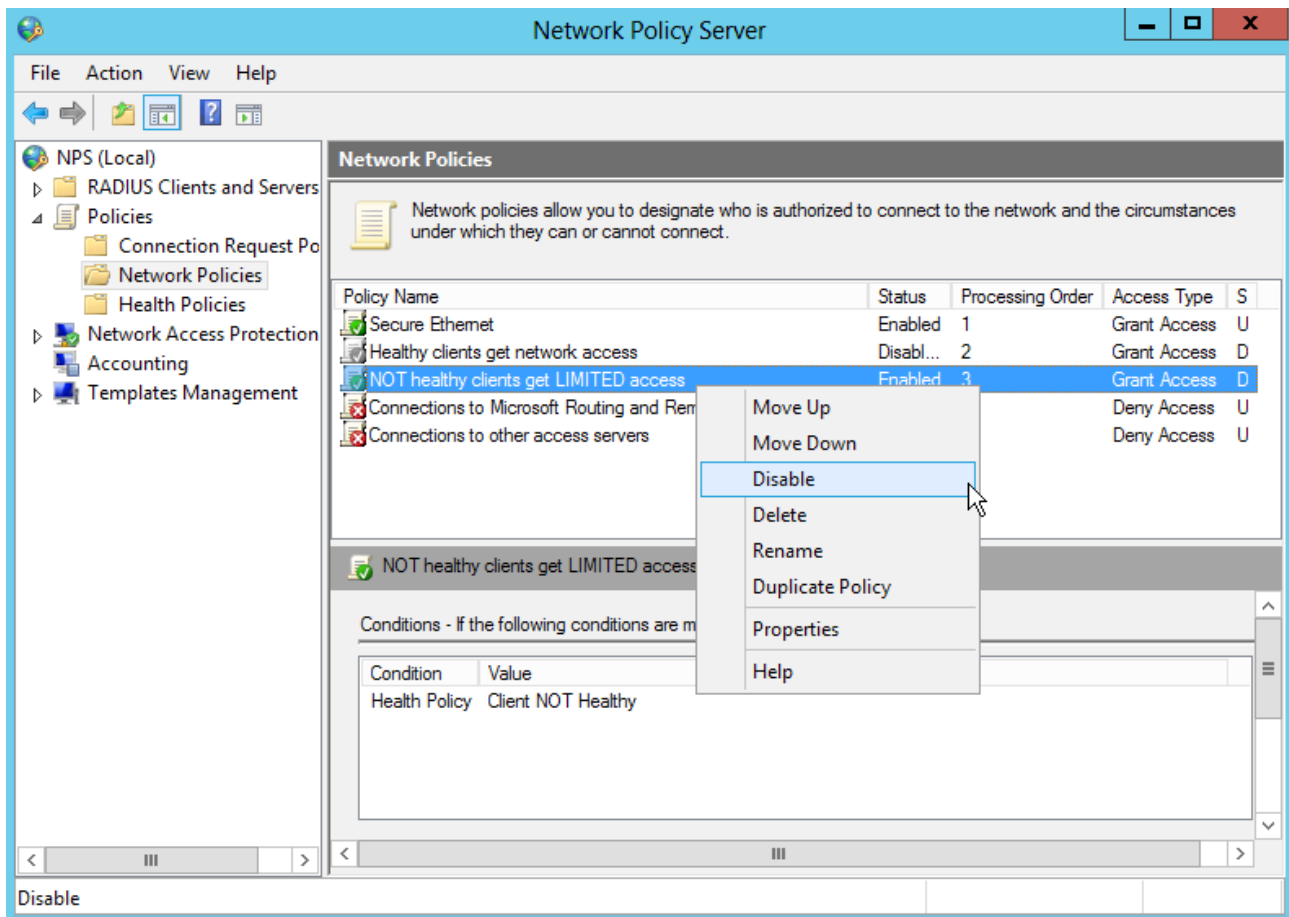
Disable the previous DHCP Network policy rules

We have already disabled the previous DHCP rules on the DHCP server, now we disable the DHCP rules on the NPS server as well.

1 right click to the rule what gives full network access to your healthy clients, and from the popup menu select the “Disable” command



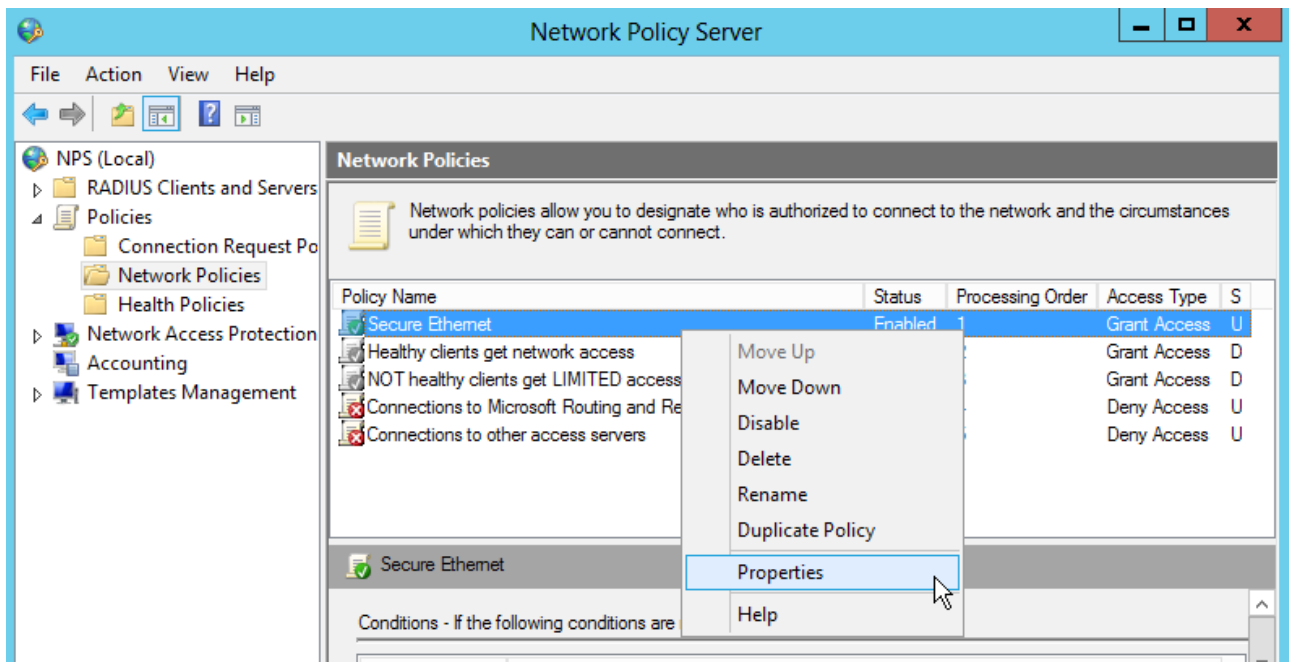
2 similarly right click to the rule what gives limited network access to your non healthy clients, and from the popup menu select the “Disable” command



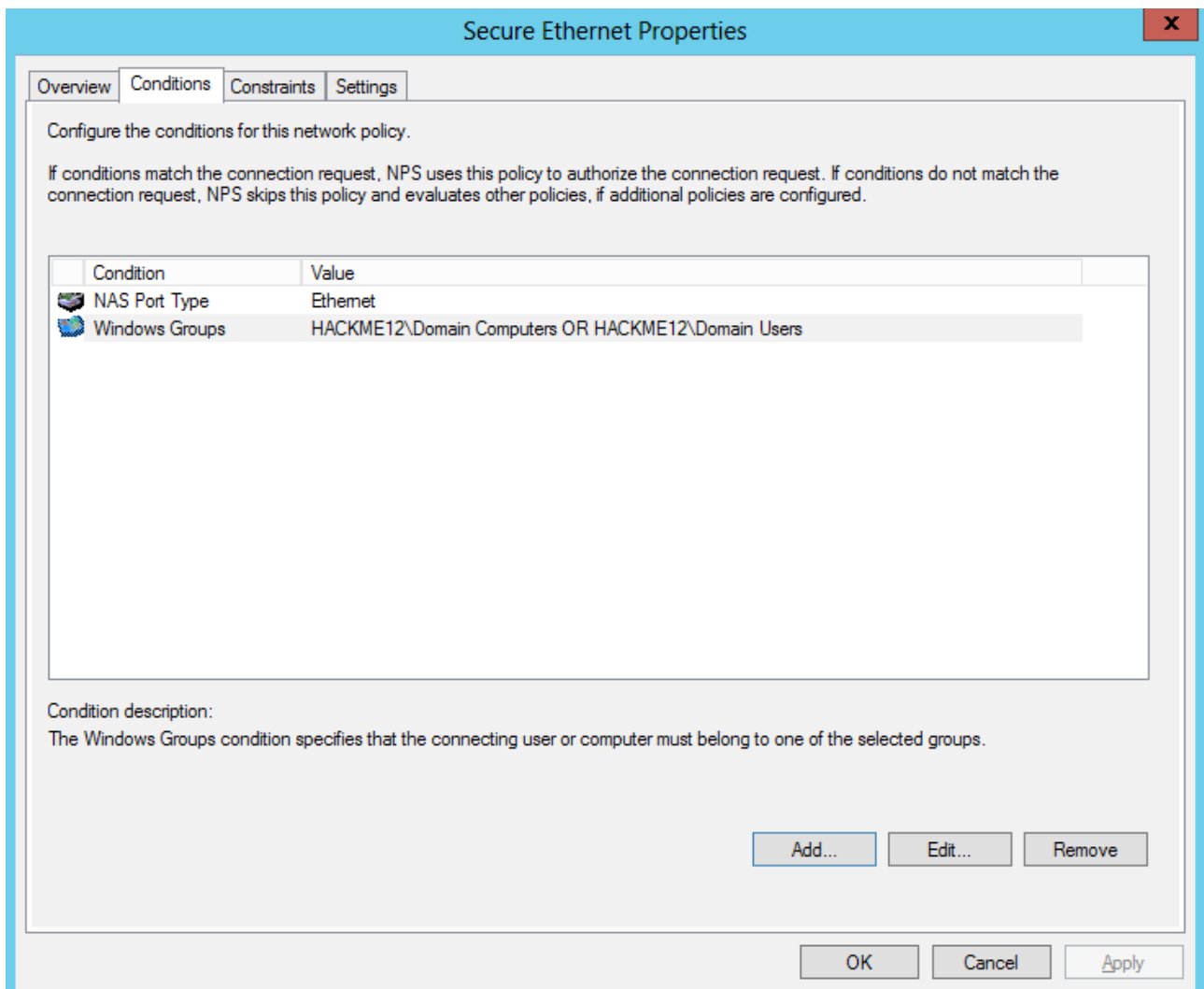
Modify the 802.1x authentication Network Policy, to check the health too

During the first part we created a rule called “Secure Ethernet”, to do the 802.1x network authentication. Now we modify this rule, to request not only user authentication, but check the system health too. We will have to create two rules, one for the compliant machines, and another for the non compliant machines. We create the first one by modifying the already existing rule, then we create a second one.

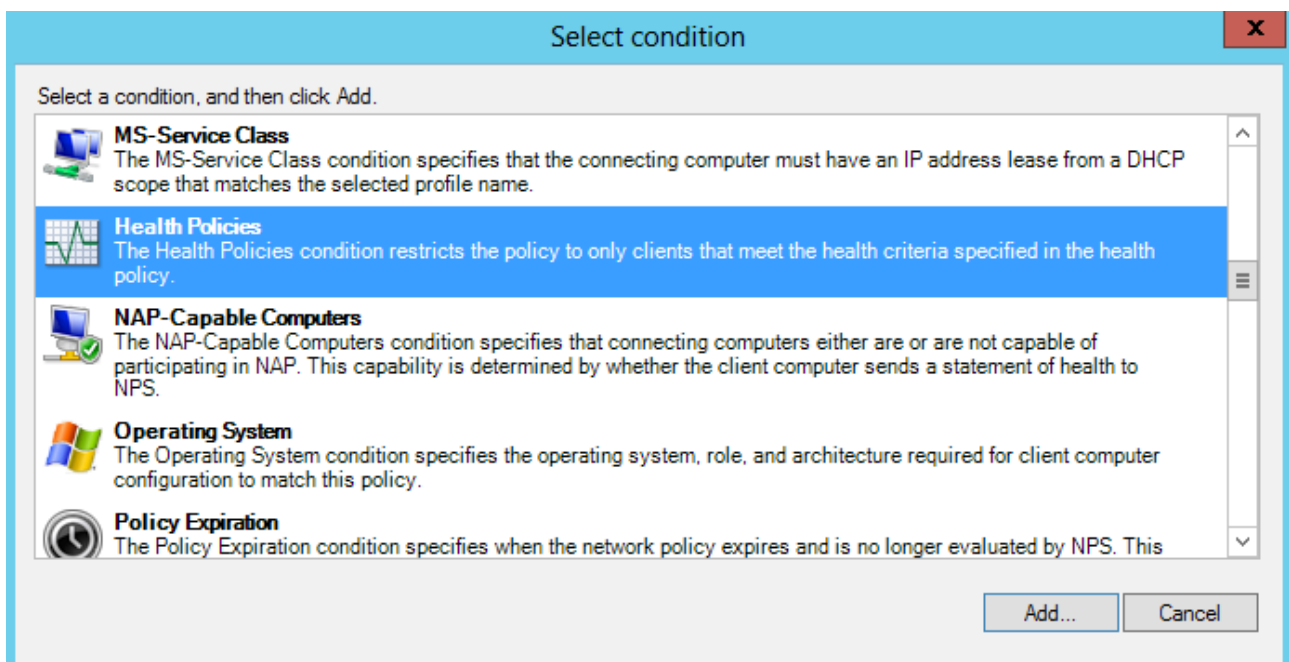
1 right click to the “Secure Ethernet rule”, and select the properties from the popup menu.



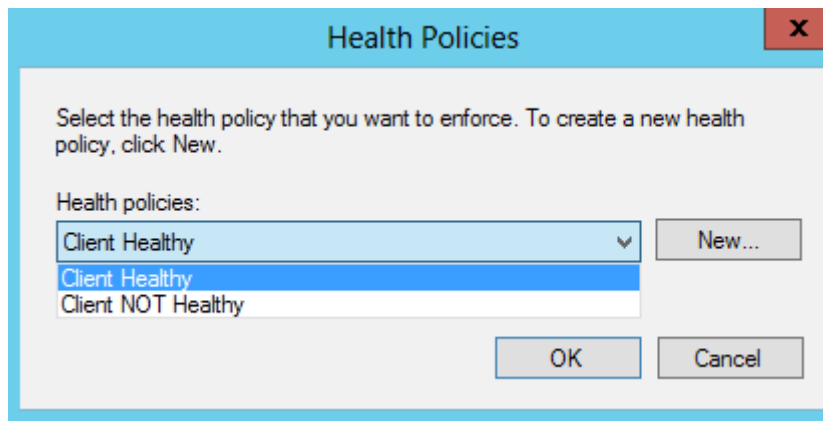
2 go to the “Conditions” tab, and click to the “Add...” button.



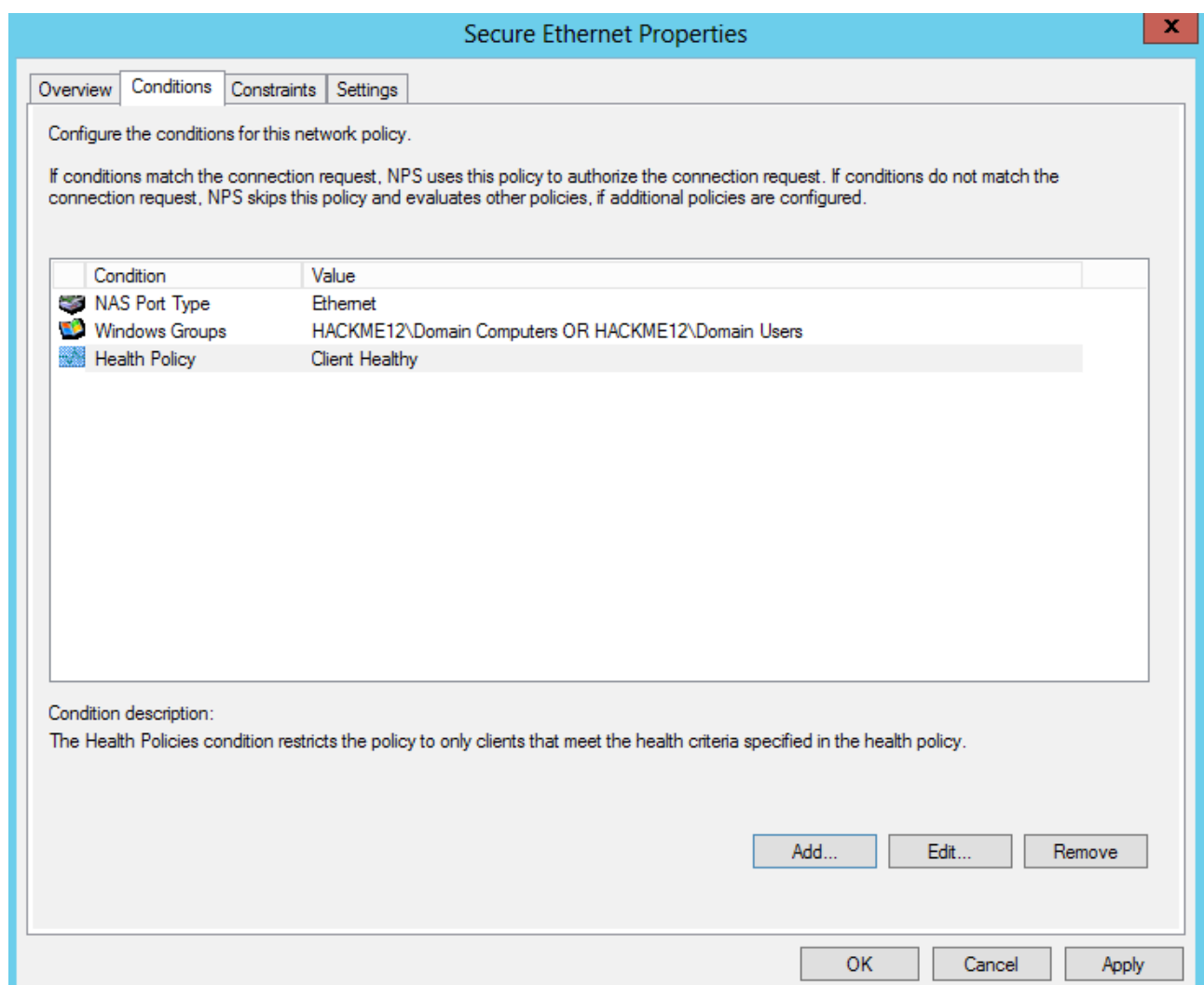
3 select "Health Policies", then click to the "Add..." button



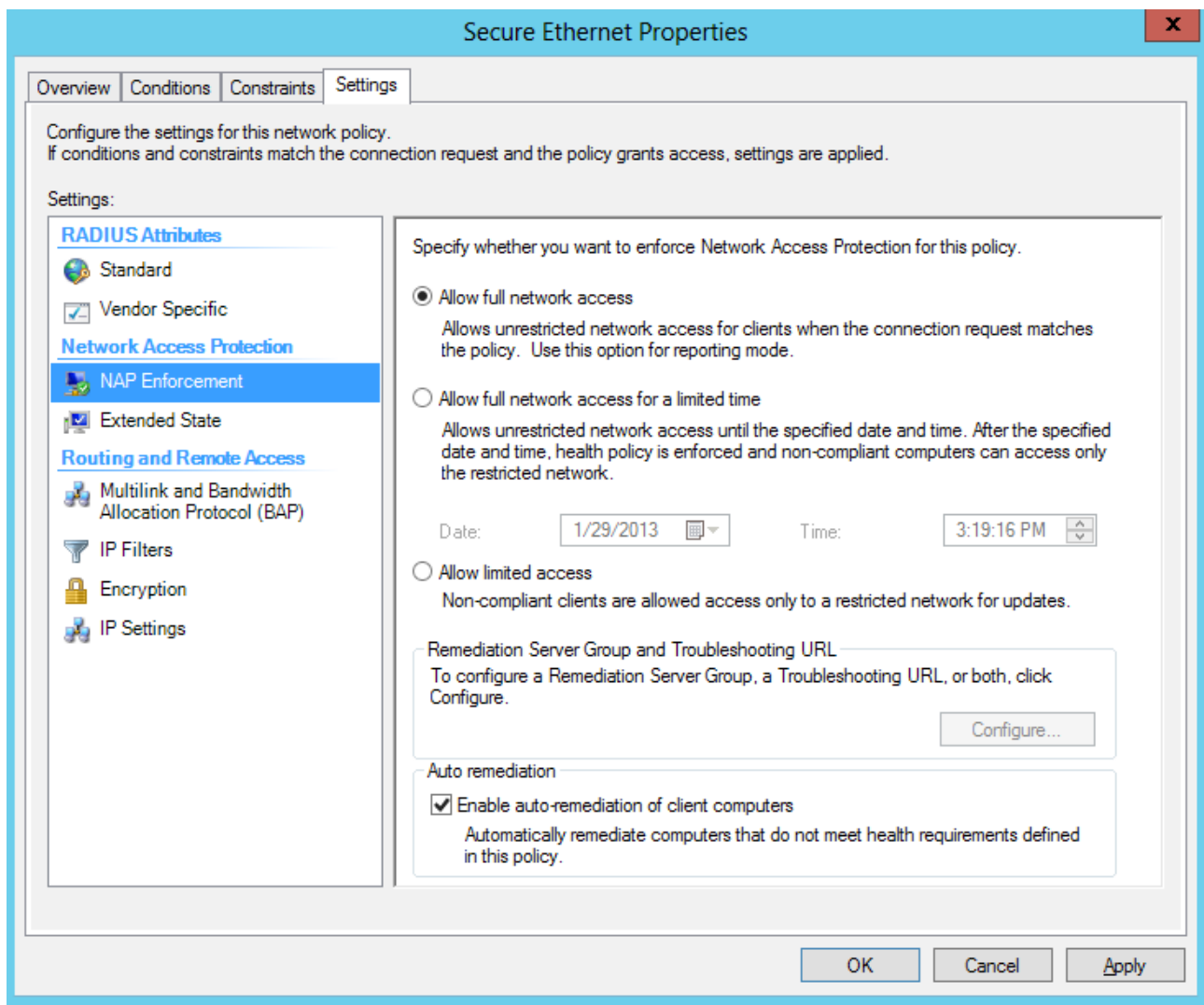
4 Select the "Client Healthy" health policy then click to the OK button



