Configuring Wired 802.1x Authentication on Windows Server 2012

Johan Loos

johan@accessdenied.be

Version 1.0

Why 802.1x Authentication?

The purpose of this document is to guide you through the procedure how to enable 802.1x authentication to add an additional level of security when client computers are connecting to your local area network. Before a client computer has access to your network, the client computer needs be authenticated. If authentication is successful, the client computer is granted access. If authentication fails, the client computer has no or limited access. Clients can be authenticated using a password or a certificate.

802.1x authentication offers visibility since all clients are identified and authenticated. Offers security if the strongest authentication method is used and offers transparency because there is no involvement of the end-user.

Without proper access to your network, malicious users can use your network to access private data or launch attacks to servers or client computers on your network.
Example:
A consultant enters your company, plugs its computer into a socket wall, the client adapter request an IP address from a DHCP server which is located on the local area network. The client computers now have access to your network.

802.1x Authentication Overview

802.1x is an authentication framework to restrict unauthorized devices from connecting to the local area network. The authentication server authenticates each client connected to a switch port before the client can access any network resources.
Before the client can access network resources, only EAPOL traffic is allowed between the switch port and the client. If the client gets finally authenticated, normal traffic can flow through the switch port.

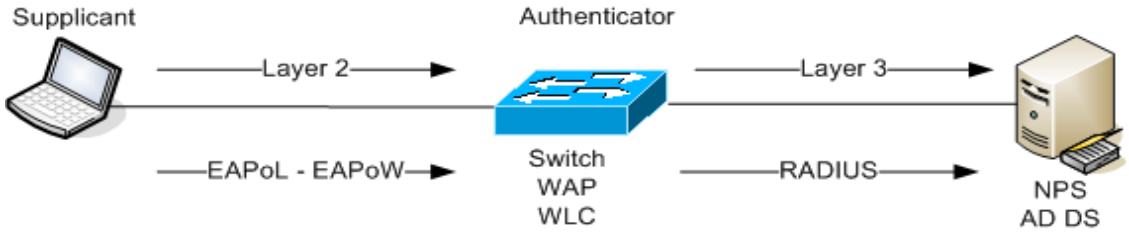
To protect your network, you have to use a proper authentication method:

- Authentication requires that the user provides some valid credentials such as username and password or a certificate stored on the client computer or smartcard.

Some components that you can use to protect the wired environment are:

- One or more 802.1x capable switches which are compatible with RADIUS
- Active Directory Domain Services for user and group management
- Active Directory Certificate Services for certificate management
- Network Policy Server to provide authentication, authorization and accounting

802.1x Components



Supplicant (workstation): Is a client that request access to the local area network and respond to requests from the switch.

Authentication server (NPS Server): This server actually authenticates the client. The authentication server validates the identity of the client and informs the switch if the client is authorized to access the local area network. The authentication server is basically a RADIUS server configured to support EAP authentication.

Authenticator (switch, wireless access point, wireless controller): Controls physical access to the network based on the authentication status of the client. This device relays the supplicant credentials to the authentication server.

EAP Protocol

EAPOL works at Layer 2 to authenticate a supplicant before access is granted on the network. EAPOL creates specialized EAP packets to allow EAP packets in the packet body. The goal of port based authentication is to transport the EAP-Method data which implements the actual authentication method.

EAP Packet Structure

Version	Type	Length	Packet Body

Version field identifies the version of the EAPOL protocol. The value is one octet in length and has the value '0000 0002'.

Type field identifies the type of packet being sent and is one octet in length.

EAP-Packet: '0000 0000'

EAPOL-Start: '0000 0001'

EAPOL-Logoff: '0000 0010'

EAPOL-Key: '0000 0011'

EAPOL-Encapsulated-ASF-Alert: '0000 0100'

Length field defines the length of the packet body and is two octets in length. For example an EAPOL Length field value of '0000 0000 0001 1010' indicates that the Packet Body field contains 22 octets of data.

Packet Body field is the payload portion

EAP Packet

Extensible Authentication Protocol is an authentication protocol which supports multiple authentication methods. It works at the Data link layer and does not need IP to operate.

EAP Header

Code	Identifier	Length	Data	Type

Code field specifies the type of EAP packet and is one 1 byte long. The six EAP packet types can be used:

Code	**Description**
x01	EAP-Request
x02	EAP-Response
x03	EAP-Success
x04	EAP-Failure
x05	EAP-Initiate
x06	EAP-Finish

Identifier field to match EAP-Response packets to Request packets and is one byte in length.

Length field includes the size of the EAP packets including EAP header and data fields and is two bytes long.

Data field is variable in length, can contain zero or more bytes as indicated in the Length field.

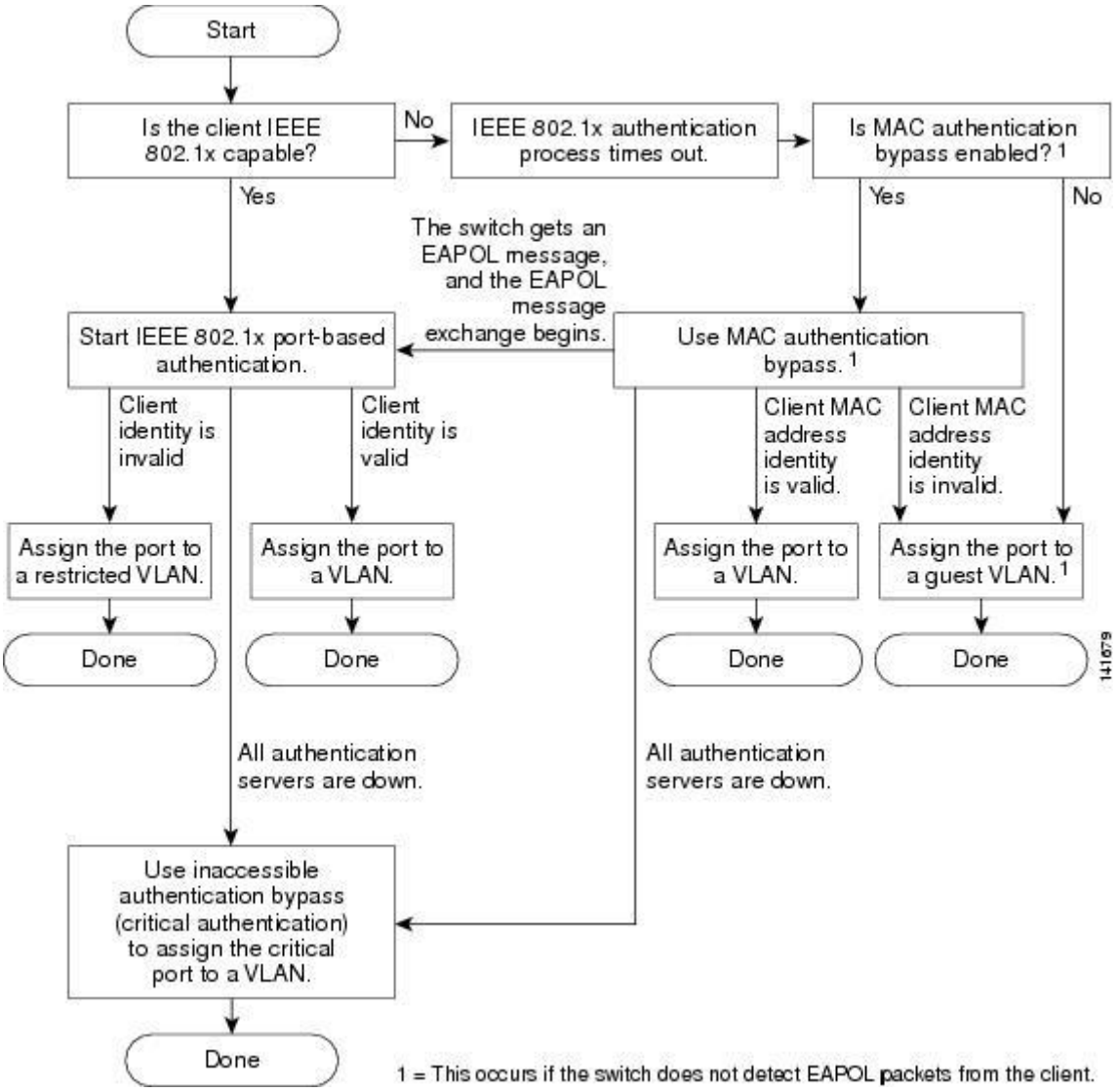
Type field defines the EAP packet type and is eight bits long.