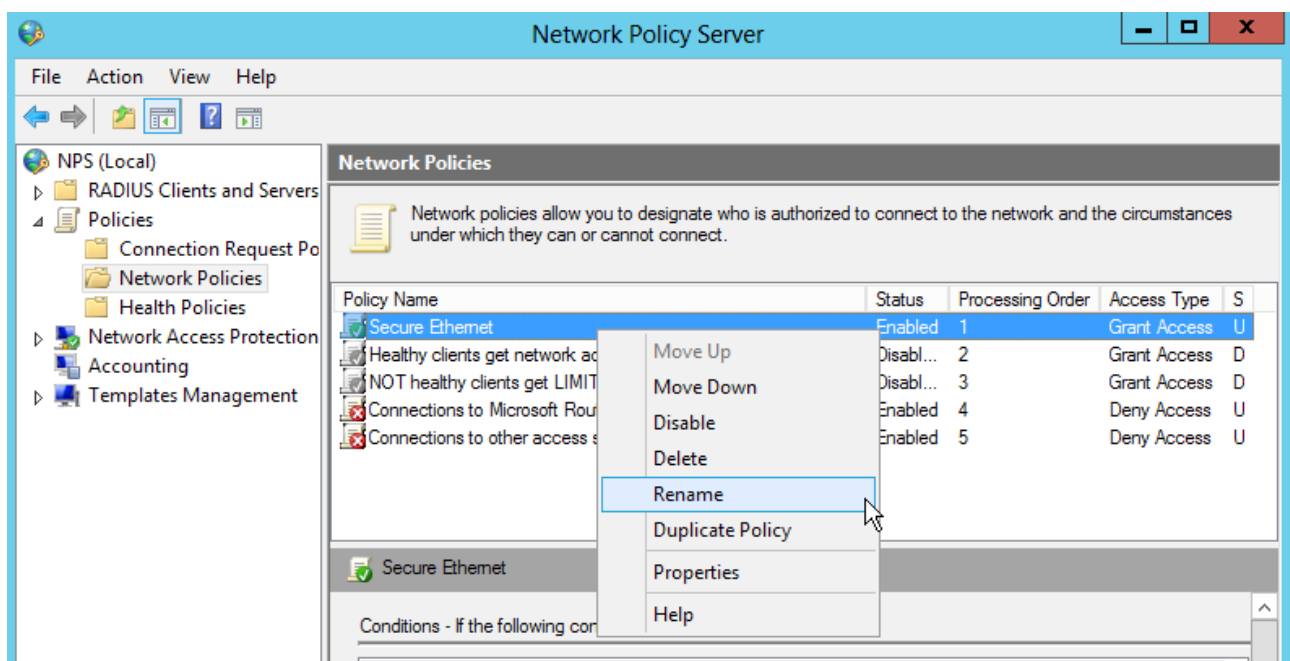
5 Check if the condition appears, then click to the settings tab

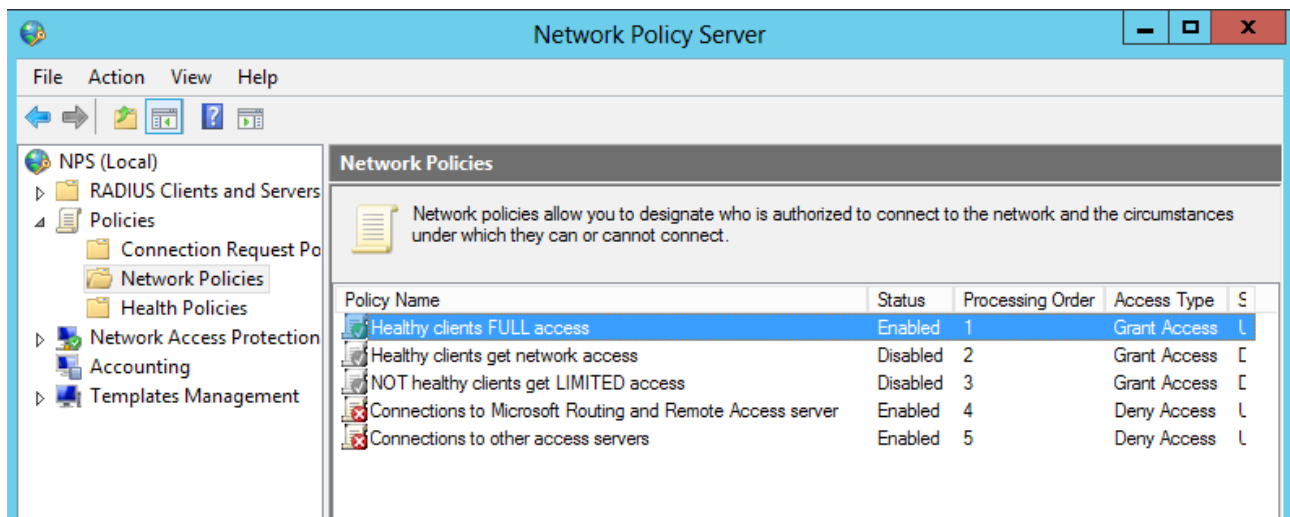


6 click to the NAP enforcement, and set it to “Allow full network access”, then click to the OK.



7 Right click to the rule, and rename it as “Healthy clients FULL access”

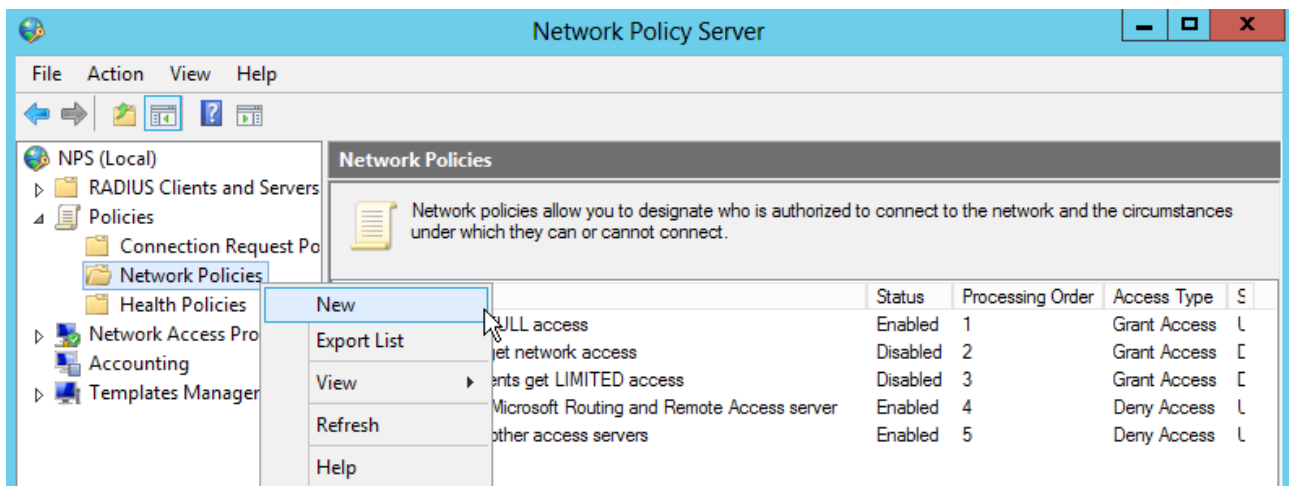




Create a new Network policy rule for the non compliant machines

Create a separate rule for the non compliant computers. We could duplicate the previous rule, and modify only the health policy, but it worth to go through it.


1 right click to the Policies / Network Policies, and from the popup menu select “New”



2 give some name to this new policy, and set the “Type of network access server” to “Unspecified”, then click to the “next” button.

New Network Policy

X



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

NOT healthy client LIMITED access

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, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

Unspecified

☐ Vendor specific:

10

Previous

Next

Finish

Cancel

3 On the “Specify conditions” window click to the “Add...” button.

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
-----------	-------

Condition description:

Add... Edit... Remove

Previous Next Finish Cancel

4 Select "NAS Port Type", then click to the "Add..." button

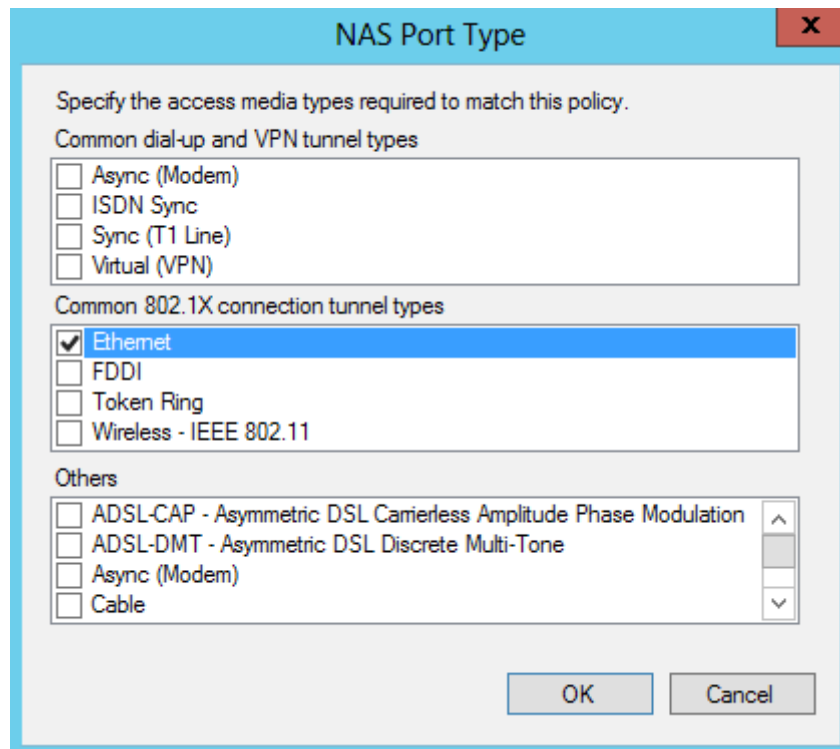
Select condition

Select a condition, and then click Add.

- NAS Identifier**
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.
- NAS IPv4 Address**
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.
- NAS IPv6 Address**
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.
- NAS Port Type**
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.

Add... Cancel

5 Select “Ethernet” as “NAS Port Type”, then click to the OK button



6 On the “Specify conditions” window click again to the “Add....” button.

New Network Policy
✕

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

	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.

Add...
Edit...
Remove

Previous
Next
Finish
Cancel

7 Now select “Windows Groups”, then click to the “Add...” button

Select condition
✕

Select a condition, and then click Add.

Groups

Windows Groups

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

Machine Groups

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

User Groups

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

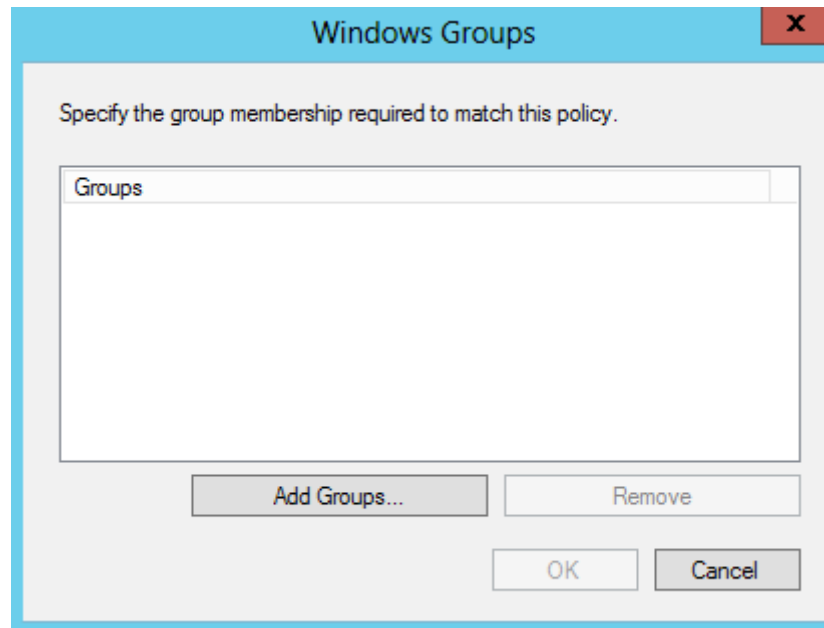
HCAP

Location Groups

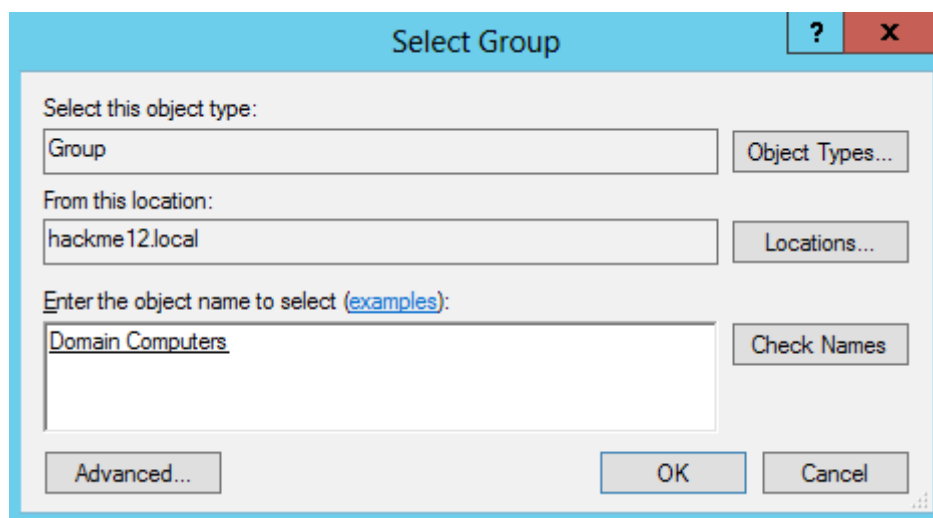
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

Add...
Cancel

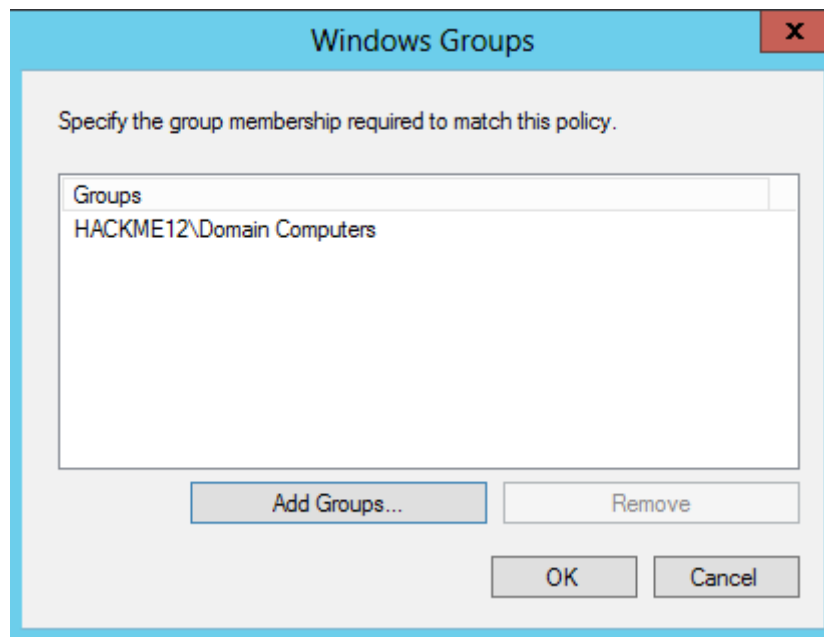
8 On the “Windows Groups” window click to the “Add Groups...”



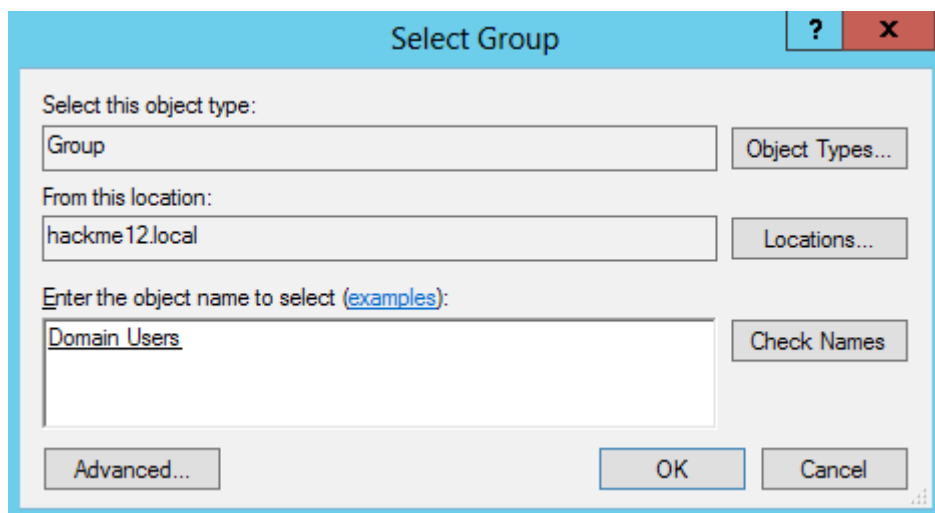
9 Type “Domain Computers”, then click to the Check Names. If it recognized then click to the OK button



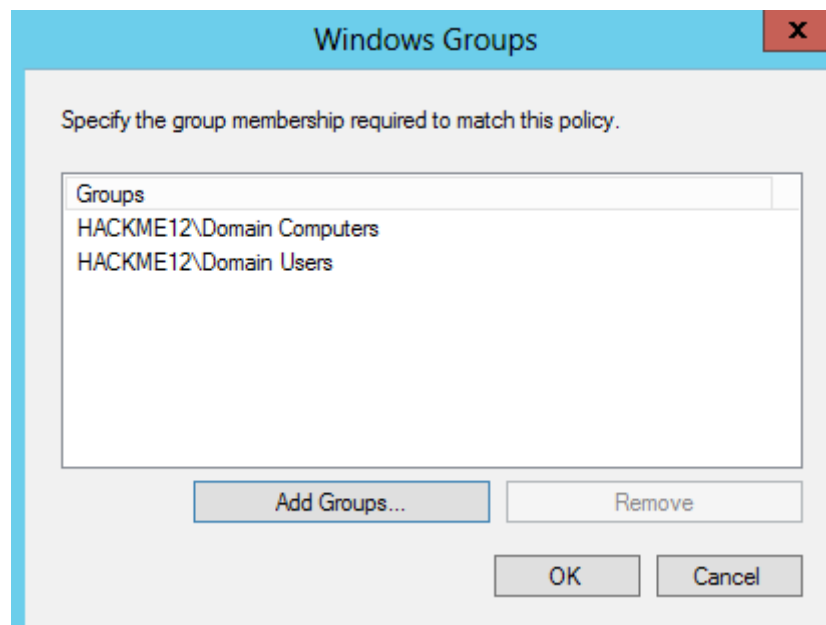
10 On the “Windows Groups” window click again to the “Add Groups...”