Type	Description
1	Identity
2	Notification
3	NAK
4	MD5-Challenge
5	One-Time password
13	EAP-TLS
21	EAP-TTLS
25	PEAP
26	MS-EAP authentication
29	EAP-MSCHAP-V2
49	MS-IKEv2

Authentication process

When you enable 802.1x authentication, following events occur:

- If the identity of the client is valid and 802.1x authentication is successful, the switch grants the client access to the network
- If 802.1x authentication times out and MAC authentication bypass is enabled, the switch can use the MAC address of the client for authorization
- If the client cannot be identified and a restricted VLAN is specified, the switch can assign the client to the restricted VLAN



The switch re-authenticates the client when one of the following events occurs:

- Periodic re-authentication is enabled and the re-authentication timer expires
- You manually re-authenticate the client

User and Computer authentication

Authentication can be performed for a user, computer or both. The user or computer can be authenticated via passwords or certificates.

EAP-TLS

EAP-TLS requires client-side and server side certificates for mutual authentication.

1. Authentication server submits certificate to supplicant

2. Supplicant validates server certificate (check if the FQDN is the same as the name in the certificate and if the certificate is signed by a trusted CA, or that the certificate is not revoked
3. Supplicant submits certificate to server
4. Server validates the certificate of the supplicant

PEAP-EAP-MSCHAPv2

PEAP-EAP-MSCHAPv2 requires that the authentication server presents a certificate to the supplicant. The supplicant must have the Root CA of the CA that signed the authentication server certificate. It first creates a secure tunnel between the authentication server and the supplicant. This tunnel is created using a valid server certificate that the authentication server sends to the supplicant. Within this secure channel, a new EAP negotiation takes place to authenticate the client.

Authentication is based on a password, so this type of attack is susceptible to a dictionary attack.

1. Authentication server submits certificate to supplicant
2. Supplicant validates server certificate
3. Supplicant submits password through encrypted tunnel
4. Authentication server validates supplicant password

If the authentication server is unavailable, 802.1x fails and all supplicants will be denied access.

Authentication Initiation and Message Exchange

The connection can be initiated by the switch or by the client. The switch sends an EAP-request/identity frame to the client to request its identity. The client responds with an EAP-response/identity frame.

If the switch is not configured to supports 802.1x authentication and the client sends any EAPOL frames, these frames are dropped. If the client is configured to supports 802.1x authentication, and the client does not receive an EAP-request/identity frame after three

attempts, the client transmits frames as if the port is in authorized state. A port in authorized state means that the client has been successfully authenticated.

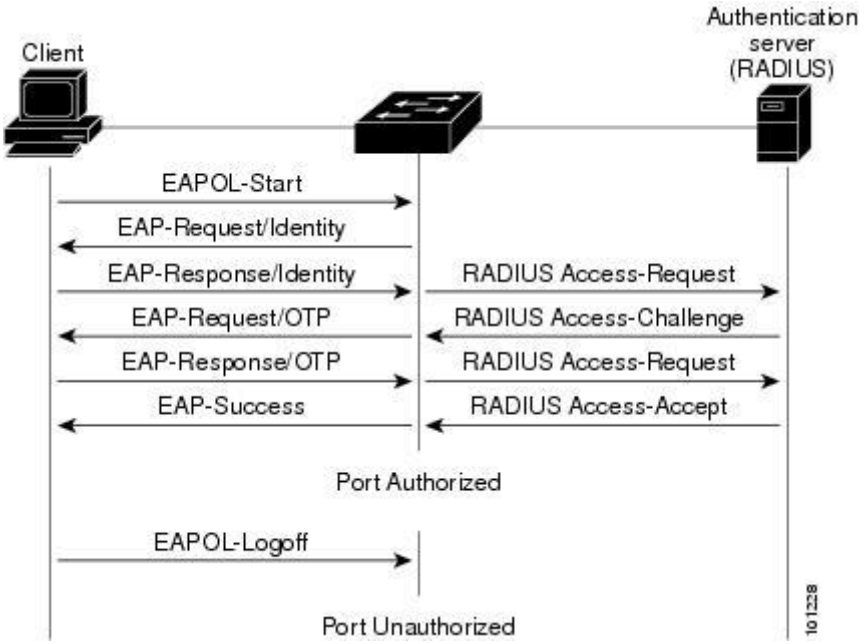
When the client supplies its identity, the switch passes EAP frames between the client and authorization server until authorization fails or succeeds.

If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network. If the switch gets an invalid identity from an 802.1x capable client, the switch can assign the client to a restricted VLAN that provides limited services.

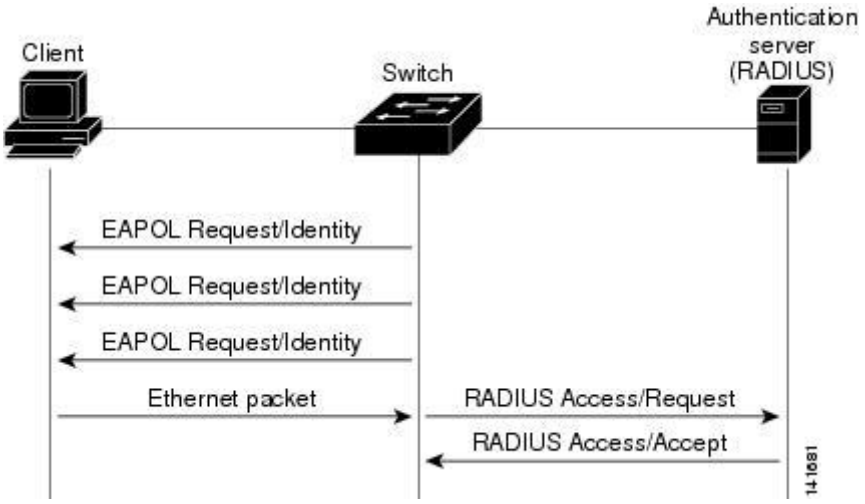
The switch can re-authenticate the client at regular times or when the re-authentication timer expires. You can configure the switch to use timers based on Session-Timeout (attribute 27) and the Termination-Action (attribute 29). Session-Timeout specifies the time when re-authentication occurs and Termination-Action specifies the action to take during re-authentication. The action can be *Initialize* or *Re-Authenticate*. When you set the Initialize action, the 802.1x session ends and the client will lose connectivity. When you set Re-Authenticate, the client will not lose the connection and simple re-authenticates.

Do not use Re-authentication and session timers if you are using MAB. The switch does not re-learn the MAC address but sends the previously learned MAC address to the RADIUS server. If you use these timers, MAB succeeds when 802.1x authentication fails. So at this point, the client loses connectivity.

Message exchange process



Message Exchange during MAC authentication bypass



Ports in authorized and unauthorized states

The switch port state determines if the client is authorized to access the local area network or not. The port starts in unauthorized state. In this state, the port disallows all traffic except for 802.1x frames. When a client is successfully authenticated, the port is in authorized state and allows all traffic from the client to the switch.

If a client does not support 802.1x authentication and connects to an unauthorized port, the switch request the client's identity. In this case, the client cannot responds to the request and the port remains in unauthorized state. The client is not granted access to the network.

When an 802.1x enabled client connects to a port which is not enabled for 802.1x authentication. The client initiates the authentication process by sending the EAPOL-start frame. When the client does not receive a response from the switch, then client sends the request for a number of times.

You can control the port authorization state by using dot1x port-control interface configuration command:
Force-authorized: Disable 802.1x authentication and causes the port to the authorized state without any authentication exchange required.
Force-unauthorized: Causes the port to remain in unauthorized state, ignoring all attempts by the client to authenticate.
Auto: Enable 802.1x authentication and causes the client to begin in the authorized state, allowing only EAPOL traffic to be sent and receive through the port.

When the client receives an accept frame from the authentication server, the client is successfully authenticated and the state of the switch port is set to authorized. If the authentication fails, the switch port remains in unauthorized state, but the client is able to retry the authentication process.

If the authentication server cannot be reached, the switch will retransmit the request. If the switch does not receive any responses from the authentication server after a specific number of attempts, the authentication will fail and the client is not able to access resources on the local area network.

When a client logs of, the client sends an EAP-logoff message, and the switch changes this port back to unauthorized state.

Configuring 802.1X authentication on Catalyst 3560 Switch

```
addevsw01#config t
addevsw01(config)#aaa new-model
addevsw01(config)#aaa authentication dot1x default group radius
addevsw01(config)#aaa authorization network default group radius
addevsw01(config)#dot1x system-auth-control
addevsw01(config)#interface fa0/2
addevsw01(config-if)#switchport mode access
addevsw01(config-if)#authentication port-control auto
```

Configuring switch-to-RADIUS server communication

A RADIUS server is identified with its hostname or IP address and specific UDP port numbers for authentication and accounting.

The following configuration shows how to configure the switch to use a RADIUS server with IP address 10.32.5.15 to use port 1812 as authorization port and 1813 for accounting, and set the RADIUS secret to accessdenied

```
addevsw01(config)#radius-server host 10.32.5.15 auth-port 1812
acct-port 1813 key accessdenied
```

The RADIUS secret must match the secret key on the NPS server.

Enabling periodic re-authentication

You can also specify periodic 802.1x client re-authentication and how often it needs to be occurred. The number of seconds between re-authentication is by default 3600 seconds. The switch can re-authenticate the client at regular times or when the re-authentication timer expires. If the switch is configured to use a RADIUS server, you can configure the switch to use timers based on the following RADIUS attributes.

RADIUS Attribute	Value
[27] Session-Timeout	Value in seconds
[29] Termination-Action	Value in seconds

The Termination-Action specifies which action to take during re-authentication. Possible actions are Initialize and Re-authenticate. When you use Initialize, the 802.1x session ends

and connectivity is lost during re-authentication. When you use Re-authenticate the session is not affected during re-authentication.

This configuration shows how to enable periodic re-authentication and set the number of seconds between re-authentication attempts to 4800

```
addevsw01(config)#int fa0/2
addevsw01(config-if)#authentication periodic
addevsw01(config-if)#authentication timer reauthenticate 4800
```

You can manually re-authenticate the client computer connected to a specific port at any time by entering the following command:

```
addevsw01(config)#dot1x re-authenticate int fa0/2
```

Configuring the quiet period

When the switch is not able to authenticate the client, the switch remains idle for a period of time, and then tries again. The idle time is determined with the quiet period.

This example shows how to configure the switch with a quiet time of 30 seconds.

```
addevsw01(config)#int fa0/2
addevsw01(config-if)#dot1x timeout quiet-period 30
```

Configuring the switch-to-client retransmission time

Dot1x timeout tx-period

Before authentication can take place, the switch sends an EAP-request/identify frame to the client. The client responds with an EAP-response/identity frame. If the switch does not receive a message within a period of time, the switch retransmits the frame.

You can configure the default retransmission time as follow:

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#dot1x timeout tx-period 30
```

Dot1x max-reauth-req:

The number of times the switch resends the request-identity frame

The default value for dot1x timeout is 30 seconds and dot1xmax-reauth-req is 2. Based on timeout = (max-reauth-req + 1) x tx-period. It takes 90 seconds for a supplicant to get access

through mac authentication bypass on guest vlan. When this timeout expired and MAB is configured, MAC authentication can takes place.

Authentication timer restart:

If 802.1x timeouts on the fallback mechanism fails or has been configured, the authenticator will wait a period of time. After this time, the authentication process starts over.

Enabling multiple hosts

You can attach multiple hosts to a single 802.1x enabled port. Only one of the attached hosts must be successfully authorized for all hosts to be granted network access.

If the port becomes un-authorized, all attached clients are denied access to the network.

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)# authentication host-mode multi-host
```

Display Statistics and Status

You can use following command to display statistics for a specific port:

```
addevsw01#show dot1x authentication int fa0/2
```

Using 802.1x Authentication with VLAN Assignment

You can limit network access by using VLAN assignment. After the switch authenticates the client on an 802.1x enabled port, the RADIUS server sends the VLAN ID to configure the switch port. This feature can be used to limit network access.