11 Type "Domain users", then click to the Check Names. If it recognized then click to the OK button



12 check if both groups are added, then click to the OK button



13 On the “Specify conditions” window click again to the “Add....” button.

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

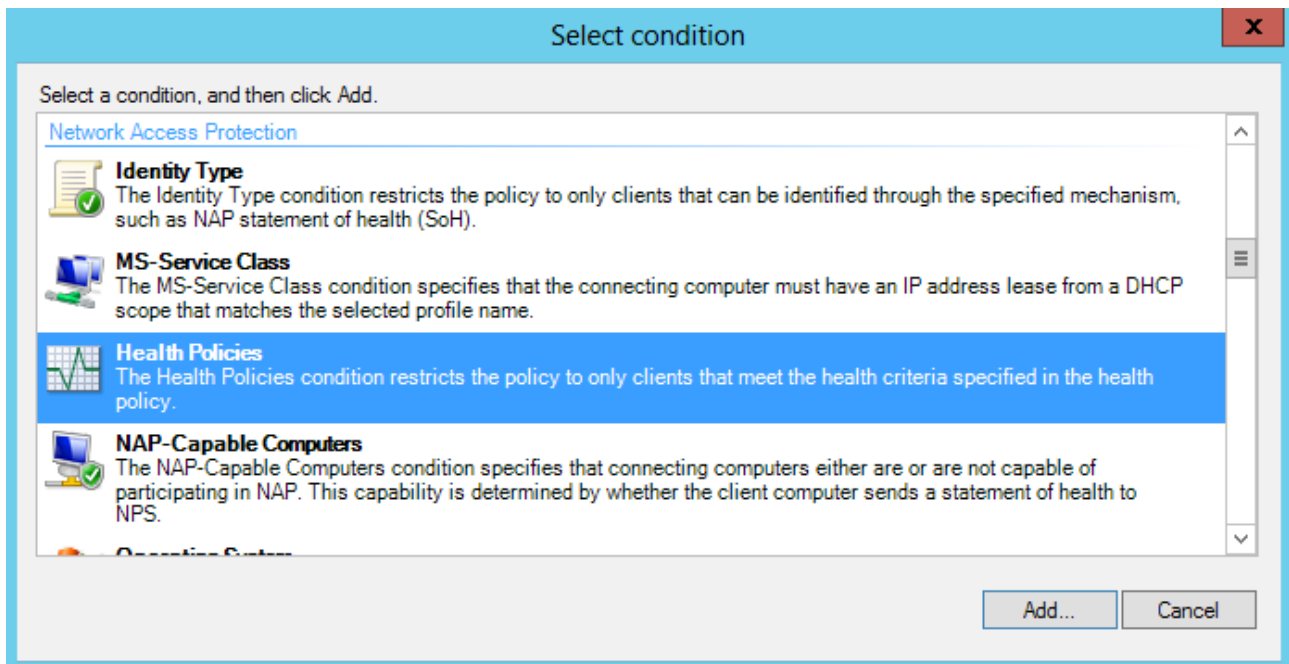
Condition	Value
NAS Port Type	Ethernet
Windows Groups	HACKME12\Domain Computers OR HACKME12\Domain Users

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

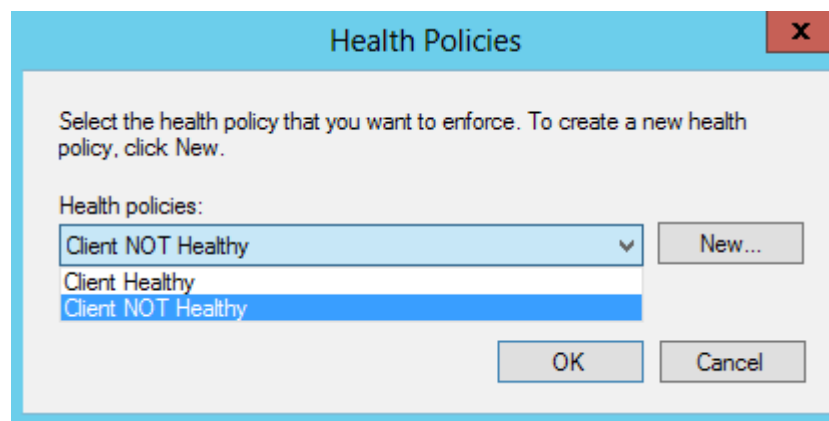
Add... Edit... Remove

Previous Next Finish Cancel

14 Select “Health Policies”, then click to the “Add...” button




15 On the Health Policies window select “Client NOT Healthy”, then click to the OK button.



16 Check if all the three conditions are added, then click to the “Next” button




New Network Policy



Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
 NAS Port Type	Ethernet
 Windows Groups	HACKME12\Domain Computers OR HACKME12\Domain Users
 Health Policy	Client NOT Healthy

Condition description:

The Health Policies condition restricts the policy to only clients that meet the health criteria specified in the health policy.

Add...

Edit...

Remove

Previous


Next

Finish

Cancel

17 On the “Specify Access Permission” window select “Access granted”, then click to the “Next” button

New Network Policy X



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous

Next

Finish

Cancel

18 On the “Configure Authentication Methods” window click to the “Microsoft Protected EAP (PEAP)”, then click to the “Edit...” button.

New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Microsoft: Protected EAP (PEAP)	Move Up
	Move Down

Add... Edit... Remove

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

Previous Next Finish Cancel

19 Select the certificate to authenticate the IAS server. Click to the Add button.

Edit Protected EAP Properties

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 to: hackdc12.hackme12.local

Friendly name: hackdc12.hackme12.local

Issuer: hackme12-HACKDC12-CA

Expiration date: 1/28/2015 3:17:25 PM

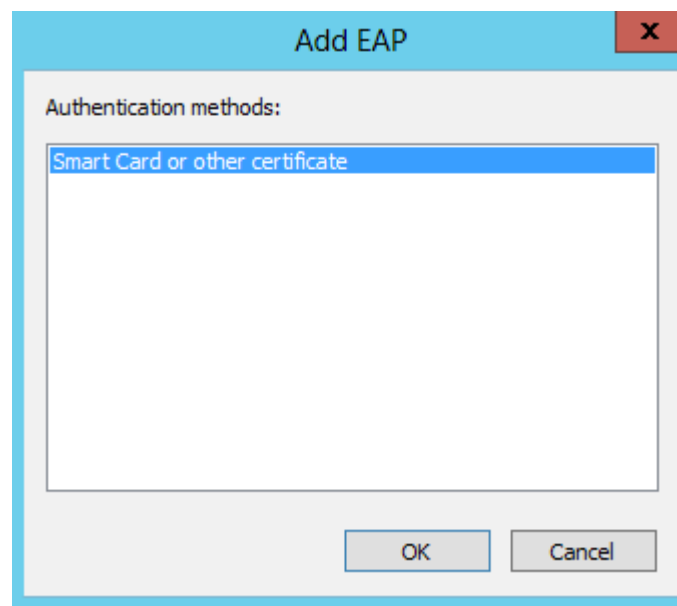
☒ Enable Fast Reconnect
☐ Disconnect Clients without Cryptobinding

Eap Types

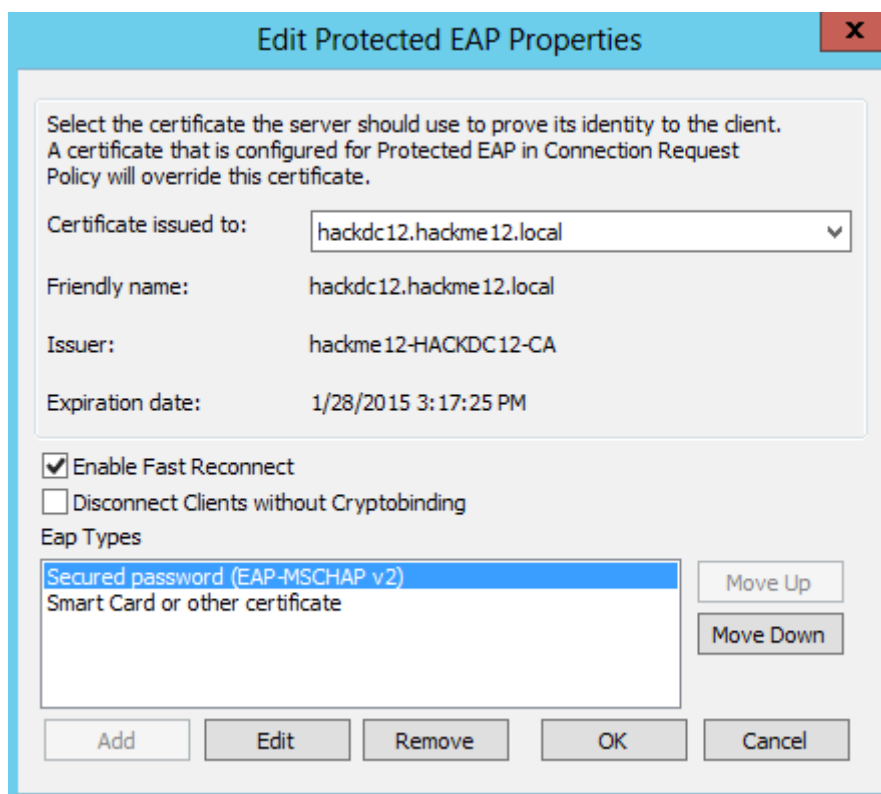
Secured password (EAP-MSCHAP v2)	Move Up
	Move Down

Add Edit Remove OK Cancel

20 On the “Add EAP” window select “Smart Card or other certificate”, later we will use certificate based user authentication, then click to the OK button.




21 click to the OK button



22 Click to the Next button

New Network Policy



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Microsoft: Protected EAP (PEAP)

Move Up

Move Down

Add...

Edit...

Remove

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

Previous


Next

Finish

Cancel

23 on the “Configure Constraint” window click to the Next button.

New Network Policy




Configure Constraints


Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.


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


Constraints:


Constraints

 Idle Timeout

 Session Timeout

 Called Station ID

 Day and time restrictions

 NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

^

v

Previous


Next

Finish

Cancel

24 On the “configure settings” window click to the “Add...” button

New Network Policy



Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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

Settings:

RADIUS Attributes

☒ Standard

☒ Vendor Specific

Network Access Protection

☒ NAP Enforcement

☒ Extended State

Routing and Remote Access

☐ Multilink and Bandwidth Allocation Protocol (BAP)

☐ IP Filters

☐ Encryption

☒ IP Settings

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.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

25 Select “Tunnel-medium-type” then click to the “Add...” button

Add Standard RADIUS Attribute X

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

Attributes:

Name
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
Tunnel-Type

Description:

Specifies the transport medium used when creating a tunnel for protocols (for example, L2TP) that can operate over multiple transports.

26 On the “Attribute Information” window click to the “Add...” button again

Attribute Information X

Attribute name:
Tunnel-Medium-Type

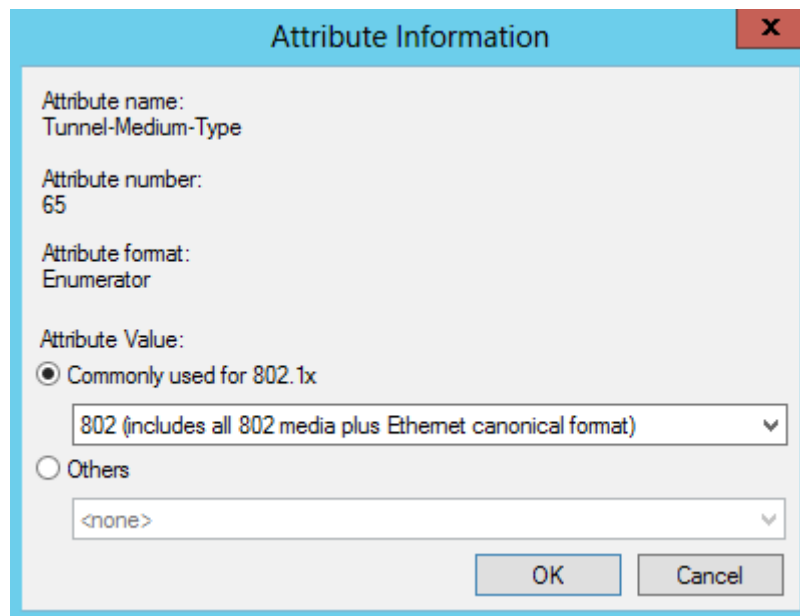
Attribute number:
65

Attribute format:
Enumerator

Attribute values:

Vendor	Value

27 From the “Commonly used for 802.1x” combo box choose the 802 (includes all 802 media plus ethernet canonical format), then click to the OK button



Attribute Information

Attribute name:
Tunnel-Medium-Type

Attribute number:
65

Attribute format:
Enumerator

Attribute Value:

☒ Commonly used for 802.1x

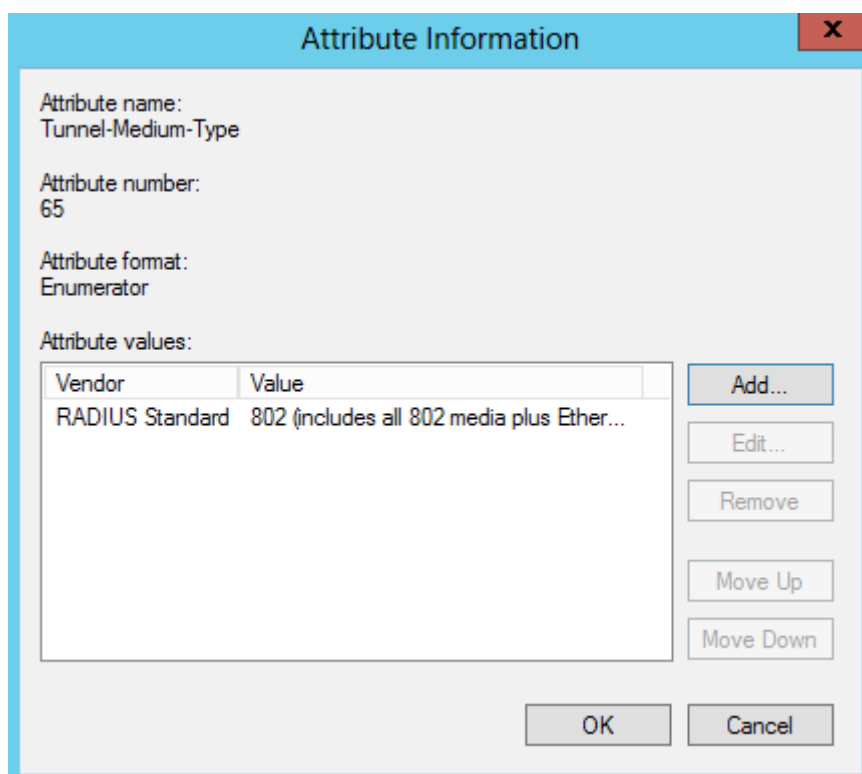
802 (includes all 802 media plus Ethernet canonical format) ▼

☐ Others

<none> ▼

OK Cancel

28 click to the OK button on the “Attribute Information” window



Attribute Information

Attribute name:
Tunnel-Medium-Type

Attribute number:
65

Attribute format:
Enumerator

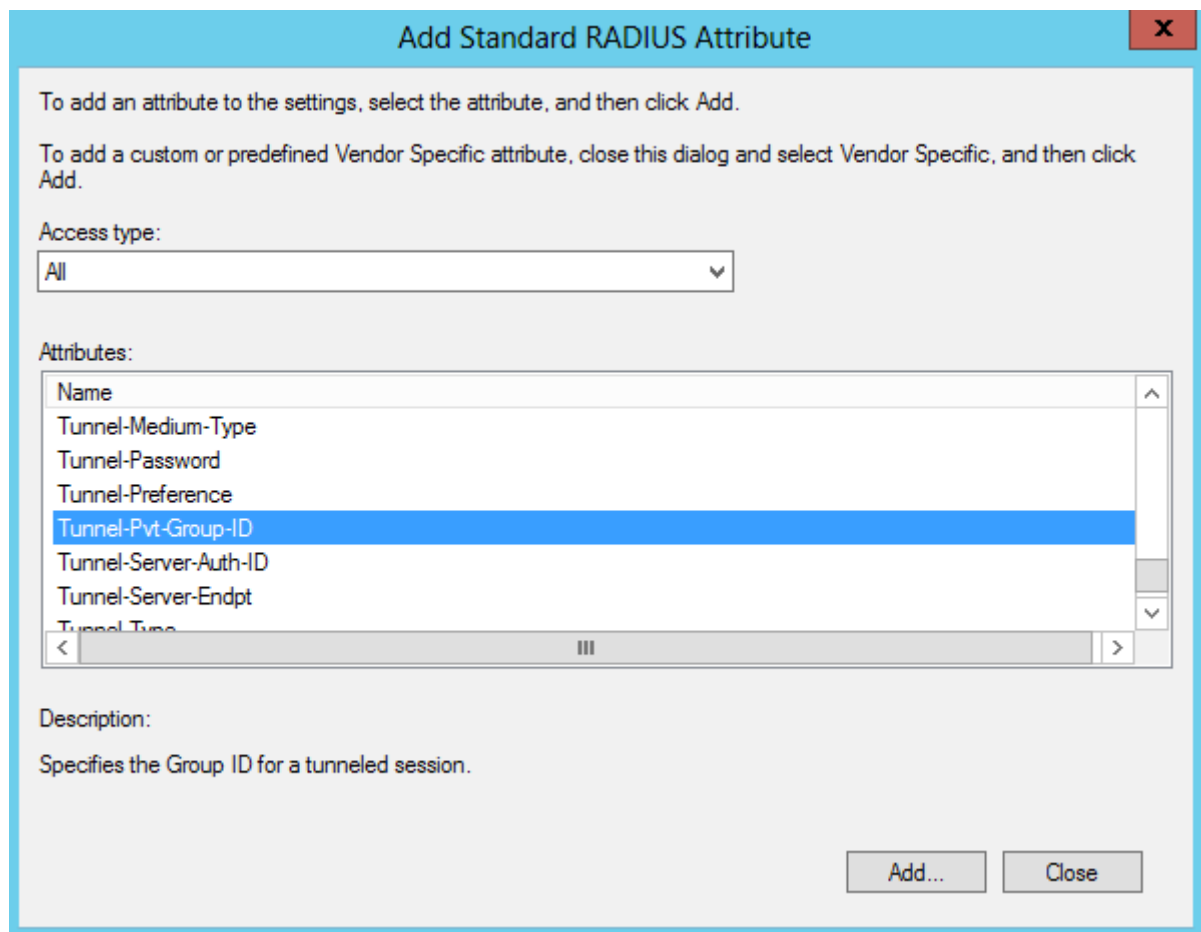
Attribute values:

Vendor	Value
RADIUS Standard	802 (includes all 802 media plus Ether...

Add... Edit... Remove Move Up Move Down

OK Cancel

29 On the “Add Standard RADIUS Attribute window” Select “Tunnel-Pvt-group-ID” then click to the “Add...” button



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

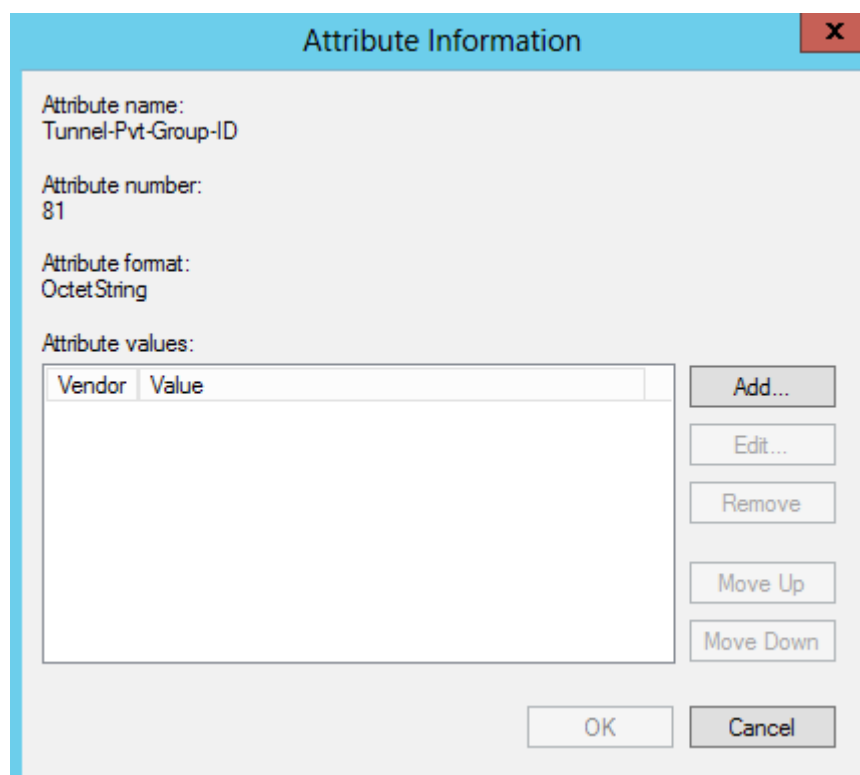
Access type:

Attributes:

Name
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
Tunnel-Type

Description:
 Specifies the Group ID for a tunneled session.

30 On the “Attribute Information” window click to the “Add...” button again



Attribute Information

Attribute name:
 Tunnel-Pvt-Group-ID

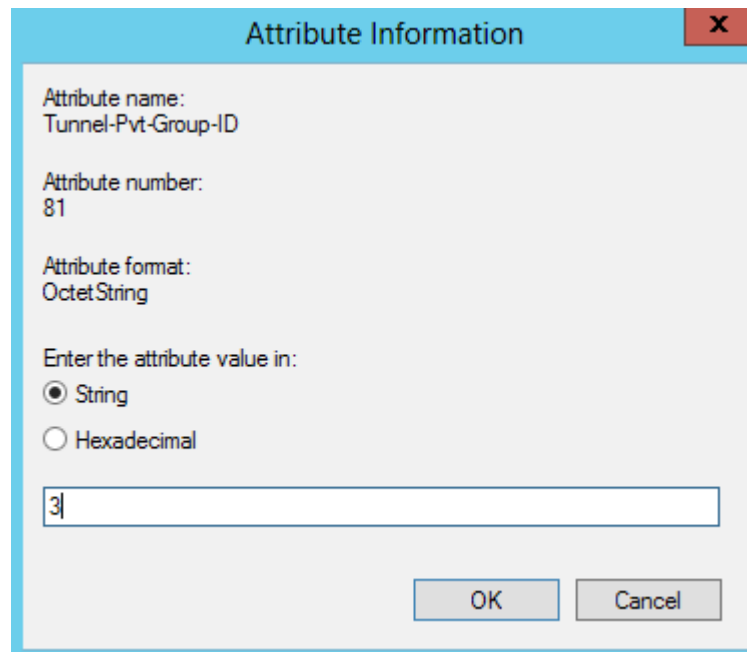
Attribute number:
 81

Attribute format:
 OctetString

Attribute values:

Vendor	Value

31 Type “3” as value (the non compliant computers will added to VLAN 3), then click to the OK button



Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

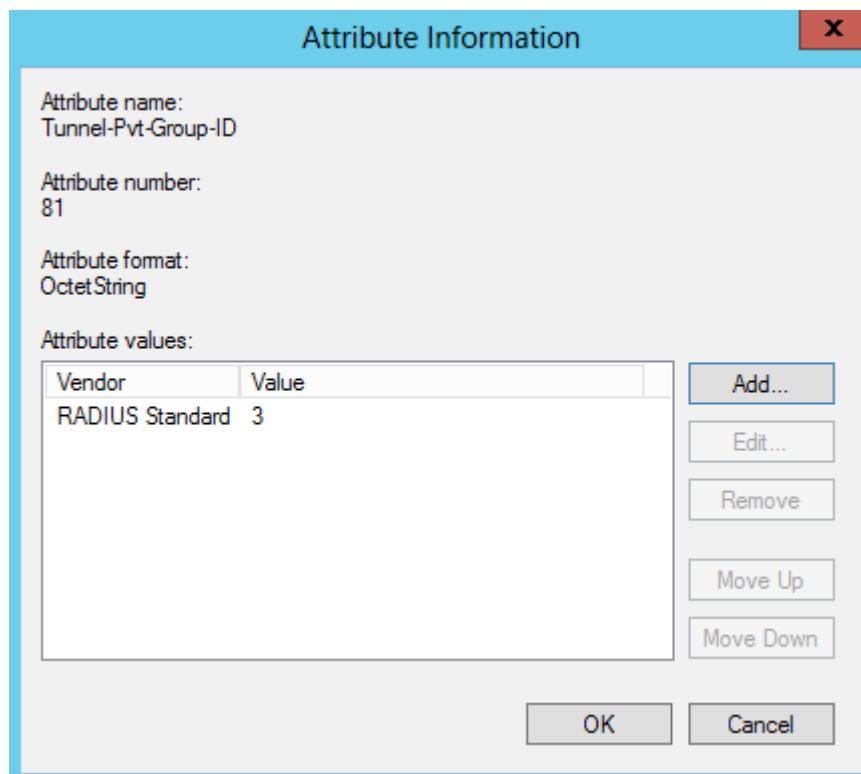
Enter the attribute value in:

☒ String
☐ Hexadecimal

3

OK Cancel

32 click to the OK button on the “Attribute Information” window



Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

Attribute values:

Vendor	Value
RADIUS Standard	3

Add...
Edit...
Remove
Move Up
Move Down

OK Cancel

33 On the “Add Standard RADIUS Attribute window” Select “Tunnel-Type” then click to the “Add...” button

Add Standard RADIUS Attribute X

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

Attributes:

Name
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
Tunnel-Type

Description:
 Specifies the tunneling protocols used.

34 On the “Attribute Information” window click to the “Add...” button again

Attribute Information X

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute values:

Vendor	Value

35 From the “Commonly used for 802.1x” combo box choose the “Virtual LANs (VLAN)”, then click to the OK button

Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute Value:

☐ Commonly used for Dial-Up or VPN

<none>

☒ Commonly used for 802.1x

Virtual LANs (VLAN)

☐ Others

<none>

OK Cancel

36 click to the OK button on the “Attribute Information” window

Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

Add... Edit... Remove Move Up Move Down

OK Cancel

37 On the “Add Standard RADIUS Attribute window” Select “Tunnel-Preference” then click to the “Add...” button

Add Standard RADIUS Attribute ✕

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

Attributes:

Name
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
Tunnel-Type

Description:

Specifies the relative preference assigned to each tunnel when more than one set of tunneling attributes is returned to the tunnel initiator.

38 Type "1" as value, then click to the OK button

Attribute Information ✕

Attribute name:
Tunnel-Preference


Attribute number:
83

Attribute format:
Integer

Attribute value:

39 On the "Configure Settings" window check if everything is set up correctly, then click to the NAP enforcement

New Network Policy



Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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

Settings:

RADIUS Attributes

☒ Standard

☒ Vendor Specific

Network Access Protection

☒ NAP Enforcement

☒ Extended State

Routing and Remote Access

☒ Multilink and Bandwidth Allocation Protocol (BAP)

☒ IP Filters

☒ Encryption

☒ IP Settings

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.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	3
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Preference	1

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

40 Select “Allow limited access”, then click to the “configure...” button, to set up the remediation servers

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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

Settings:

RADIUS Attributes

- Standard
- ☒ Vendor Specific

Network Access Protection

- NAP Enforcement**
- Extended State

Routing and Remote Access

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- ☒ IP Settings

☐ Allow full network access for a limited time

Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date:

Time:

☒ Allow limited access

Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL

To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure...

[Configure...](#)

Auto remediation

☐ Enable auto-remediation of client computers

Automatically remediate computers that do not meet health requirements defined in this policy.

Previous
Next
Finish
Cancel

41 Select the remediation server group then click to the OK button

Remediation Servers and Troubleshooting URL

Remediation Server Group

Select the remediation servers that you would like to provide to computers with limited network access.

remediation servers

<none>

remediation servers

troubleshooting URL

New Group...

Troubleshooting URL

Specify a Web page address Uniform Resource Locator (URL) that provides instructions to users on how to bring computers and devices into compliance with your network access policy.

OK
Cancel

42 On the “Configure Settings” window click to the Next button.

The screenshot shows the 'New Network Policy' window with the 'Configure Settings' tab selected. The window title is 'New Network Policy'. The 'Configure Settings' section has a sub-header 'Configure Settings' and a description: 'NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.' Below this, it says 'Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.'

The 'Settings:' section on the left lists various categories: 'RADIUS Attributes' (Standard, Vendor Specific), 'Network Access Protection' (NAP Enforcement, Extended State), 'Routing and Remote Access' (Multilink and Bandwidth Allocation Protocol (BAP), IP Filters, Encryption, IP Settings). 'NAP Enforcement' is currently selected.


The main configuration area for 'NAP Enforcement' shows two radio button options: 'Allow full network access for a limited time' (unselected) and 'Allow limited access' (selected). The 'Allow full network access for a limited time' option includes a description: 'Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.' It also has date and time pickers set to '1/29/2013' and '3:54:38 PM'. The 'Allow limited access' option includes a description: 'Non-compliant clients are allowed access only to a restricted network for updates.'

Below the radio buttons, there is a section for 'Remediation Server Group and Troubleshooting URL' with a description: 'To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.' and a 'Configure...' button. At the bottom of this section is an 'Auto remediation' section with a checkbox 'Enable auto-remediation of client computers' (unchecked) and a description: 'Automatically remediate computers that do not meet health requirements defined in this policy.'

At the bottom of the window, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

43 On the “Completing new Network Policy” window click to the Finish button

New Network Policy



Completing New Network Policy

You have successfully created the following network policy:

NOT healthy client LIMITED access

Policy conditions:

Condition	Value
NAS Port Type	Ethernet
Windows Groups	HACKME12\Domain Computers OR HACKME12\Domain Users
Health Policy	Client NOT Healthy

Policy settings:

Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	False
NAP Enforcement	Allow limited network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

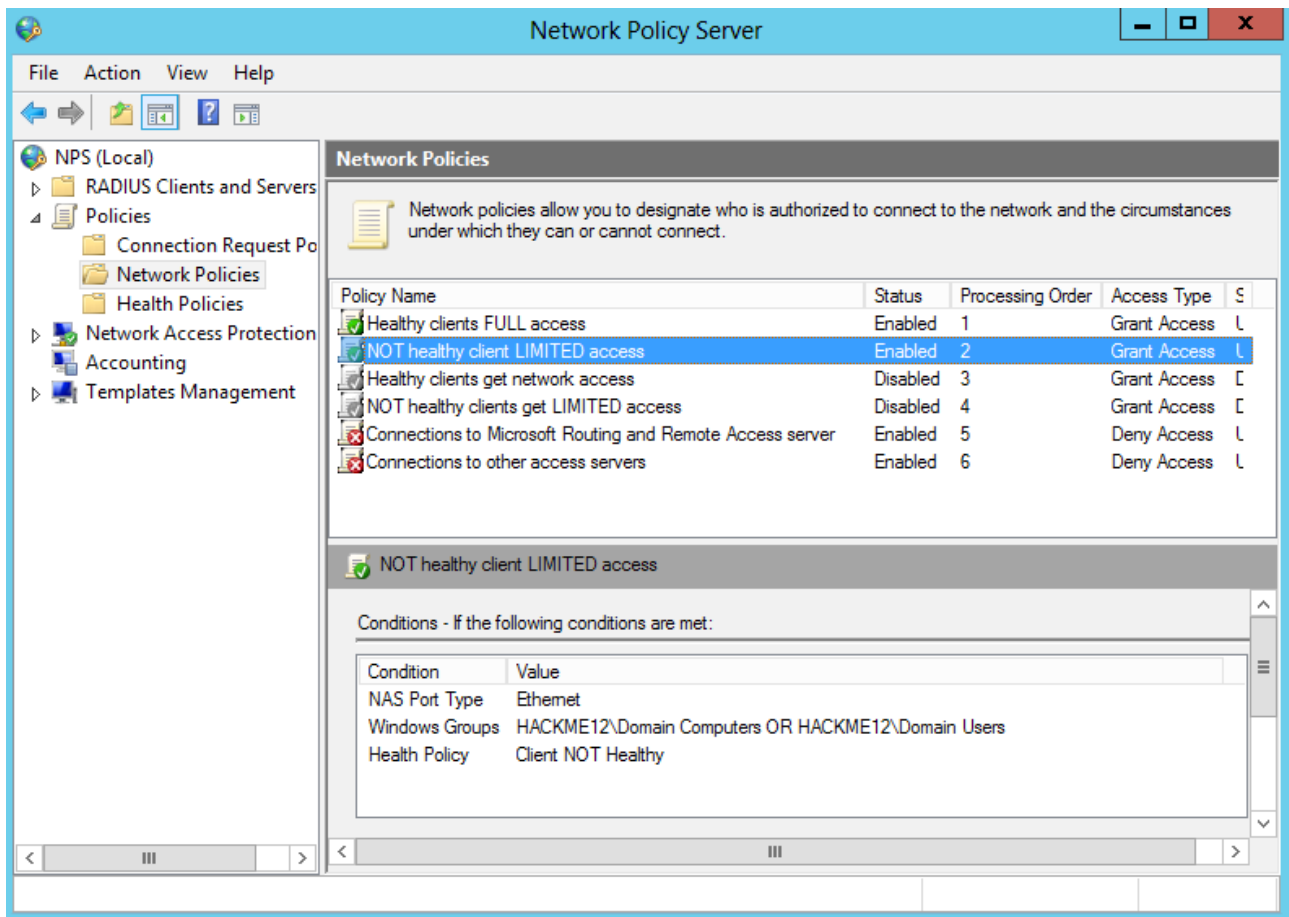
Previous

Next

Finish

Cancel

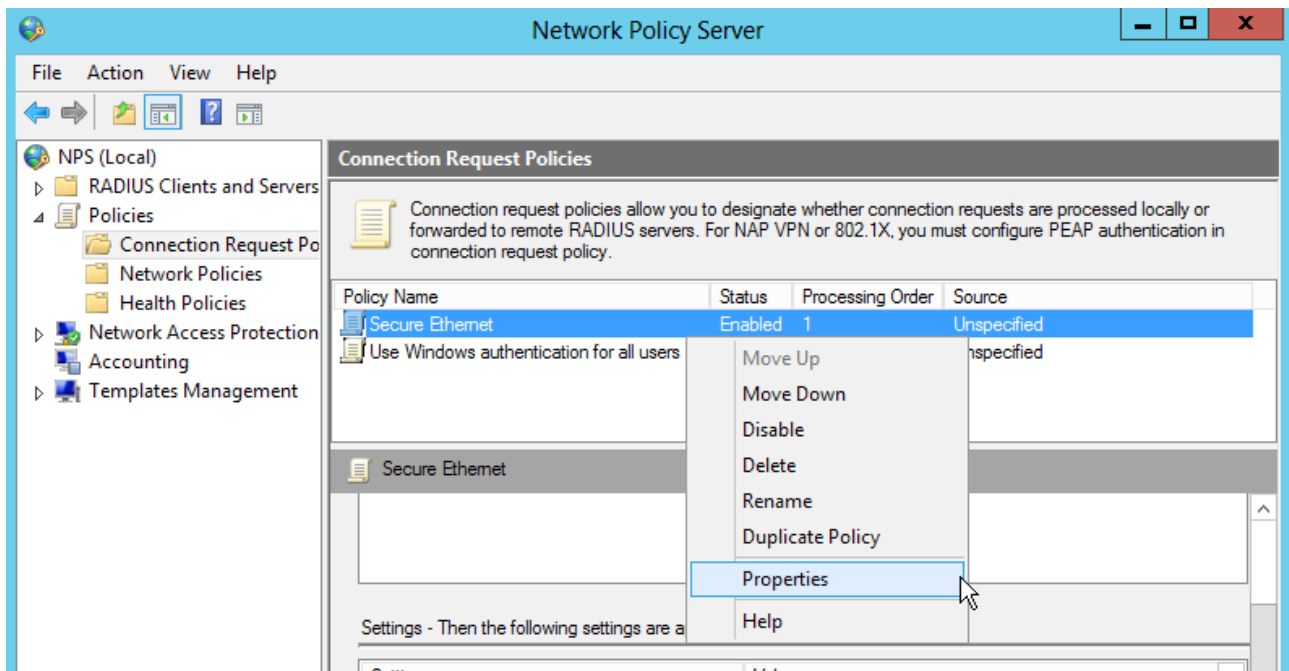
44 Check if both role are created.



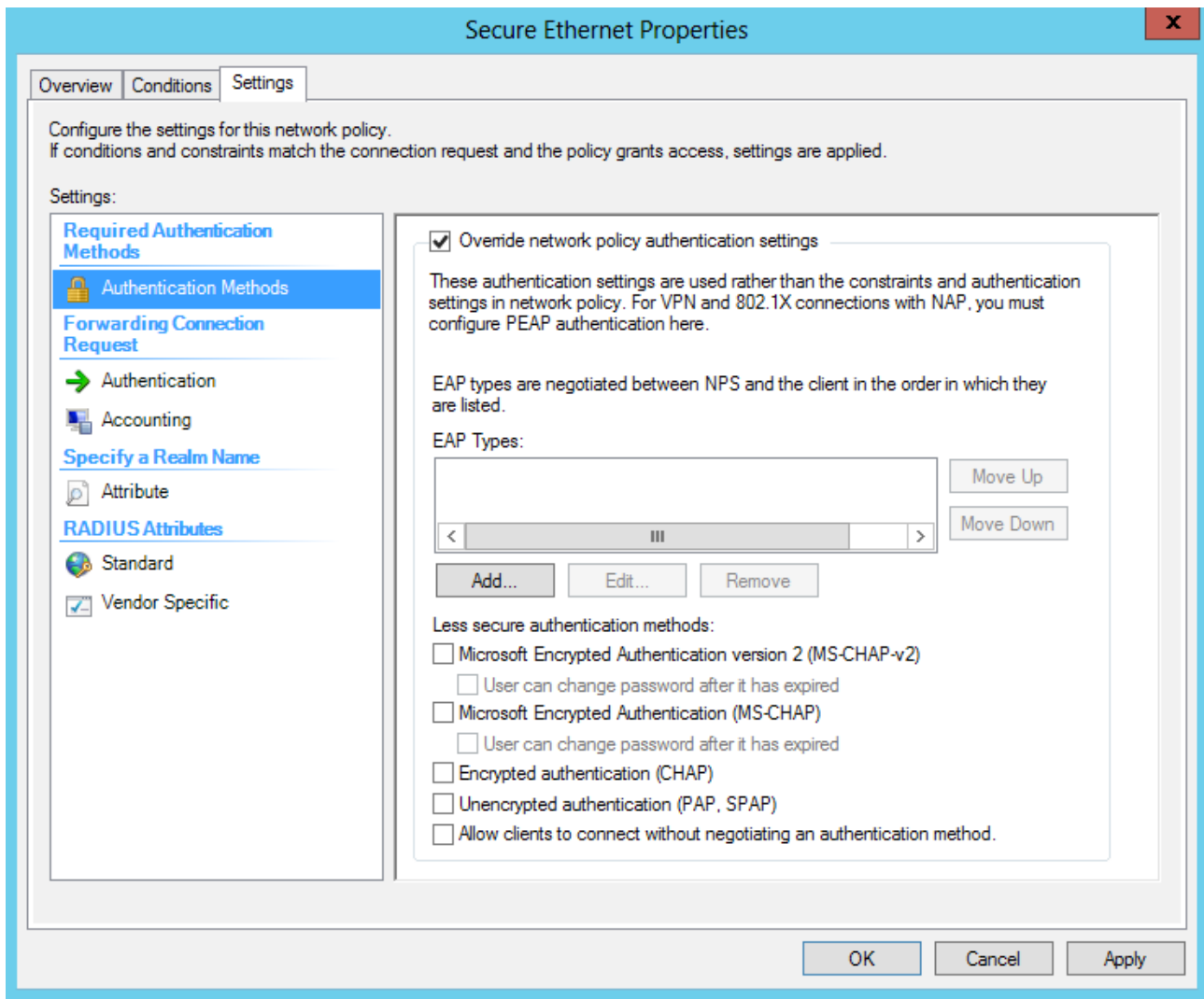
Create Connection Policy on the NPS server

We should modify the “Connection Request Policy”, to check the health status.