- When no VLAN is supplied by the RADIUS server or 802.1x authentication is disabled, the switch becomes access to its default VLAN.
- When incorrect VLAN information is supplied by the RADIUS server and 802.1x authentication is enabled, the switch place the switch port into unauthorized state to prevents ports to be member of another VLAN.
- When VLAN information is supplied correctly by the RADIUS server and 802.1x authentication is enabled, the switch port is configured with the VLAN after successful authentication.
- If multiple-hosts mode is enabled on the switch port, all hosts are placed in the same VLAN as the first authenticated host.

It is important that VLAN 1 or management VLAN is not the default VLAN. If authentication fails, the wired client can still access the network. Shutdown all switch ports which you don't use.

A RADIUS Server must return these attributes to the switch:

RADIUS Attribute	Value
[64] Tunnel-Type	VLAN
[65] Tunnel-Medium-Type	802
[81] Tunnel-Private-Group-ID	VLAN ID

Using 802.1x Authentication with Guest VLAN

You can use a Guest VLAN to provide limited access the clients. When you enable a Guest VLAN on the switch, the client becomes a member of the Guest VLAN is authentication cannot be performed. For example the client uses an Operating System that does not contains the 802.1x client.

When the client does not send an EAPOL frame or the switch does not receive a response to an EAP request/identity frame, the switch assigns the 802.1x port to the Guest VLAN. Guest VLANs are supported on single-host or multiple-hosts mode.

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event no-response action
authorize vlan 100
```

Using 802.1x Authentication with Restricted VLAN

If for some reason an IEEE 802.1x compliant client computer is not able to authenticate, the authentication process fails and the client can be placed into a restricted VLAN. This allows client computer to access limited resources in the restricted VLAN.

These clients are 802.1x compliant but fail the authentication process. For example, the certificate of the client computer has expired.

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event fail action authorize
vlan 99
```

When the client is not able to authenticate within 3 times, the switch places the switch port into the restricted VLAN. Users for which authentication fails, remains in the restricted VLAN until the next re-authentication occurs. At configured intervals, the switch port sends a re-authentication message. If re-authentication fails, the switch port remains in the restricted VLAN. Otherwise the switch port is configured in to configured VLAN or the VLAN ID sent by the RADIUS Server. Restricted VLANs are only supported in single-host mode.

Using a Filter-ID to create a VLAN ACL

You can use this attribute to assign an ACL to a client who is authorized on the RADIUS server. The ACL must exist on the switch before connection is filtered. In the example below, access to the IIS Web Services running on that server are denied. The syntax is as follows:

```
addevsw01(config)#access-list 101 deny tcp any host 10.32.5.3 eq www
addevsw01(config)#access-list 101 permit ip any any
```

Using Cisco-AV-Pair to create a VLAN ACL

You can also use the Cisco-AV-Pair attribute to configure downloadable ACLs. This means that the ACLs don't need to be exists on the switch, but are downloaded to the authorized client computer. In the example below, access to the IIS Web Services running on that server are denied. The syntax is as follows:

```
ip:inacl#201=deny tcp any host 10.32.5.3 eq www
ip:inacl#201=permit ip any any
```

Using 802.1x Authentication with Port Security

When you enable 802.1x on a switch port and the switch port is additionally configured with port security; first authentication takes place and port security manages network access for all MAC addresses.

Interaction between 802.1x authentication and port security:

- When the client is authenticated and port security table is not full, the MAC address of the client is added to the list of secure hosts. The switch port comes up normally.
- When the client is authenticated and port security table is full, the switch port shuts down.

- When the client logs off, all entries in the secure host table are cleared and the switch port change to unauthenticated state.
- If you administratively shutdown a switch port, all entries are removed from the secure host table and the switch port becomes unauthenticated.

You can configure 802.1x authentication with port security in single-host or multiple-hosts mode.

```
addevsw01(config-if)#switchport port-security mac-address mac-address
```

Using 802.1x authentication using MAC Authentication Bypass (MAB)

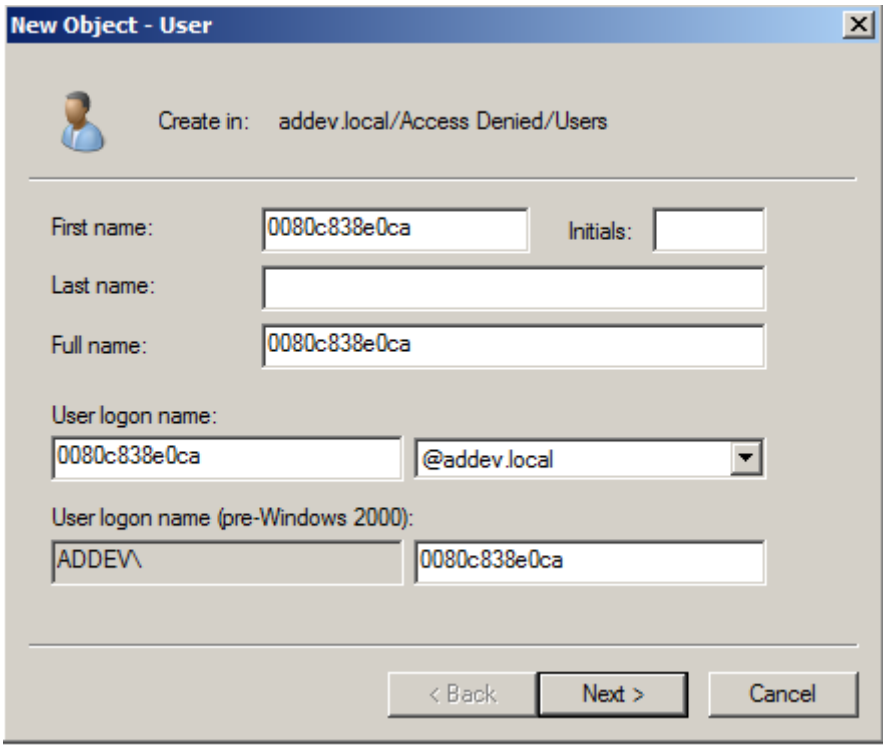
You can configure an 802.1x enabled port on the switch to authorize clients based on the MAC address. You can use Active Directory as a MAC address database for which are allowed to access the network. When the client connects to the switch, the RADIUS Server sends a RADIUS access/request message with a username and password based on the MAC address. If authorization is successful, the switch allows the client access to the network. If authorization fails, the switch assigns the client to the Guest VLAN.