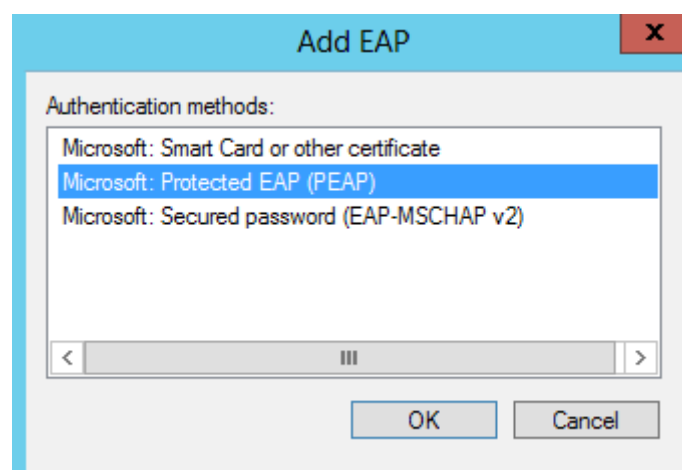
1 Right click to the already created “Secure Ethernet” rule, and from the popup menu select “Properties”



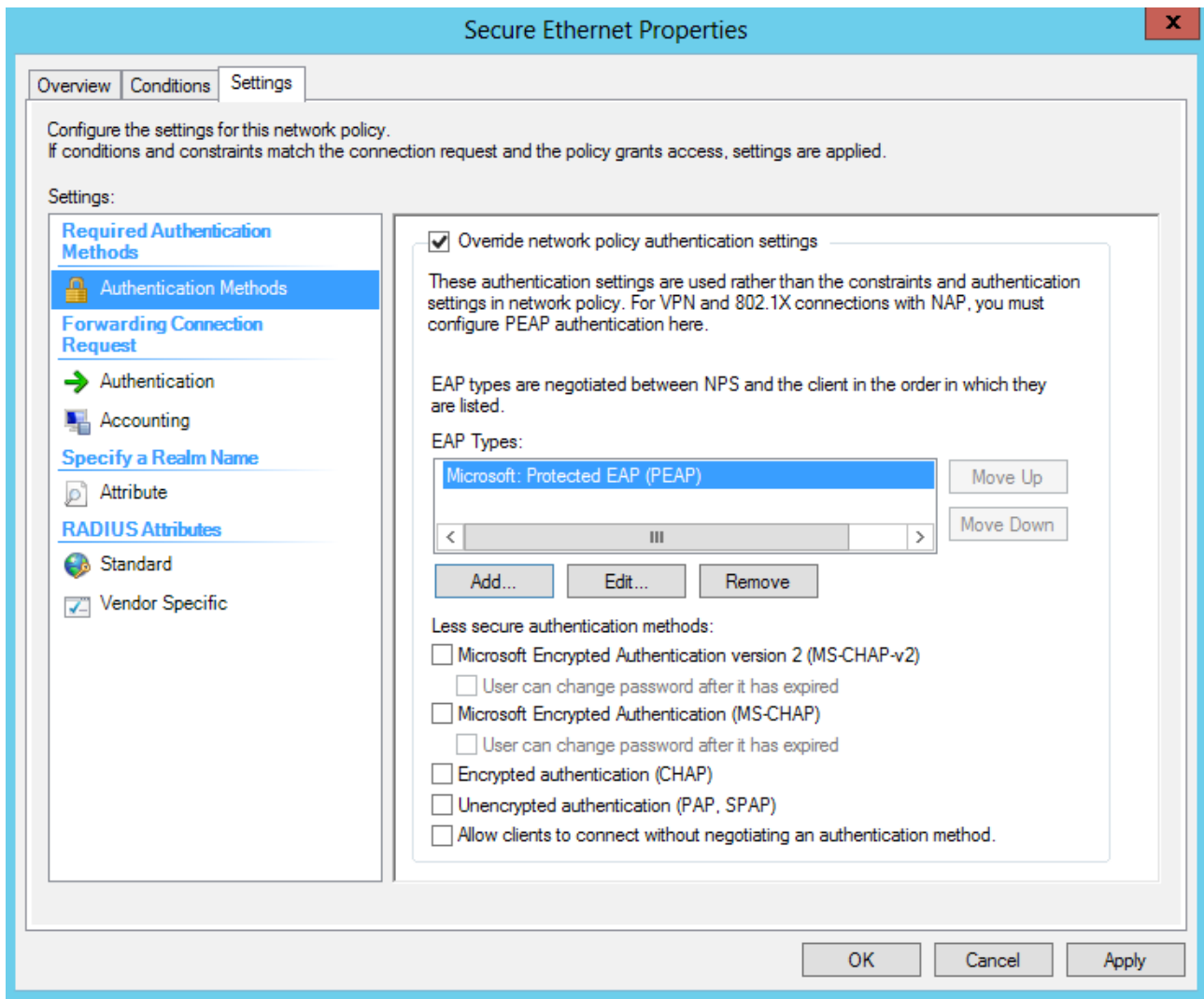
2 Go to the settings tab, and check the “Override network policy authentication” box, then click to the “Add...” button



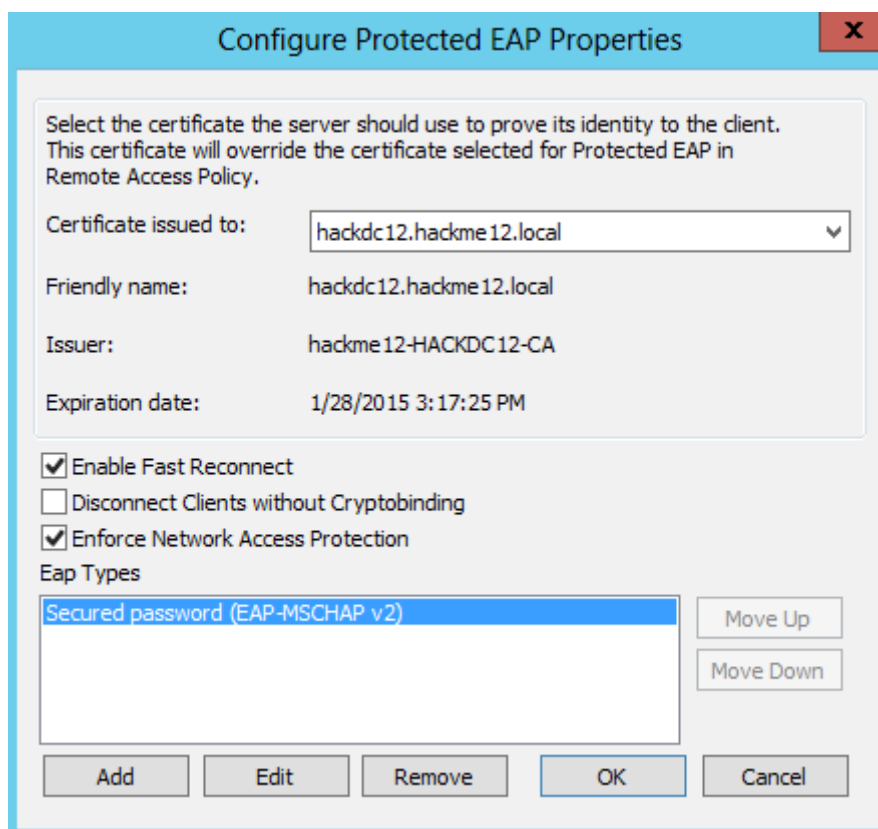
3 On the “Add EAP” window select “Microsoft: Protected EAP (PEAP)”, then click to the OK button



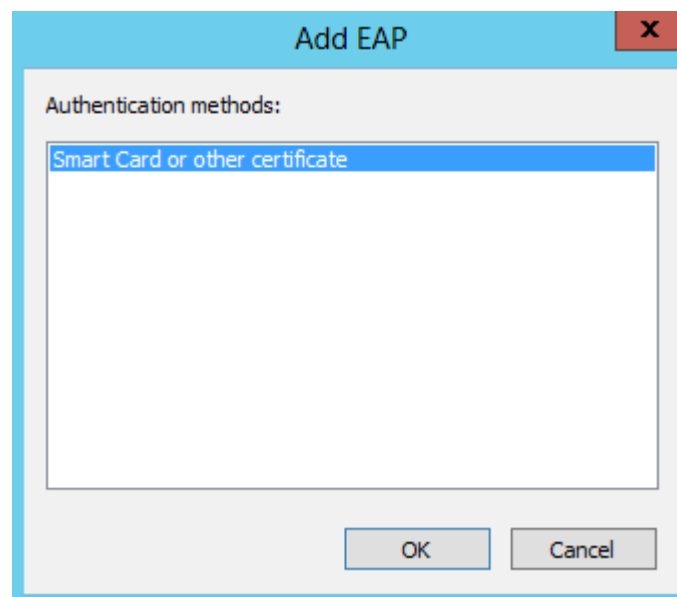
4 Select the “Microsoft: Protected EAP (PEAP)”, then click to the “Edit...” button.



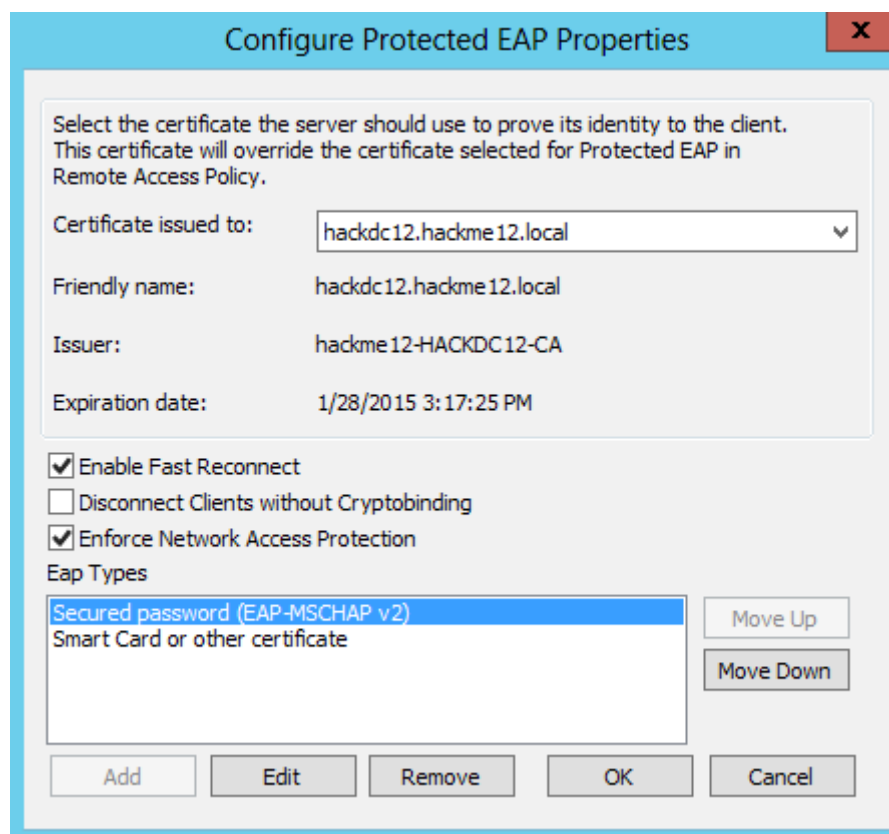
4 Select the certificate to authenticate the IAS server, and check the “Enforce Network Access Protection”. Click to the Add button.



5 On the “Add EAP” window select “Smart Card or other certificate”, then click to the OK button, later we will change the user authentication to certificate based.



6 On the “Configure Protected EAP Properties” click to the OK button



7 On the “Secure Ethernet Properties” window click to the OK button

Secure Ethernet Properties

OverviewConditionsSettings

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

Settings:

Required Authentication Methods

Authentication Methods

Forwarding Connection Request

Authentication

Accounting

Specify a Realm Name

Attribute

RADIUS Attributes

Standard

Vendor Specific

☒ 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:

Microsoft: Protected EAP (PEAP)

<|||>

Move Up

Move Down

Add...

Edit...

Remove

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.

OK

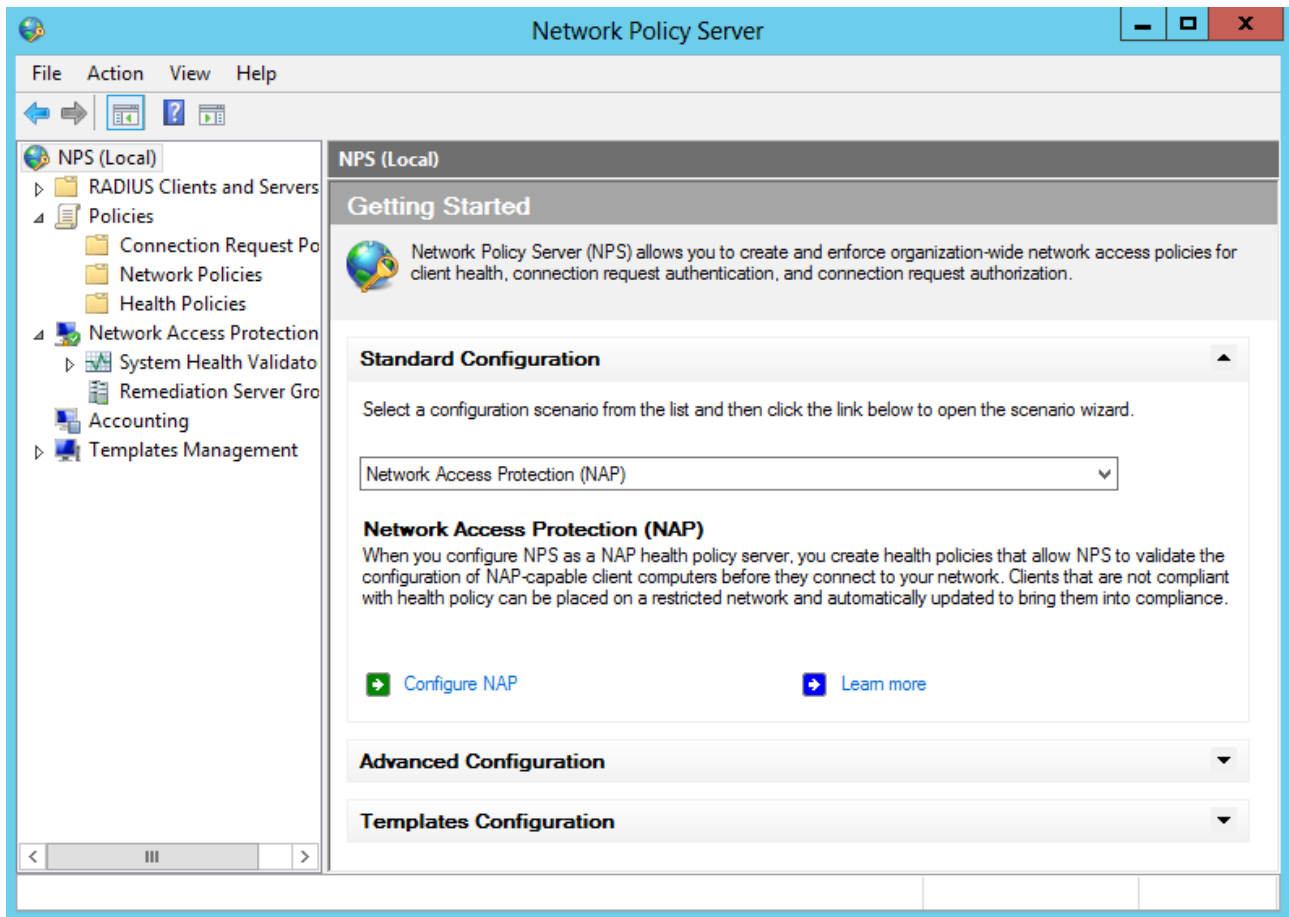
Cancel

Apply

Set up the NPS by wizard

All these things what we had done manually can be done through a wizard.


1 Go to the NPS text on the tree view and click to the “Configure NAP” link.



2 On the “Configure NAP” window select “IEEE 802.1x (Wired)” as “Network connection method”, and give it some policy name, then click to the “Next” button

Configure NAP

X



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.

IEEE 802.1X (Wired)

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 802.1X (Wired)

Additional requirements:



You must perform additional actions to set up NAP. View additional NAP requirements by clicking on the link below.

[Additional Requirements](#)

Previous

Next

Finish

Cancel

3 On the “Configure NAP” window check if our radius clients are appearing, then click to the Next button.

Configure NAP

Specify 802.1X Authenticating Switches

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

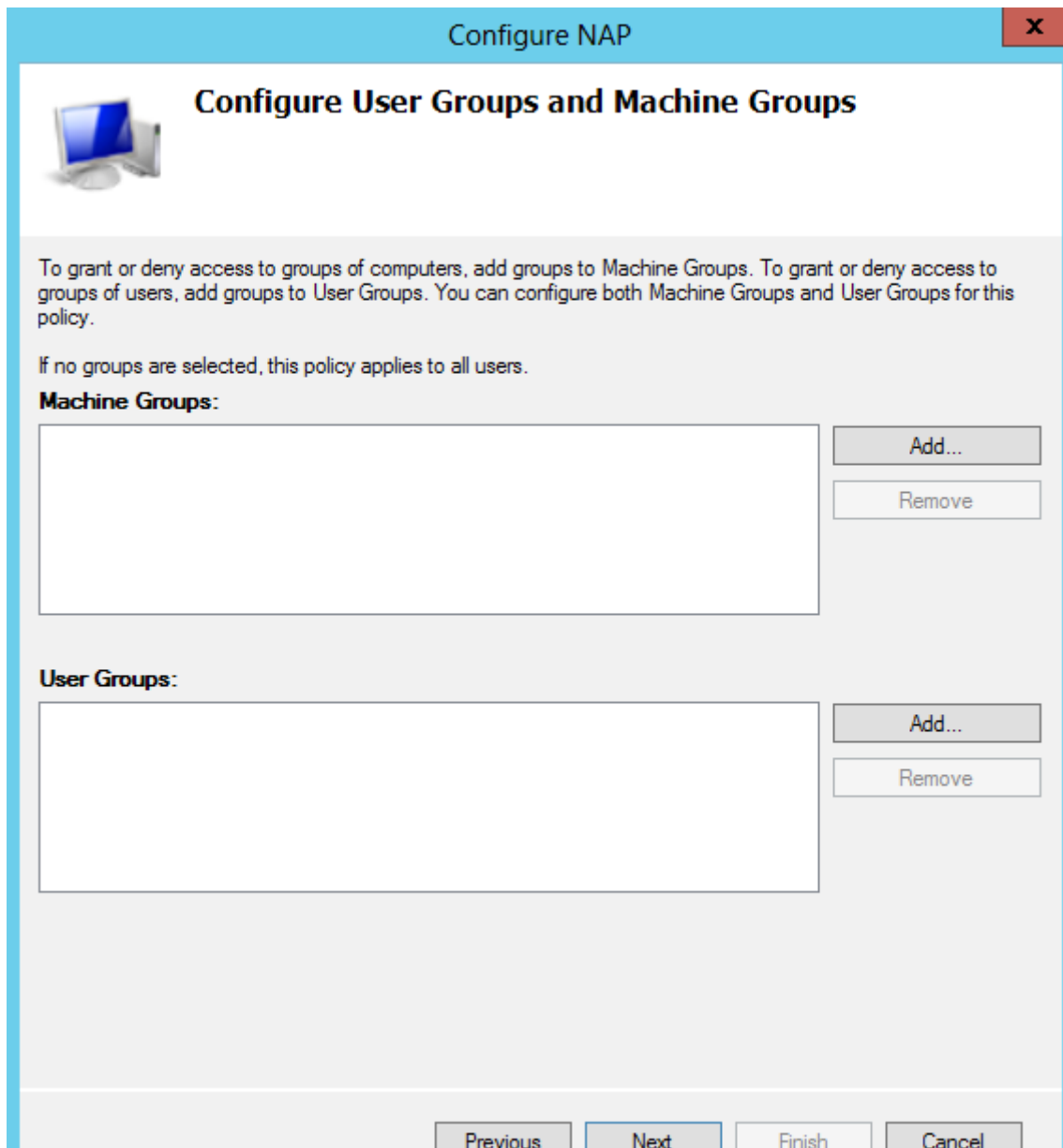
To specify a RADIUS client, click Add.

RADIUS clients:

myswitch	Add...
	Edit...
	Remove

Previous Next Finish Cancel

4 On the “Configure User Groups and Machine Groups” window click to the “Add...” button next to the machine groups



Configure NAP

Configure User Groups and Machine Groups

To grant or deny access to groups of computers, add groups to Machine Groups. To grant or deny access to groups of users, add groups to User Groups. You can configure both Machine Groups and User Groups for this policy.

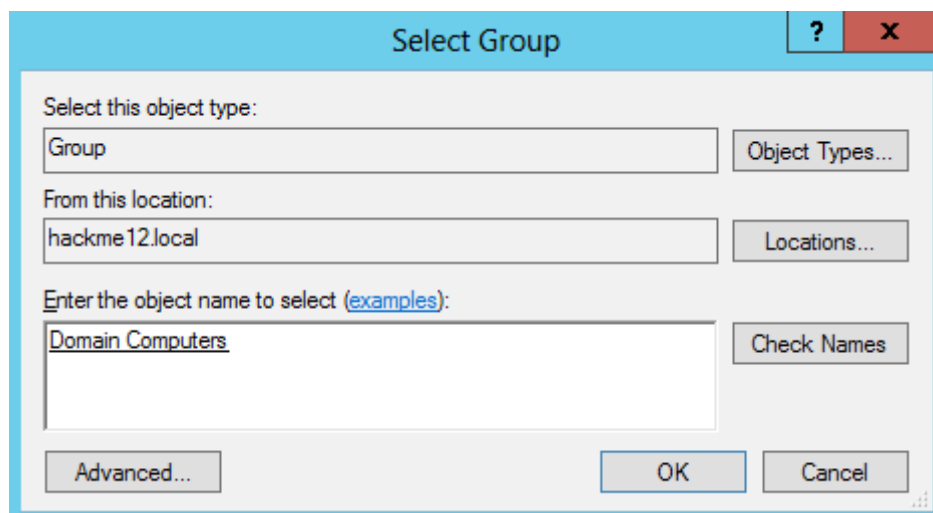
If no groups are selected, this policy applies to all users.

Machine Groups:

User Groups:

Previous Next Finish Cancel

5 On the Select Group window type “Domain Computers”, and click to the “Check Names” button. If it is recognized click to the OK button.



Select Group

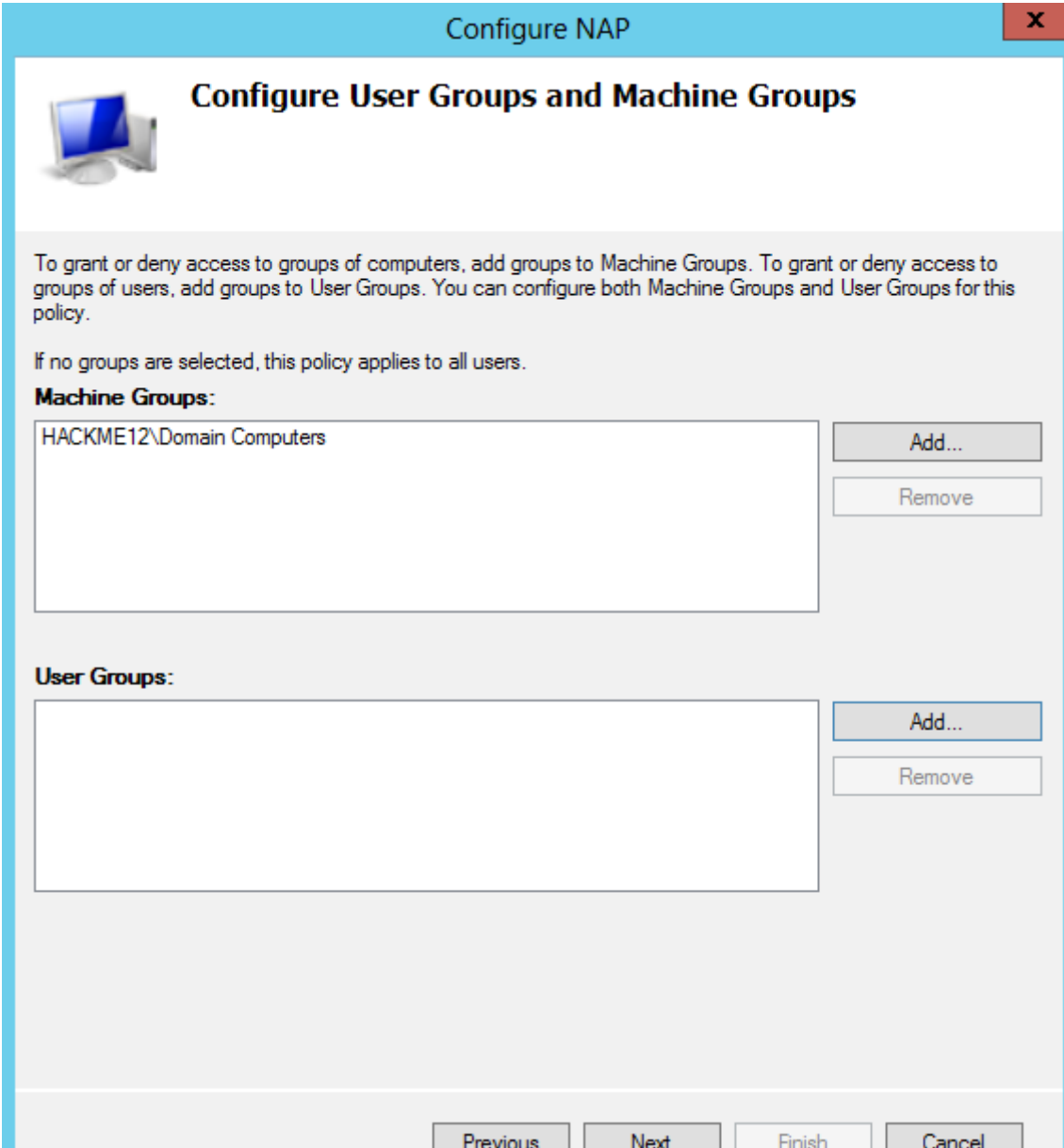
Select this object type:

From this location:

Enter the object name to select (examples):

Advanced... OK Cancel

6 click to the “Add...” button next to the user groups



The image shows the "Configure NAP" dialog box, titled "Configure User Groups and Machine Groups". It contains instructions on how to grant or deny access to groups of computers or users. Below the instructions, there are two sections: "Machine Groups" and "User Groups". Each section has a list box and two buttons: "Add..." and "Remove". The "Machine Groups" list box contains the text "HACKME12\Domain Computers". The "User Groups" list box is empty. At the bottom of the dialog, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Configure NAP

Configure User Groups and Machine Groups

To grant or deny access to groups of computers, add groups to Machine Groups. To grant or deny access to groups of users, add groups to User Groups. You can configure both Machine Groups and User Groups for this policy.

If no groups are selected, this policy applies to all users.

Machine Groups:

HACKME12\Domain Computers

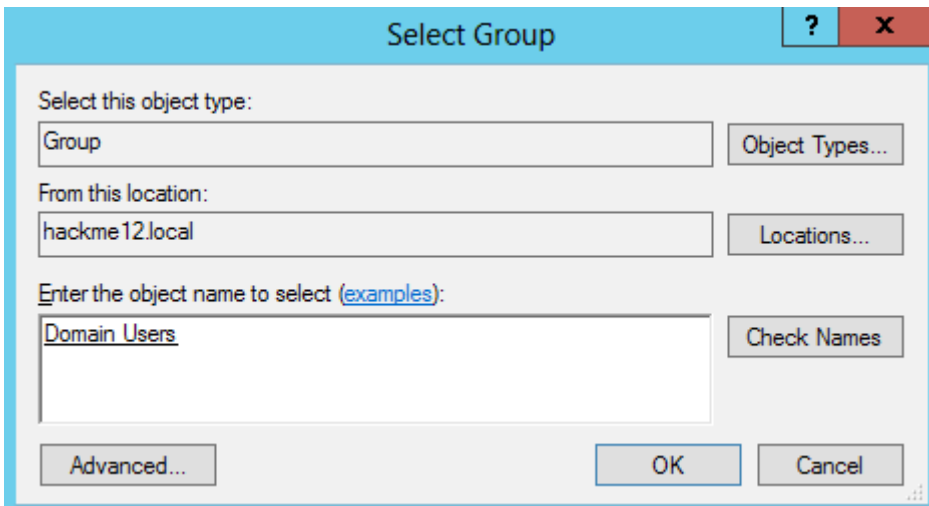
Add... Remove

User Groups:

Add... Remove

Previous Next Finish Cancel

7 On the Select Group window type “Domain Users”, and click to the “Check Names” button. If it is recognized click to the OK button.



The image shows the "Select Group" dialog box. It has a title bar with a question mark and a close button. The dialog contains several input fields and buttons. The "Select this object type:" field is set to "Group". The "From this location:" field is set to "hackme12.local". The "Enter the object name to select (examples):" field is set to "Domain Users". There are buttons for "Object Types...", "Locations...", "Check Names", "Advanced...", "OK", and "Cancel".

Select Group

Select this object type:

Group

Object Types...

From this location:

hackme12.local

Locations...

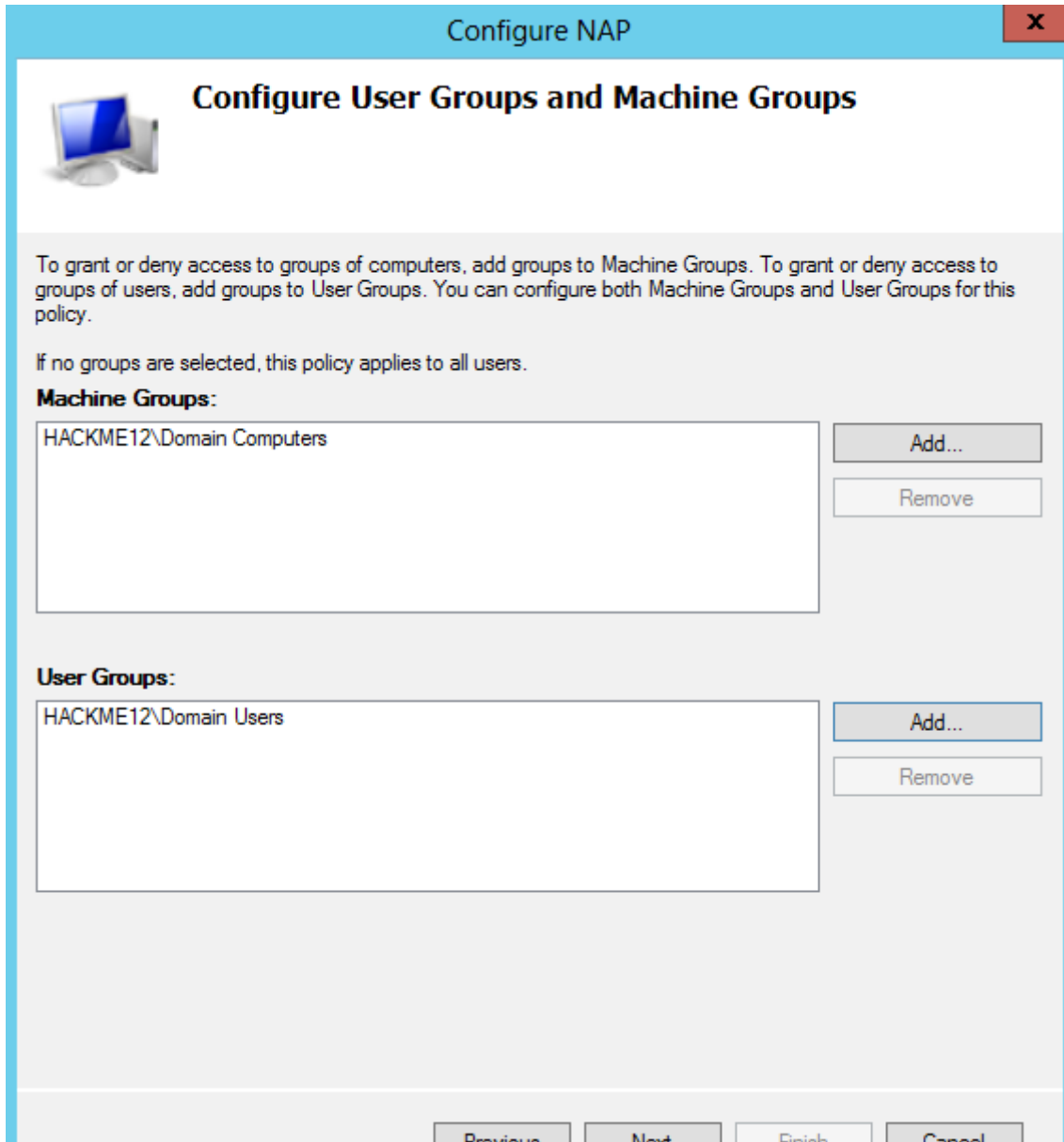
Enter the object name to select (examples):

Domain Users

Check Names

Advanced... OK Cancel

8 On the “Configure User Groups and Machine Groups” window click to the Next button



Configure NAP

Configure User Groups and Machine Groups

To grant or deny access to groups of computers, add groups to Machine Groups. To grant or deny access to groups of users, add groups to User Groups. You can configure both Machine Groups and User Groups for this policy.

If no groups are selected, this policy applies to all users.

Machine Groups:

HACKME12\Domain Computers

Add... Remove

User Groups:


HACKME12\Domain Users

Add... Remove

Previous Next Finish Cancel

9 On the “Configure an Authentication Method” window check if the NPS server certificate is correct. Select “Secure Password (PEAP-MS-CHAP v2)” as authentication. If want to use later certificate based user authentication select the “Smart Card or other certificate (EAP-TLS)” too.

Configure NAP



Configure an Authentication Method

Protected Extensible Authentication Protocol (PEAP) is the authentication method used with wireless access points and authenticating switches. To configure PEAP, you must select a server certificate on the NPS server and you must configure an authentication type.

NPS Server Certificate

To select a server certificate issued by your organization trusted root certification authority (CA) or a public CA that is trusted by client computers, click Choose. To view the selected certificate, click View.

hackdc12.hackme12.local (Valid until 1/28/2015 3:17:25 PM)

View...

Choose...

EAP types:
Select EAP types to use with PEAP. The authentication type determines the kind of credentials that NPS can accept from client computers and users (either user name and password or a certificate).

☒ Secure Password (PEAP-MS-CHAP v2). This authentication type permits users to type password-based credentials during authentication.

☒ Smart Card or other certificate (EAP-TLS). This authentication type requires certificates on smart cards or in the client computer certificate store. For this authentication type you must deploy your own trusted root CA.

Previous


Next

Finish

Cancel

10 On the “Configure Traffic Controls” window next to the “Full access network” click to the “configure...” button.

Configure NAP



Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. Examples of traffic controls include virtual LANs (VLANs) or access control lists (ACLs). Your RADIUS client might also support other traffic control attributes. To configure these attributes, enter values for the full access network and the restricted access network.

If you do not use traffic controls or will configure them later, click Next.

Full access network

Configure RADIUS attributes for computers that are granted full network access.

Configure...

Restricted access network

Configure RADIUS attributes for computers that are granted restricted network access.

Configure...

Previous

Next

Finish

Cancel

11 On the “Configure RADIUS Attributes” window at the “RADIUS Standard Attributes” tab select “Tunnel-Type”, and click to the “Edit...” button.

Configure RADIUS Attributes

RADIUS Standard Attributes

Vendor-Specific Attributes

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.

Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	<not configured>
Tunnel-Medium-Type	<not configured>
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

Description:

Edit...

OK

Cancel

12 On the “Attribute Information” window click to the “Add...” button.

Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute values:

Vendor	Value
--------	-------

Add...

Edit...

Remove

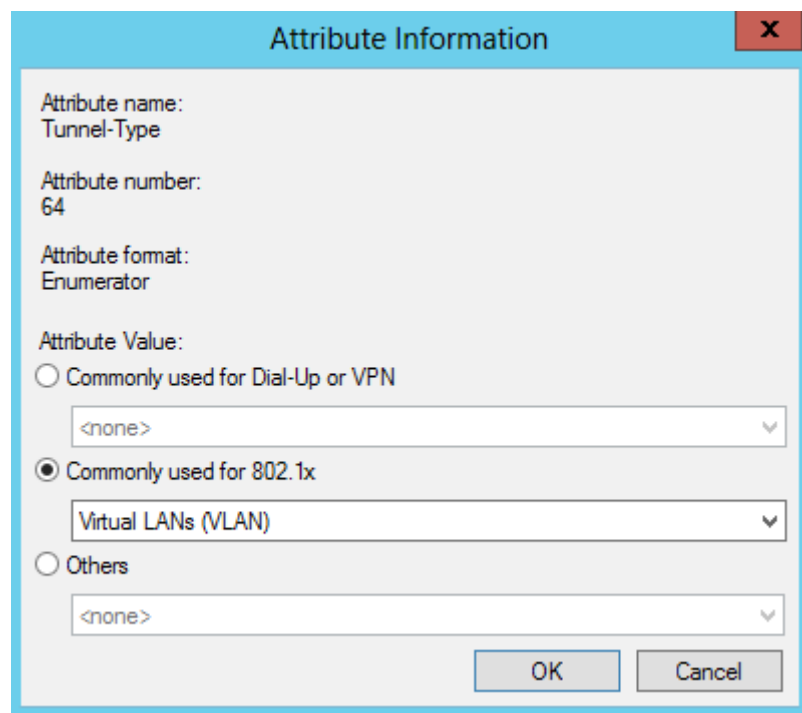
Move Up

Move Down

OK

Cancel

13 On the “Attribute Information” window select under the “Commonly used for 802.1x” the “Virtual LANs (VLAN)”.



The "Attribute Information" dialog box shows the configuration for the "Tunnel-Type" attribute. The attribute number is 64 and the format is Enumerator. Under the "Commonly used for 802.1x" section, "Virtual LANs (VLAN)" is selected in the dropdown menu. The "OK" and "Cancel" buttons are at the bottom right.

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute Value:

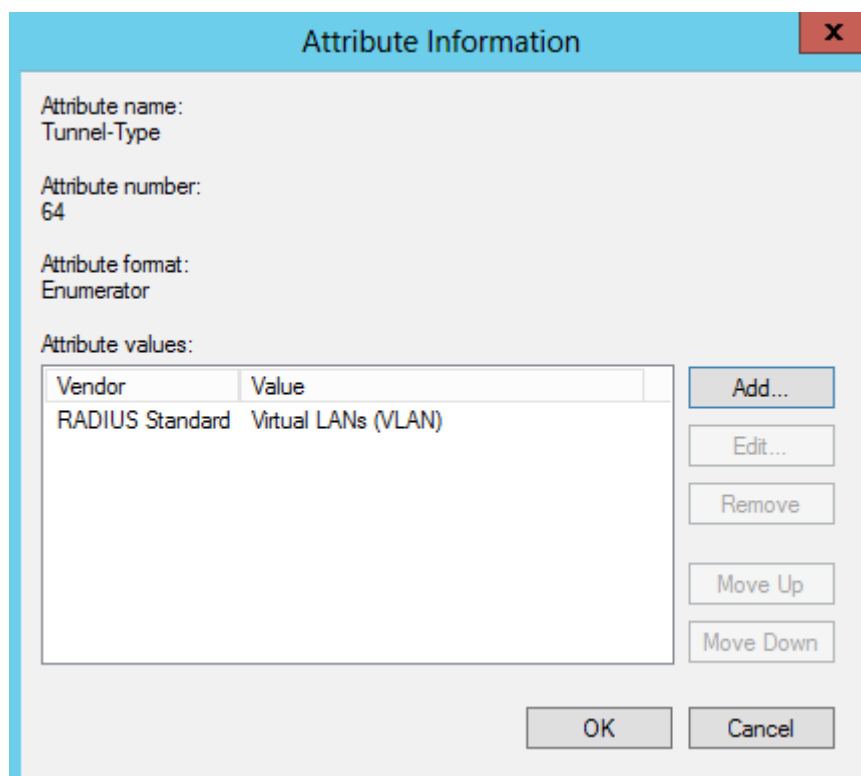
☐ Commonly used for Dial-Up or VPN
<none>

☒ Commonly used for 802.1x
Virtual LANs (VLAN)

☐ Others
<none>

OK Cancel

14 Click OK on the “Attribute Information” window



The "Attribute Information" dialog box shows the configuration for the "Tunnel-Type" attribute. The attribute number is 64 and the format is Enumerator. The "Attribute values" section contains a table with one row: "RADIUS Standard" and "Virtual LANs (VLAN)". To the right of the table are buttons for "Add...", "Edit...", "Remove", "Move Up", and "Move Down". The "OK" and "Cancel" buttons are at the bottom right.

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

Add...
Edit...
Remove
Move Up
Move Down

OK Cancel

15 On the “Configure RADIUS Attributes” window at the “RADIUS Standard Attributes” tab select “Tunnel-Medium-Type”, and click to the “Edit...” button.

Configure RADIUS Attributes [X]

RADIUS Standard Attributes | Vendor-Specific Attributes

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.

Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	<not configured>
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the transport medium used when creating a tunnel for protocols (for example, L2TP) that can operate over multiple transports.

Edit...

OK Cancel

16 On the “Attribute Information” window click to the “Add...” button.

Attribute Information [X]

Attribute name:
Tunnel-Medium-Type

Attribute number:
65

Attribute format:
Enumerator

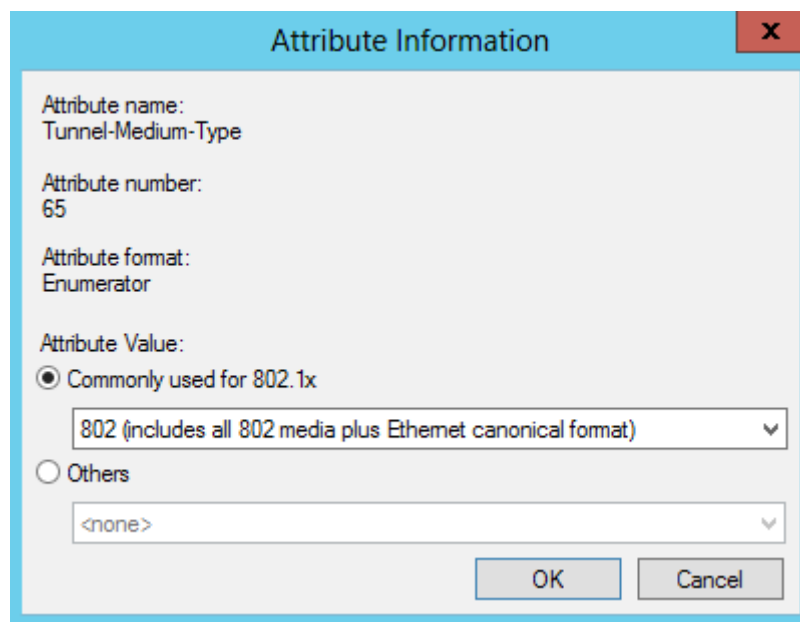
Attribute values:

Vendor	Value
--------	-------

Add...
Edit...
Remove
Move Up
Move Down

OK Cancel

17 On the “Attribute Information” window select under the “Commonly used for 802.1x” the “802 (includes all 802 media plus Ethernet canonical format)”.