If the switch detects an EAPOL frame from an 802.1x capable client, the switch uses 802.1x authentication instead of MAC authentication bypass.

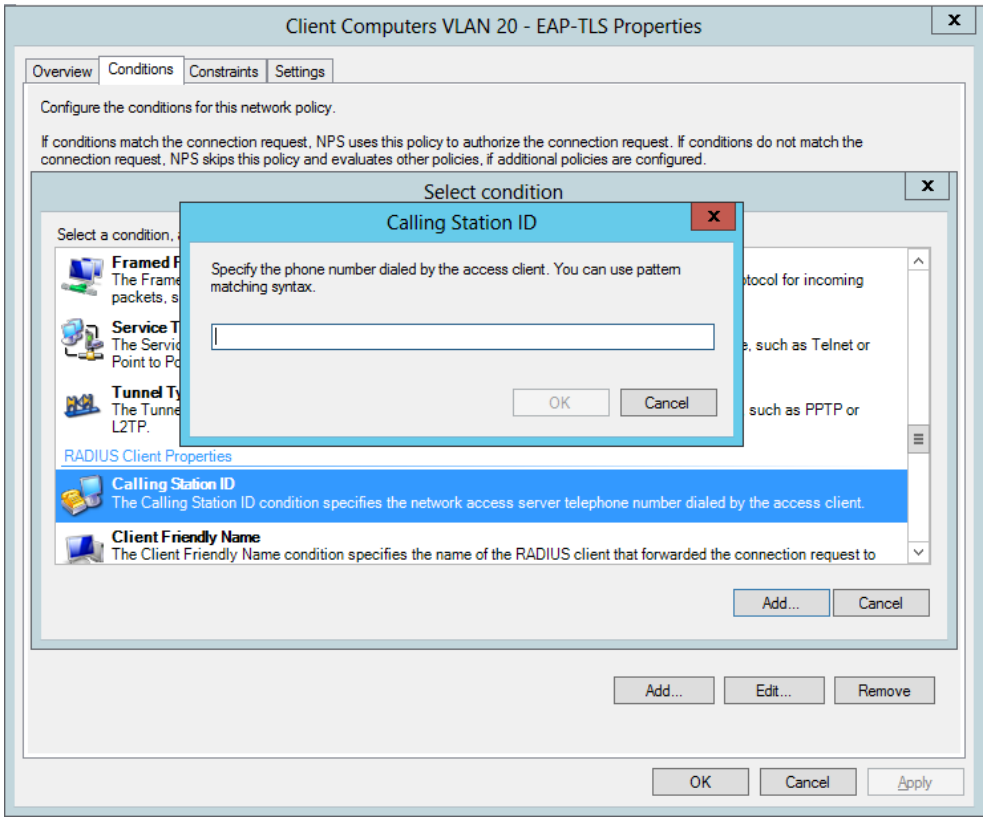
If the switch already authorized a port using MAC authentication bypass and detects an 802.1x capable client, the switch does not unauthorized the client. When re-authentication occurs, the switch uses 802.1x authentication as preferred method.

Clients that where authorized with MAC authentication bypassed can be re-authenticated. If re-authentication is successful, the switch keeps the port in the same VLAN. Otherwise the switch assigns the port to the Guest VLAN.

You need to create a domain user and password in Active Directory for all your clients which need to be authenticated via MAB.



To be able to authenticate those clients with only the MAC information, you need to create a policy on NPS which includes the **Calling Station ID** as condition.



To authenticate users, you need only unencrypted authentication and disable all the others.

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#mab
```

Before MAB is in place, the port enabled for MAB must be timeout on 802.1x authentication first.

RADIUS Message Types

Access-Request: Sent by a RADIUS client to request authentication and authorization for a network access connection attempt.

Access-Accept: Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is authenticated and authorized.

Access-Reject: Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is rejected. A RADIUS server sends this message if either the credentials are not authentic or the connection attempt is not authorized.

Access-Challenge: Sent by a RADIUS server in response to an Accept-Request message. This message is a challenge to the RADIUS client that requires a response.

Accounting-Request: Sent by a RADIUS client to specify accounting information for a connection that was accepted.

Accounting-Response: Sent by the RADIUS server in response to the Accounting-Request message. This message acknowledges the successful receipt and processing of the Accounting-Request message.

IP Address Assignment

After successful authentication, the wired client needs to receive an IP address before further communication can takes place. The client can receives an IP address from a DHCP server available on the network or from a DHCP server configured on your switch or other network device. In this paper, we use a Microsoft DHCP Server and create the necessary scopes.

Creating VLANs

Before you assign VLAN ID attribute via RADIUS you need to configure the required VLANs on your switch.

The following creates a VLAN 5

```
addevsw01(config)#vlan 5
```

The following creates a VLAN 10

```
addevsw01(config)#vlan 10
```

The following creates a VLAN 20

```
addevsw01(config)#vlan 20
```

The following creates a VLAN 99

```
addevsw01(config)#vlan 99
```

The following creates a VLAN 100

```
addevsw01(config)#vlan 100
```

Assigning IP address

Assign an IP address to the interface of VLAN 5

```
addevsw01(config)#interface vlan 5
addevsw01(config-if)#ip address 10.32.5.254 255.255.255.0
addevsw01(config-if)#no shutdown
```

Assign an IP address to the interface of VLAN 10

```
addevsw01(config)#interface vlan 10
addevsw01(config-if)#ip address 10.32.10.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
addevsw01(config-if)#no shutdown
```

Assign an IP address to the interface of VLAN 20

```
addevsw01(config)#interface vlan 20
addevsw01(config-if)#ip address 10.32.20.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
```

```
addevsw01(config-if)#no shutdown
```

Assign an IP address to the interface of VLAN 99

```
addevsw01(config)#interface vlan 99
addevsw01(config-if)#ip address 10.32.99.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
addevsw01(config-if)#no shutdown
```

Assign an IP address to the interface of VLAN 100