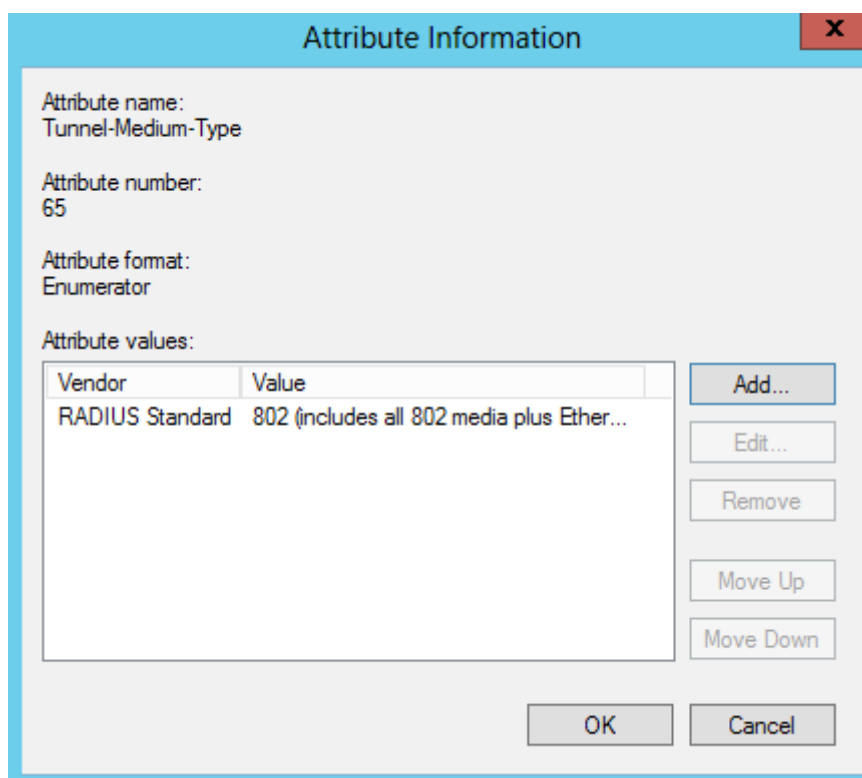


The "Attribute Information" dialog box is shown. It has a title bar with a close button (X). The fields are as follows:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerator
- Attribute Value:
 - ☒ Commonly used for 802.1x
 - 802 (includes all 802 media plus Ethernet canonical format)
 - ☐ Others
 - <none>

Buttons: OK, Cancel

18 Click OK on the “Attribute Information” window



The "Attribute Information" dialog box is shown. It has a title bar with a close button (X). The fields are as follows:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerator
- Attribute values:

Vendor	Value
RADIUS Standard	802 (includes all 802 media plus Ether...

Buttons: Add..., Edit..., Remove, Move Up, Move Down, OK, Cancel

19 On the “Configure RADIUS Attributes” window at the “RADIUS Standard Attributes” tab select “Tunnel-Pvt-Group-ID”, and click to the “Edit...” button.

Configure RADIUS Attributes

RADIUS Standard Attributes | Vendor-Specific Attributes

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.

Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the Group ID for a tunneled session.

Edit...

OK Cancel

20 On the “Attribute Information” window click to the “Add...” button.

Attribute Information

Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

Attribute values:

Vendor	Value
--------	-------

Add...

Edit...

Remove

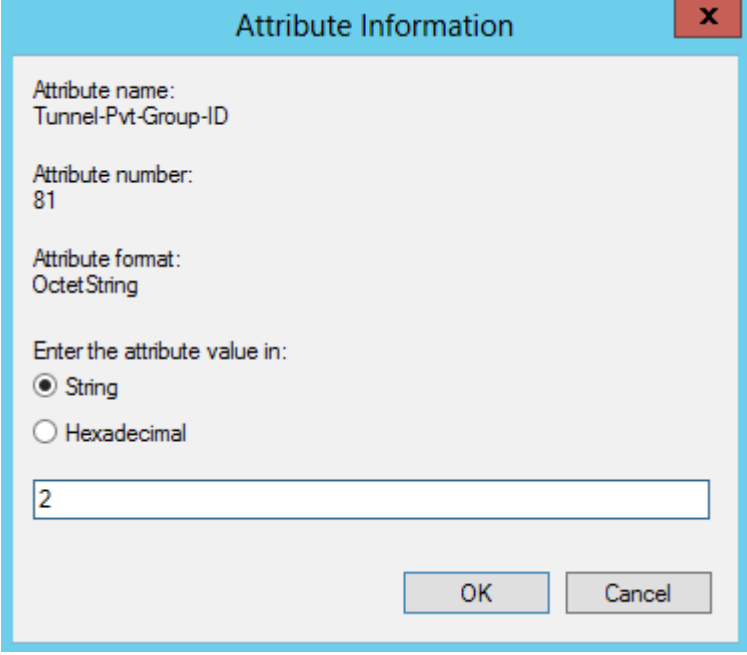
Move Up

Move Down

OK Cancel

21 On the “Attribute Information” window type “2” as value (the compliant computers will be the

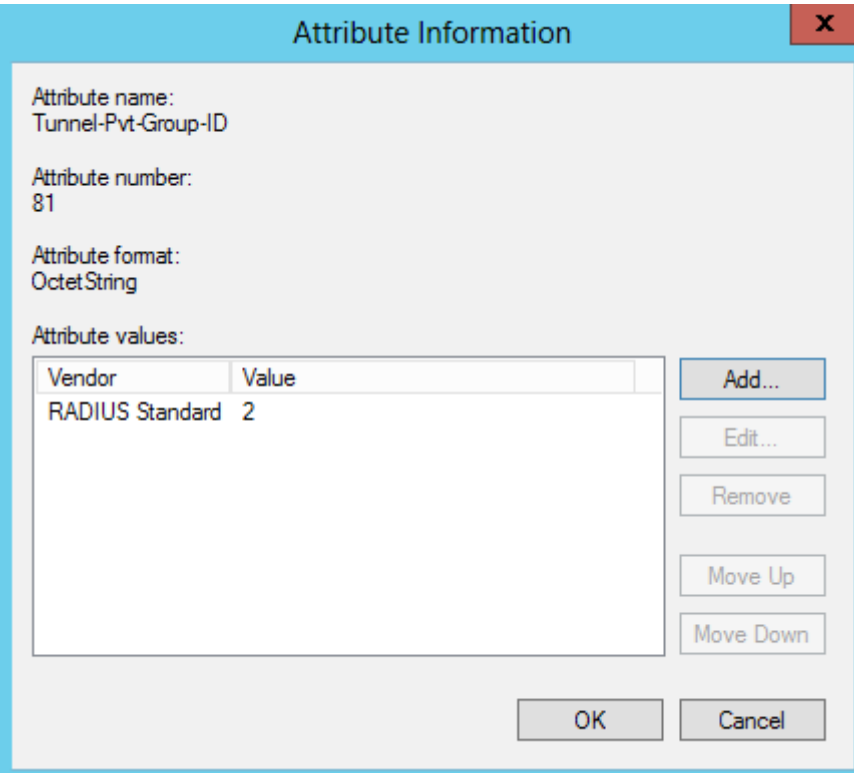
member of VLAN 2). Then click to the OK button.



The "Attribute Information" dialog box has a light blue title bar with a red close button. The main area is light gray and contains the following fields and controls:

- Attribute name:** Tunnel-Pvt-Group-ID
- Attribute number:** 81
- Attribute format:** OctetString
- Enter the attribute value in:**
 - ☒ String
 - ☐ Hexadecimal
- Value input field:** A text box containing the number "2".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

22 On the “Attribute Information” window click to the OK button



The "Attribute Information" dialog box is shown with a table for attribute values. The table has two columns: "Vendor" and "Value". The first row contains "RADIUS Standard" and "2". To the right of the table are five buttons: "Add...", "Edit...", "Remove", "Move Up", and "Move Down". The "OK" and "Cancel" buttons are at the bottom right.

Vendor	Value
RADIUS Standard	2

23 On the “Configure RADIUS Attributes” window click to the OK button.

Configure RADIUS Attributes

RADIUS Standard Attributes

Vendor-Specific Attributes

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.

Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	2
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the tunnel to which a session is assigned.

Edit...

OK

Cancel

24 On the “Configure Traffic Controls” window next to the “Restricted access network” click to the “configure...” button.

Configure NAP

Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. Examples of traffic controls include virtual LANs (VLANs) or access control lists (ACLs). Your RADIUS client might also support other traffic control attributes. To configure these attributes, enter values for the full access network and the restricted access network.

If you do not use traffic controls or will configure them later, click Next.

Full access network
Configure RADIUS attributes for computers that are granted full network access.

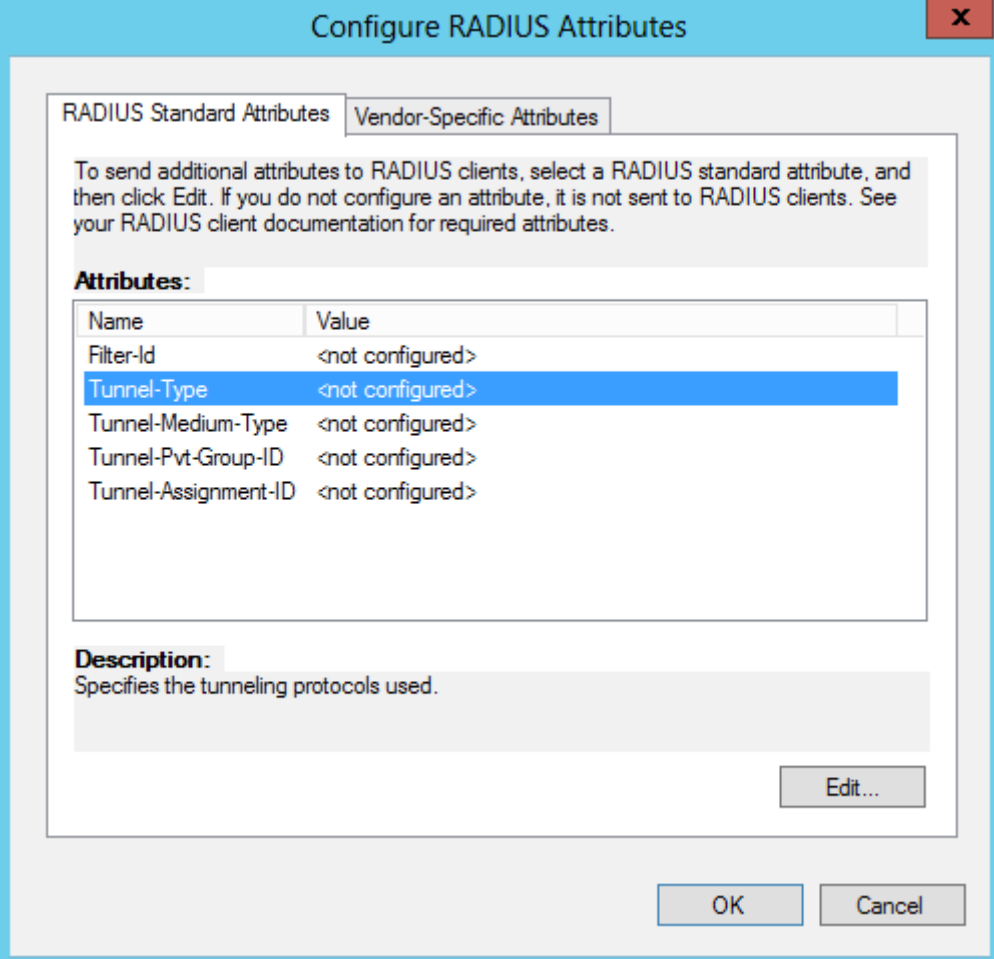
Configure...

Restricted access network
Configure RADIUS attributes for computers that are granted restricted network access.

Configure...

Previous Next Finish Cancel

25 On the “Configure RADIUS Attributes” window at the “RADIUS Standard Attributes” tab select “Tunnel-Type”, and click to the “Edit...” button.



Configure RADIUS Attributes

RADIUS Standard Attributes Vendor-Specific Attributes

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.

Attributes:

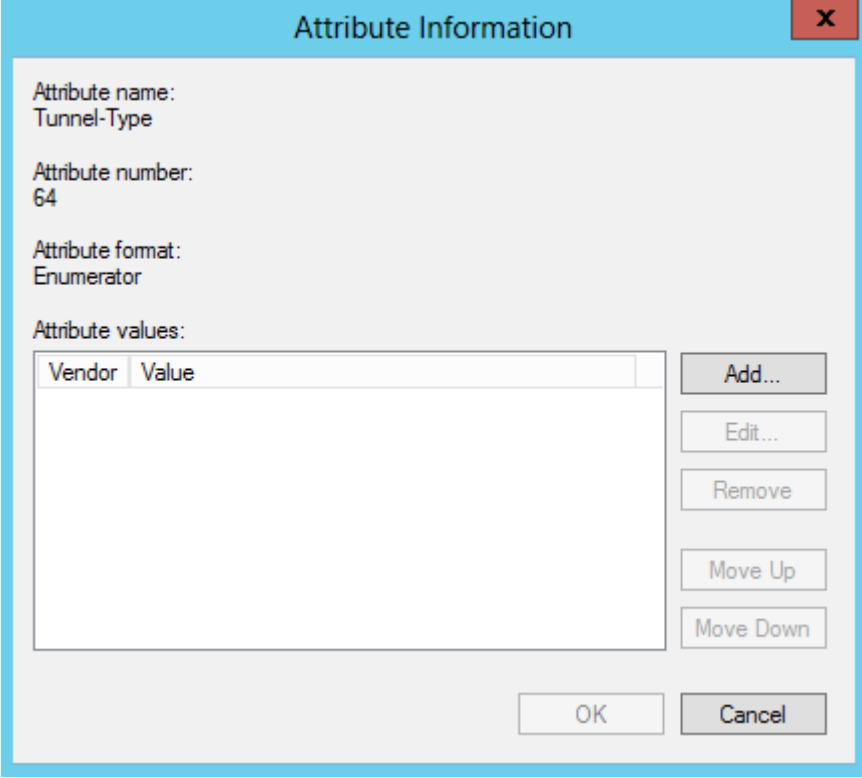
Name	Value
Filter-Id	<not configured>
Tunnel-Type	<not configured>
Tunnel-Medium-Type	<not configured>
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the tunneling protocols used.

Edit...

OK Cancel

26 On the “Attribute Information” window click to the “Add...” button.



Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute values:

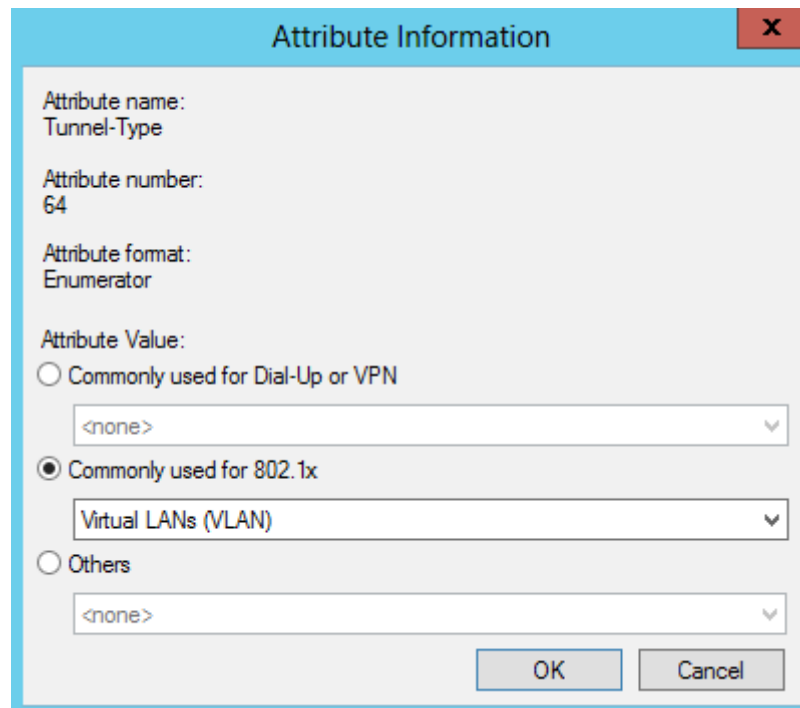
Vendor	Value
--------	-------

Add...
Edit...
Remove
Move Up
Move Down

OK Cancel

27 On the “Attribute Information” window select under the “Commonly used for 802.1x” the

“Virtual LANs (VLAN)”.

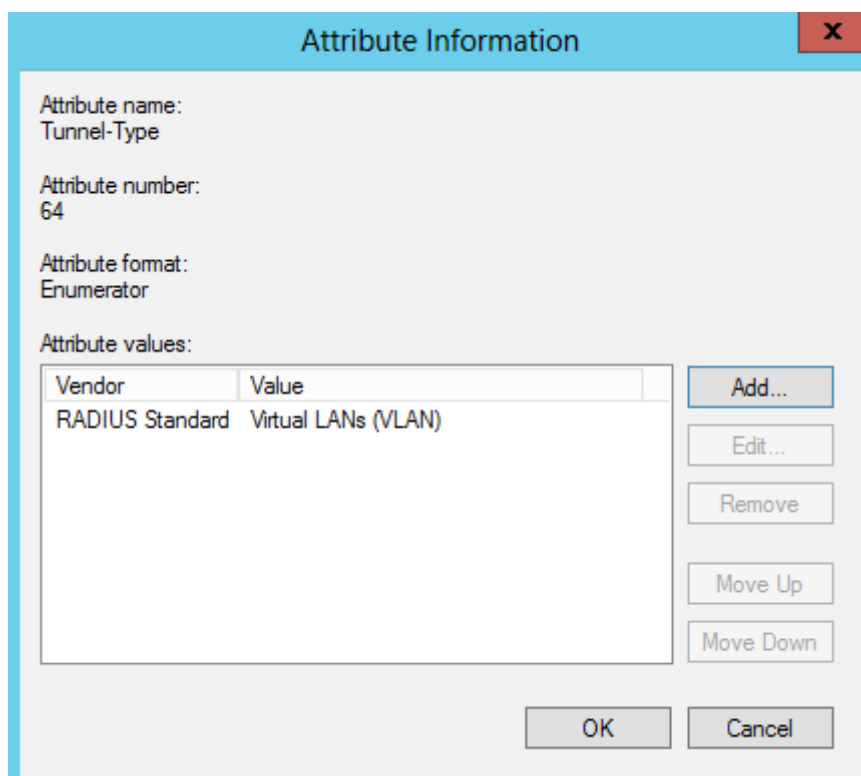


The "Attribute Information" dialog box is shown. It has a title bar with a close button (X). The fields are as follows:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute Value:
 - ☐ Commonly used for Dial-Up or VPN
 - <none>
 - ☒ Commonly used for 802.1x
 - Virtual LANs (VLAN)
 - ☐ Others
 - <none>

Buttons: OK, Cancel

28 Click OK on the “Attribute Information” window



The "Attribute Information" dialog box is shown. It has a title bar with a close button (X). The fields are as follows:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

Add...

Edit...