```
addevsw01(config)#interface vlan 100
addevsw01(config-if)#ip address 10.32.100.254 255.255.255.0
addevsw01(config-if)#ip helper-address 10.32.5.3
addevsw01(config-if)#no shutdown
```

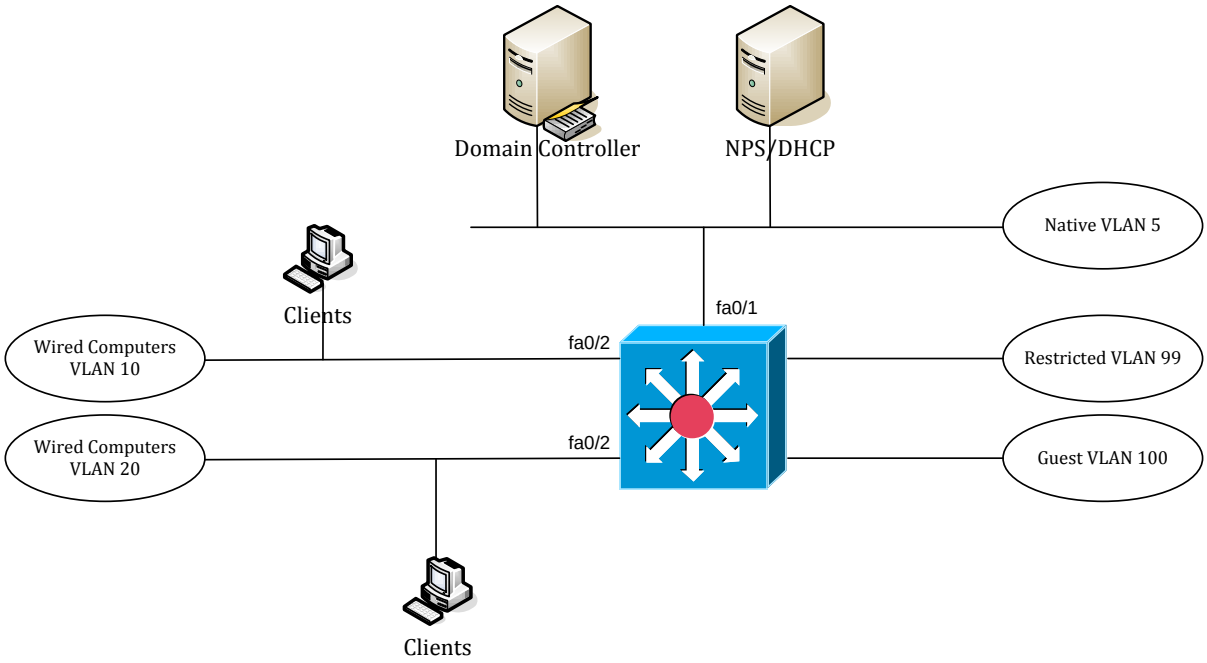
VLAN information can be retrieved as follows

```
addevsw01#show vlan
```

Schematic Design

For this lab, I use a Cisco Catalyst 3560 switch which also provides inter-VLAN routing between the various networks.

Name	Software	Role
ADDEVDC01	Windows Server 2008 R2	DC,DNS,CA
ADDEVDC04	Windows Server 2012	NPS, DHCP
ADDEVWKS01	Windows 7	Client
ADDEVSW01	Cisco Catalyst 3560	Switch



To enable routing between VLANs, use the following command:

```
addevsw01(config)#ip routing
```

The IP address of addevdc01 is 10.32.5.3, the IP address of addevdc04 is 10.32.5.15 and the addevwks01 is configured as a DHCP client.

Table overview of network configuration:

Network ID	VLAN ID	Default Gateway	Description
10.32.5.0/24	5	10.32.5.254	Native vlan
10.32.10.0/24	10	10.32.10.254	Clients vlan
10.32.20.0/24	20	10.32.20.254	Clients vlan
10.32.99.0/24	99	10.32.99.254	Restricted vlan
10.32.100.0/24	100	10.32.100.254	Guest vlan

Prepare the environment for 802.1x Authentication Task List

You need to prepare the environment with the appropriate groups to support 802.1x based authentication. The next step is to create Active Directory Security Groups for authorized access and certificate enrollment.

- Create a group AutoEnroll Server Authentication Certificate
- Create a group AutoEnroll Client Authentication Certificate
- Create a group Wired Computers VLAN 10

Create a group AutoEnroll NPS Server Authentication Certificate

- Open **Active Directory Users and Computer** from **Administrative Tools**
- Select Organizational Unit you want to create the group
- Right click on the OU, select **New – Group**
- On the **New–Group** window, type the name of the group *AutoEnroll Server Authentication Certificate*, and click **OK**

Create a group AutoEnroll Client Authentication Certificate

- Select Organizational Unit you want to create the group
- Right click on the OU, select **New – Group**
- On the **New – Group** window, type the name of the group *AutoEnroll Client Authentication Certificate*, and click **OK**

Create a group Wired Computers VLAN 10

- Select Organizational Unit you want to create the group
- Right click on the OU, select **New – Group**
- On the **New – Group** window, type the name of the group *Wired Computers VLAN 10*, and click **OK**

Configuring and Deploying 802.1x Authentication Certificates Task List