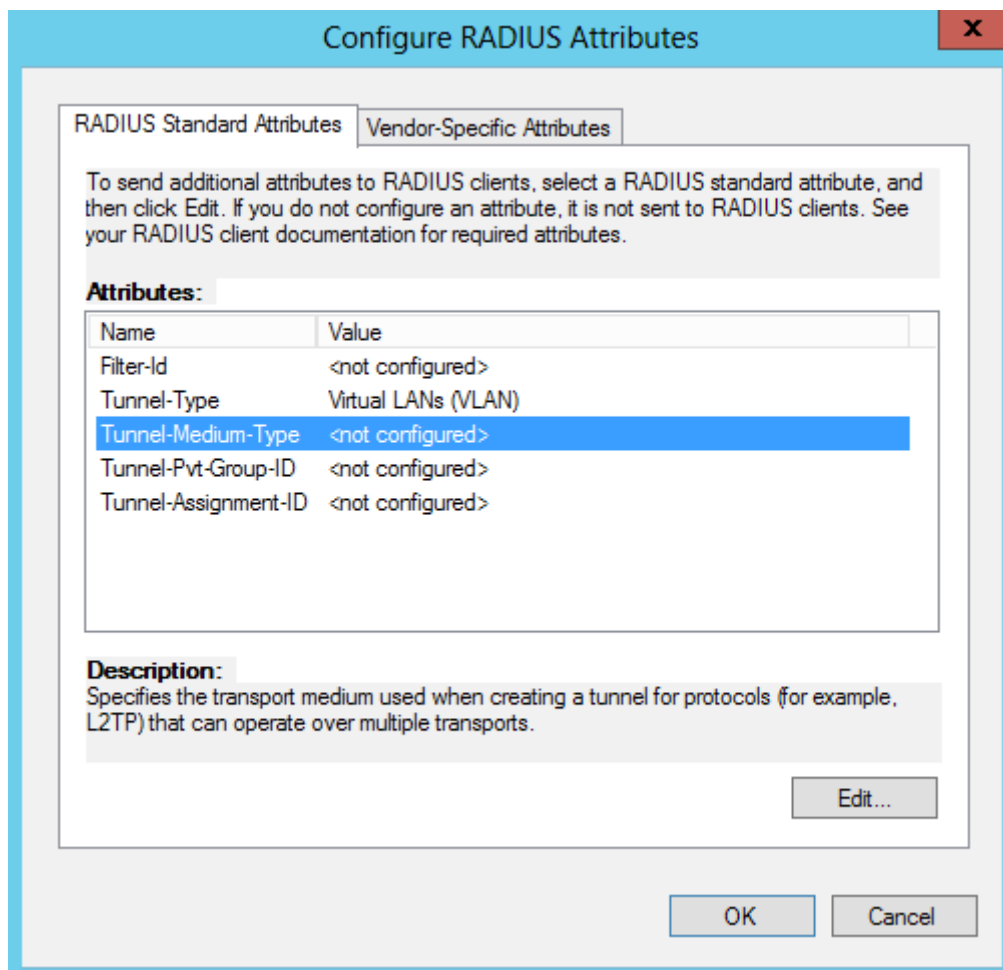
Remove

Move Up

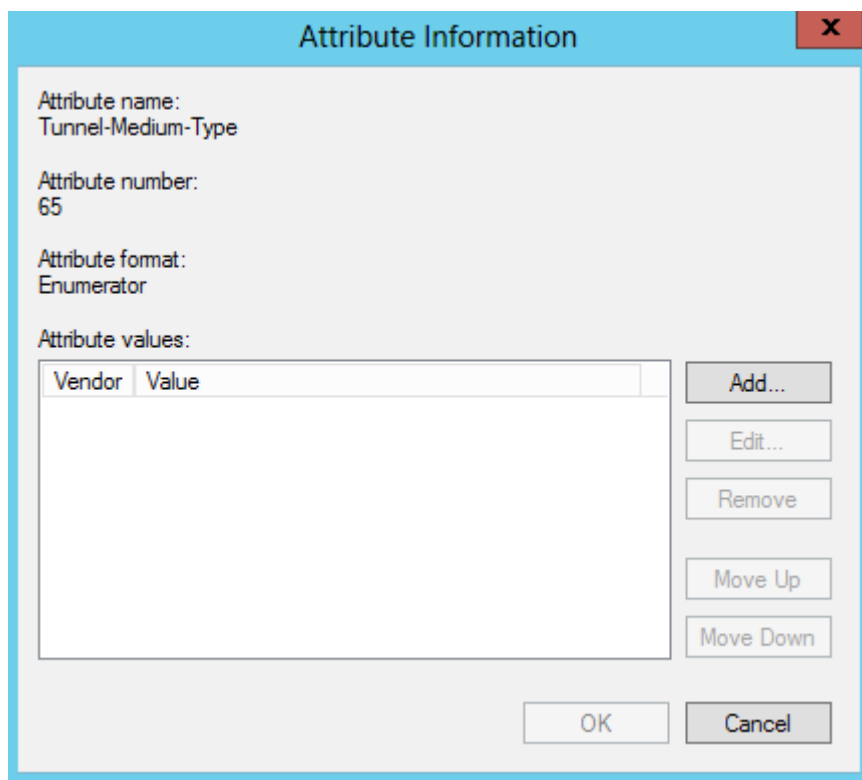
Move Down

Buttons: OK, Cancel

29 On the “Configure RADIUS Attributes” window at the “RADIUS Standard Attributes” tab select “Tunnel-Medium-Type”, and click to the “Edit...” button.

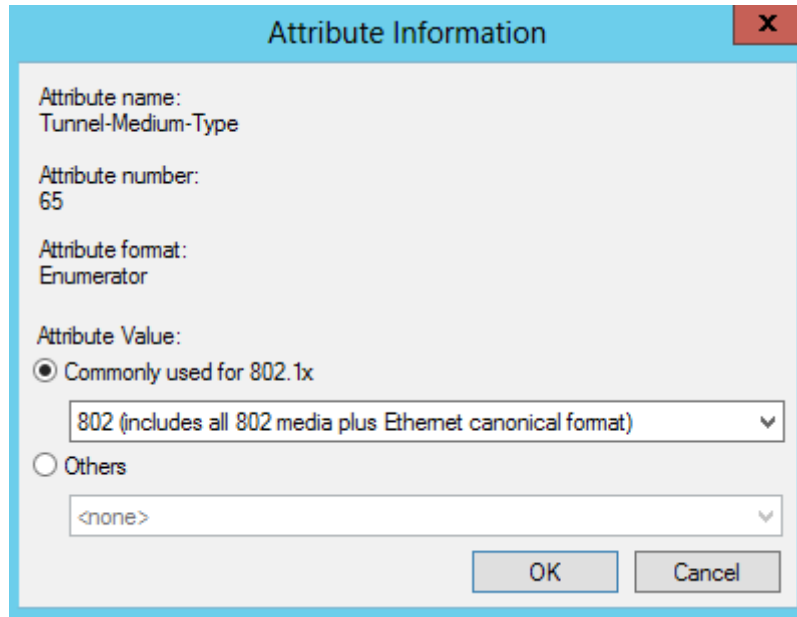


30 On the “Attribute Information” window click to the “Add...” button.



31 On the “Attribute Information” window select under the “Commonly used for 802.1x” the “802

(includes all 802 media plus Ethernet canonical format)”).

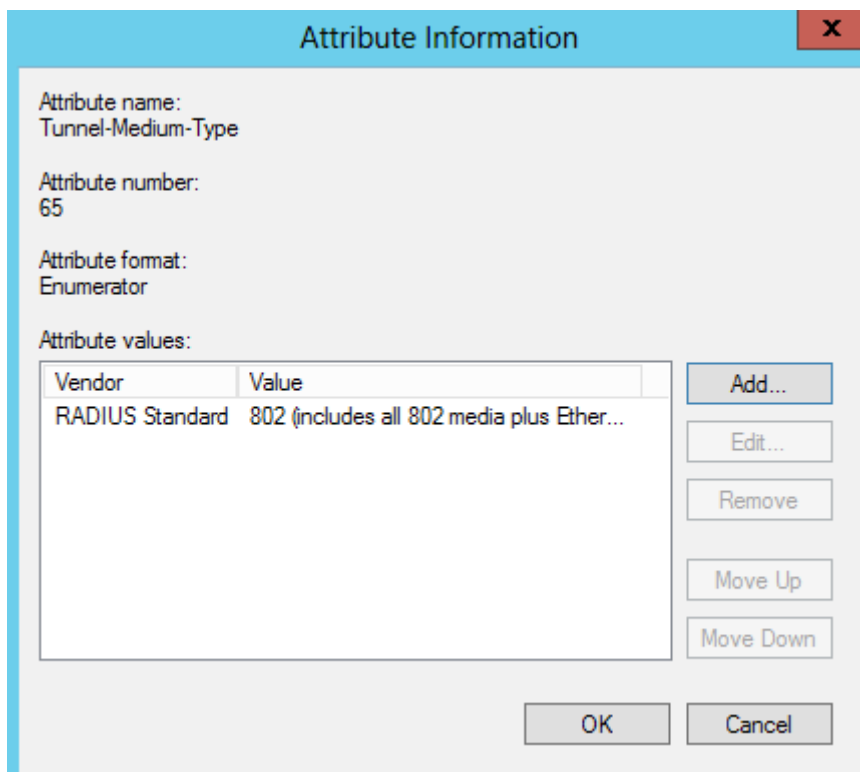


The "Attribute Information" dialog box displays the following fields:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerator
- Attribute Value:
 - ☒ Commonly used for 802.1x
 - 802 (includes all 802 media plus Ethernet canonical format)
 - ☐ Others
 - <none>

Buttons: OK, Cancel

32 Click OK on the “Attribute Information” window



The "Attribute Information" dialog box displays the following fields:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerator
- Attribute values:

Vendor	Value
RADIUS Standard	802 (includes all 802 media plus Ether...

Add...

Edit...

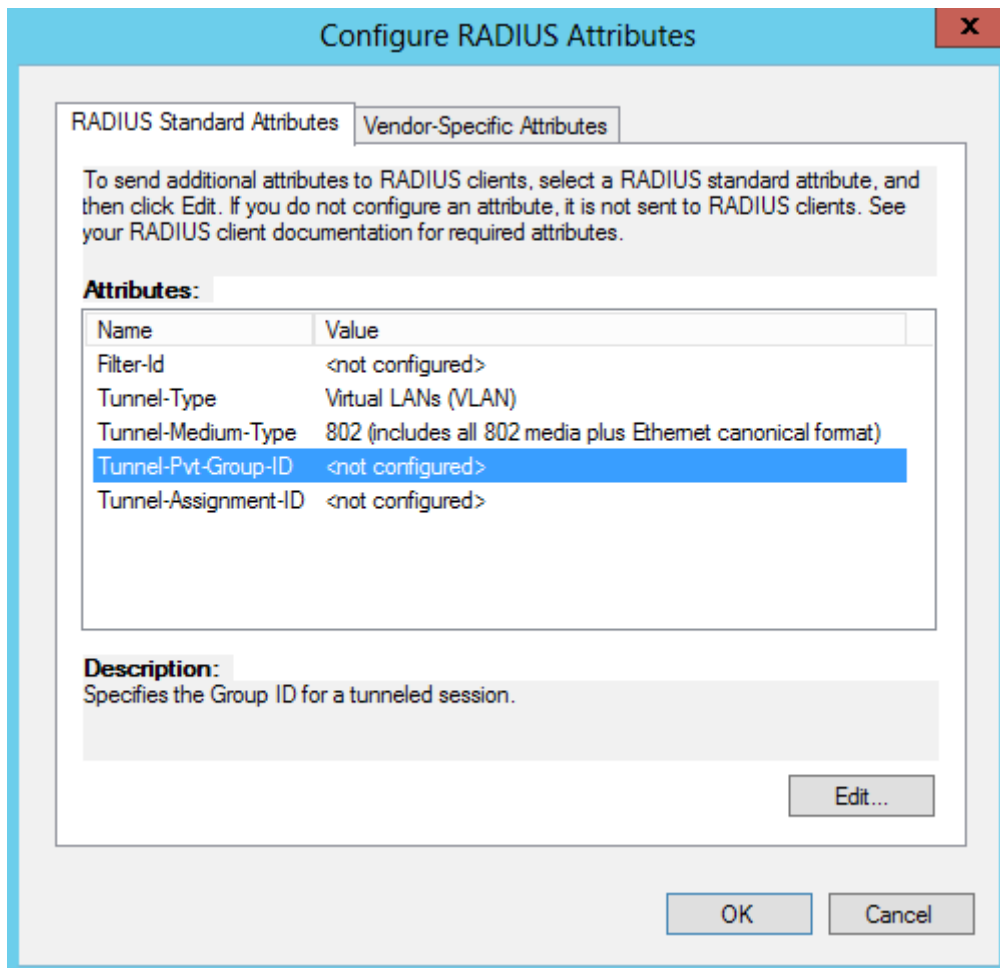
Remove

Move Up

Move Down

Buttons: OK, Cancel

33 On the “Configure RADIUS Attributes” window at the “RADIUS Standard Attributes” tab select “Tunnel-Pvt-Group-ID”, and click to the “Edit...” button.



Configure RADIUS Attributes

RADIUS Standard Attributes | Vendor-Specific Attributes

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.

Attributes:

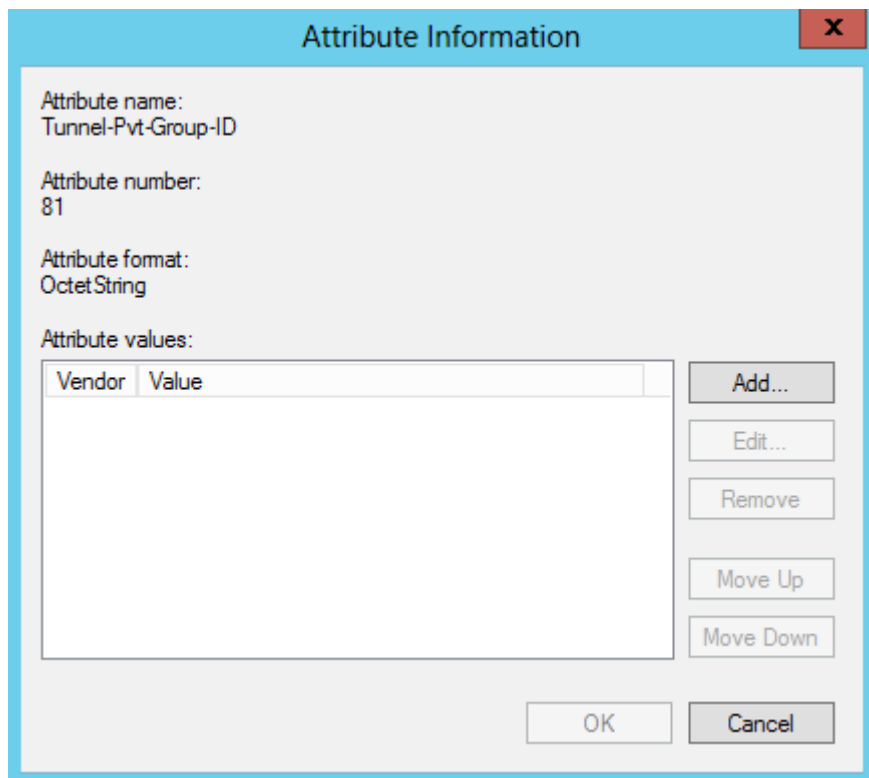
Name	Value
Filter-Id	<not configured>
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the Group ID for a tunneled session.

Edit...

OK Cancel

34 On the “Attribute Information” window click to the “Add...” button.



Attribute Information

Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
Octet String

Attribute values:

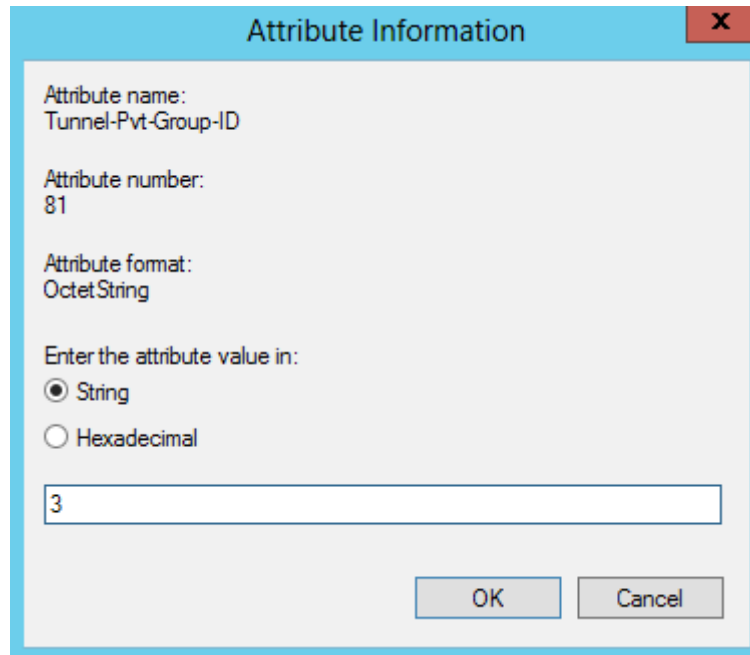
Vendor	Value
--------	-------

Add...
Edit...
Remove
Move Up
Move Down

OK Cancel

35 On the “Attribute Information” window type “3” as value (the compliant computers will be the

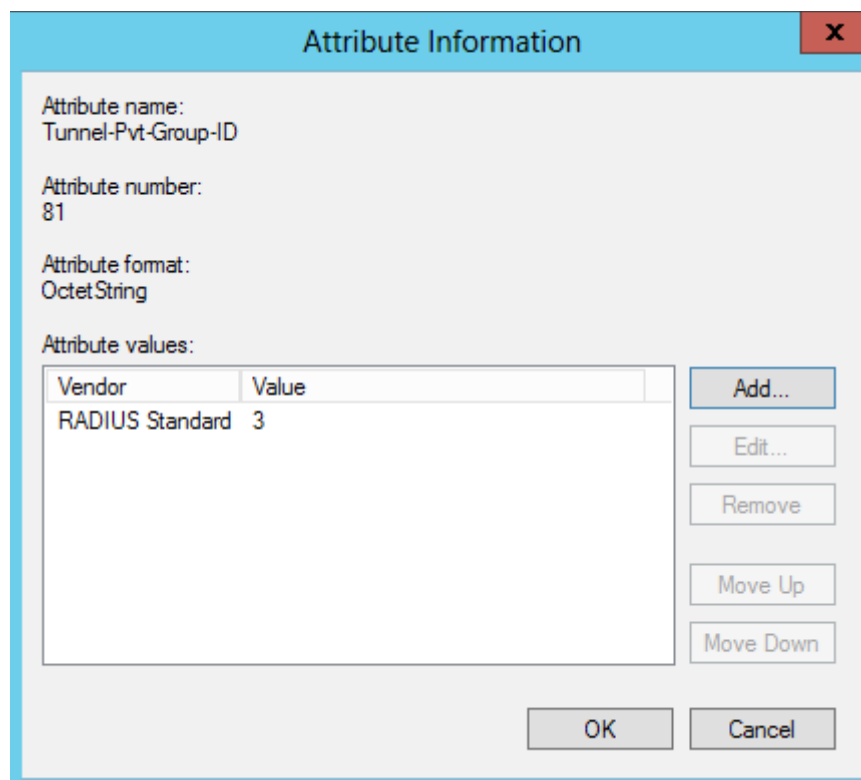
member of VLAN 3). Then click to the OK button.



The "Attribute Information" dialog box has a title bar with a close button (X). It contains the following fields and controls:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Enter the attribute value in:
 - ☒ String
 - ☐ Hexadecimal
- A text input field containing the value "3".
- OK and Cancel buttons at the bottom right.

36 On the “Attribute Information” window click to the OK button



The "Attribute Information" dialog box is shown with a table for attribute values. The table has two columns: "Vendor" and "Value". The first row contains "RADIUS Standard" and "3". To the right of the table are buttons for "Add...", "Edit...", "Remove", "Move Up", and "Move Down". The "OK" and "Cancel" buttons are at the bottom right.

Vendor	Value
RADIUS Standard	3

37 On the “Configure RADIUS Attributes” window click to the OK button.

Configure RADIUS Attributes

RADIUS Standard Attributes

Vendor-Specific Attributes

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.

Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	3
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the Group ID for a tunneled session.


Edit...

OK

Cancel

38 On the “Configure Traffic Controls” window click to the “Next” button

Configure NAP



Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. Examples of traffic controls include virtual LANs (VLANs) or access control lists (ACLs). Your RADIUS client might also support other traffic control attributes. To configure these attributes, enter values for the full access network and the restricted access network.

If you do not use traffic controls or will configure them later, click Next.

Full access network

Configure RADIUS attributes for computers that are granted full network access.

Configure...

Restricted access network

Configure RADIUS attributes for computers that are granted restricted network access.

Configure...

Previous


Next

Finish

Cancel

39 On the “Define NAP health policy” select the “Window security health validator”. I cleared the “Enable auto remediation of client computers”, because it is easier to test on this way. Select the “Deny full network access to NAP-ineligible client computers...”

Configure NAP



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.

Previous

Next

Finish

Cancel

40 On the completing “NAP Enforcement Policy and RADIUS Client Configuration” window click to the finish button.



Completing NAP Enforcement Policy and RADIUS Client Configuration

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.

Health Policies:

NAP 802.1X (Wired) Compliant
NAP 802.1X (Wired) Noncompliant

Connection Request Policy:

NAP 802.1X (Wired)

Network Policies:

NAP 802.1X (Wired) Compliant
NAP 802.1X (Wired) Noncompliant
NAP 802.1X (Wired) Non NAP-Capable

[Configuration Details](#)

Previous

Next

Finish

Cancel