Before we can use 802.1x authentication we have to enroll for certificates. In this section, you will create and enroll hosts on the network to enroll for a certificate. The client computer will send his identity (computer certificate) to the switch, whereas the switch authenticates the client computer against the Network Policy server.

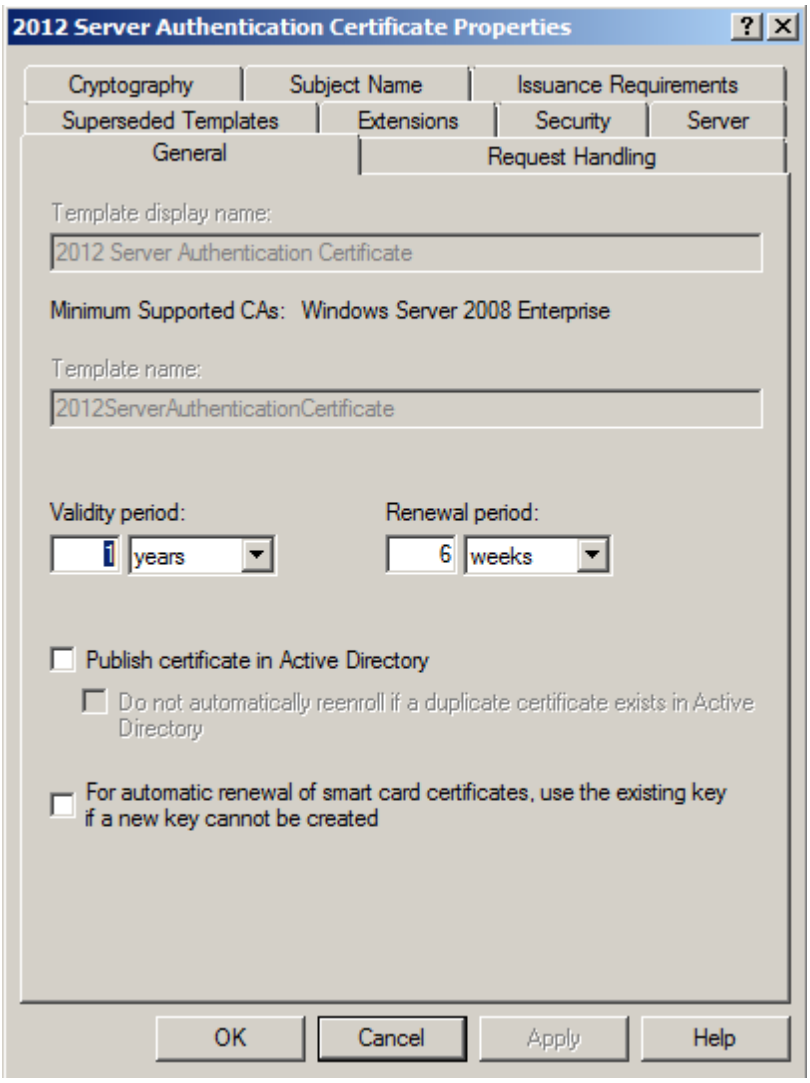
- Create a NPS Server Authentication Certificate
- Create a Workstation Authentication Certificate
- Adding the certificate templates to the Certificate Authority
- Add the NPS Server account to the autoenrollment group
- Add client computer accounts to the autoenrollment group
- Add client computer accounts to the authorized computers group

- Create a GPO for NPS Server certificate enrollment

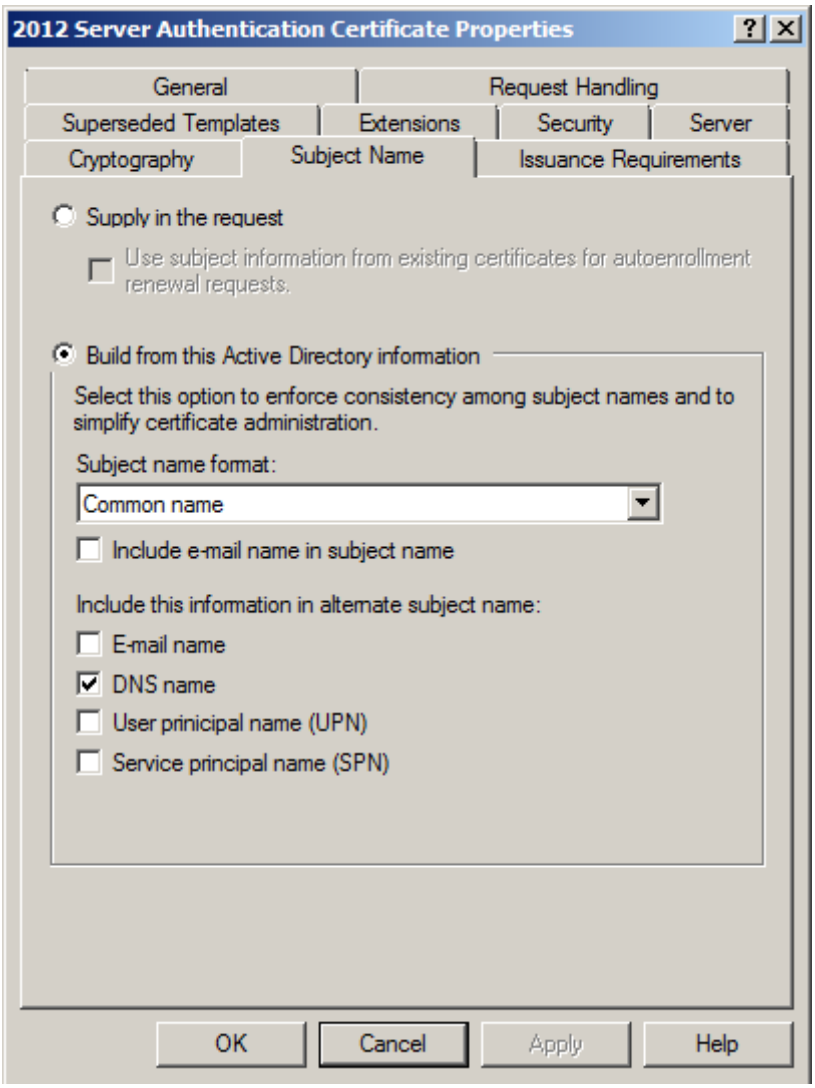
Create a NPS Server Authentication Certificate

- Open **Certificate Authority** snap-in from **Administrative Tools.**
- Right click on **Certificate Templates** and select **Manage.**
- Right click on **RAS and IAS Server certificate Template** and select **Duplicate Template.**
- On the **Duplicate Template** dialog box, select **Windows 2003 Server** and click **OK**

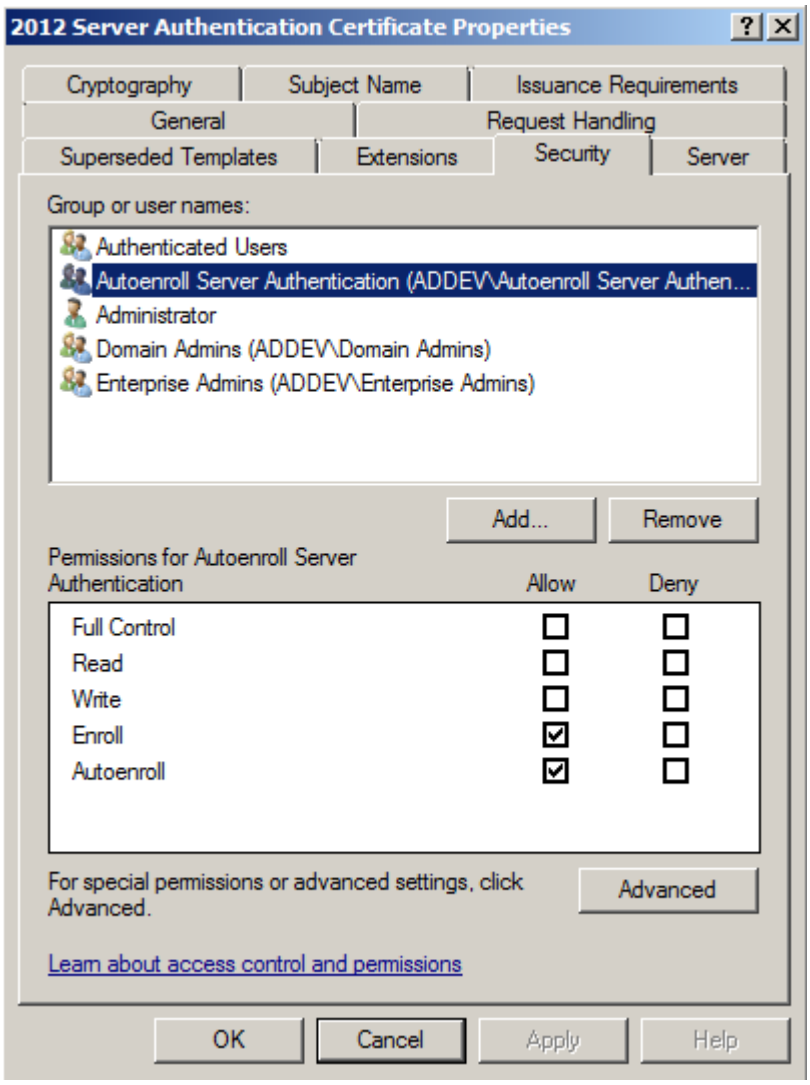
- On the **General** tab, in the **Template** display name field, type *2012 Server Authentication Certificate*.



- Click on the **Subject Name** tab, select **Build from this Active Directory information**. Ensure that the Subject name format is set to **Common name** and that only DNS Name is selected under **Include this information in subject alternative name**.



- Click on the **Security** tab, click on the **Add** button and add **AutoEnroll Server Authentication Certificate** group, assign **Enroll** and **Autoenroll** permissions and click **OK**.

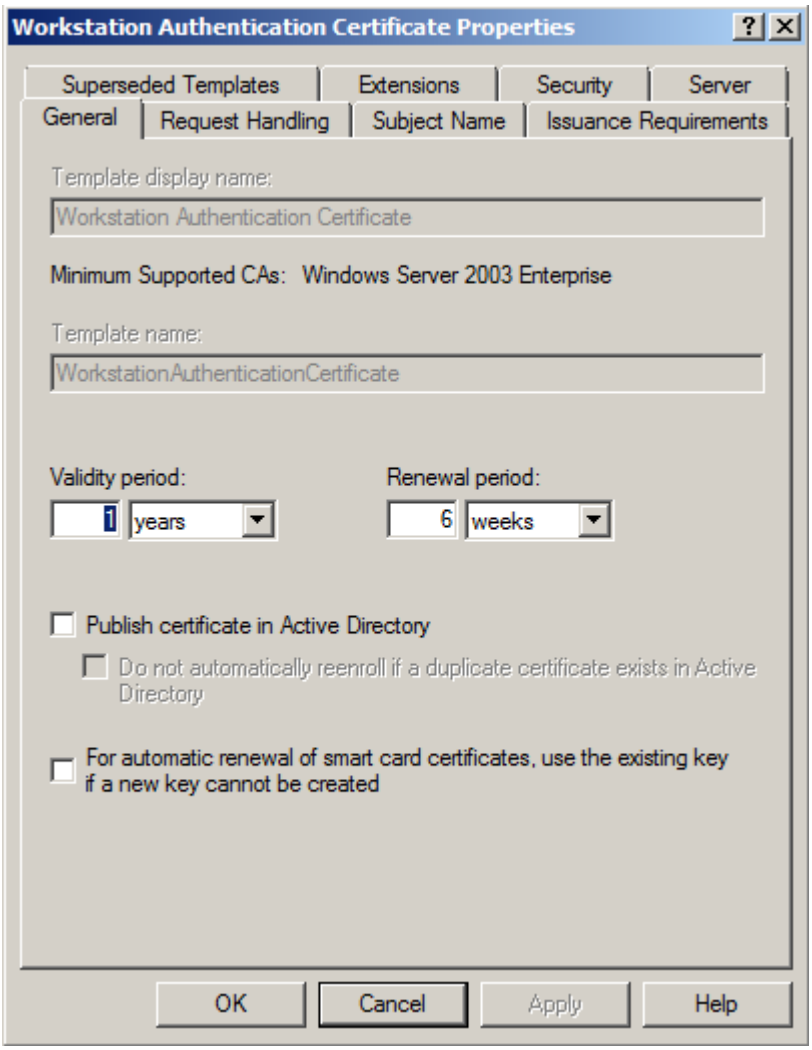


You should remove any of the other security groups that have permissions to enroll and/or autoenroll this certificate template.

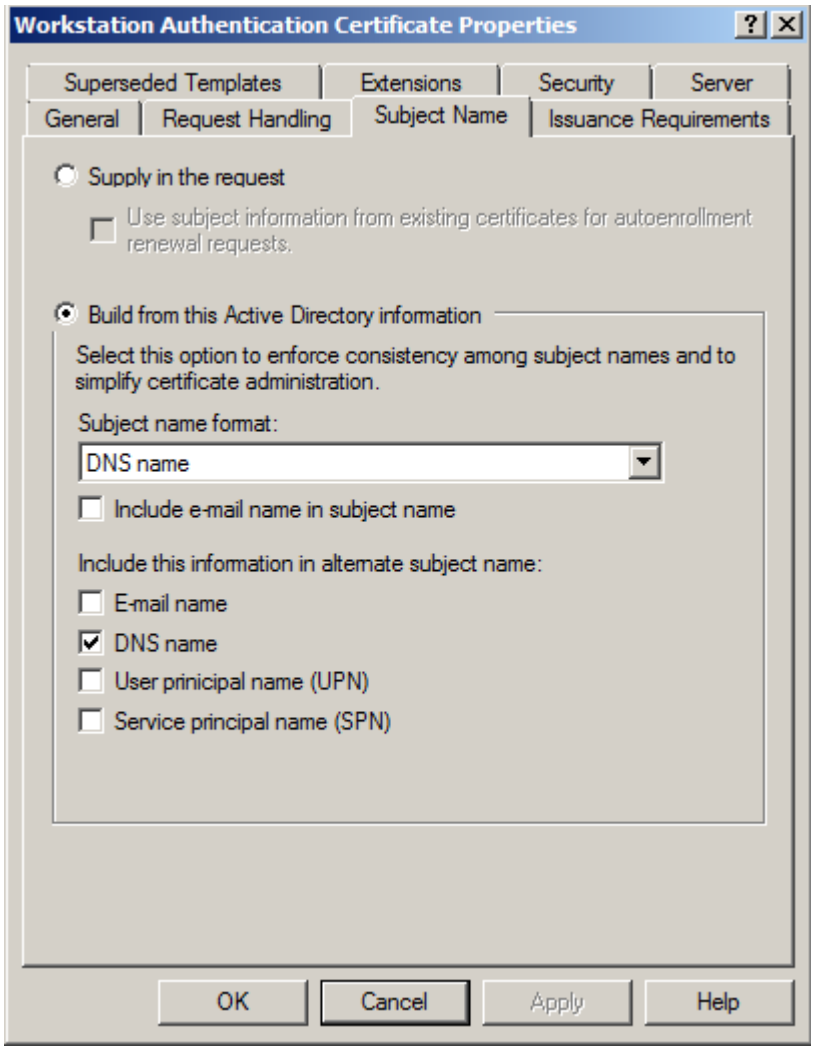
Create a Workstation Authentication Certificate

A certificate is required to authenticate computers for port based authentication.

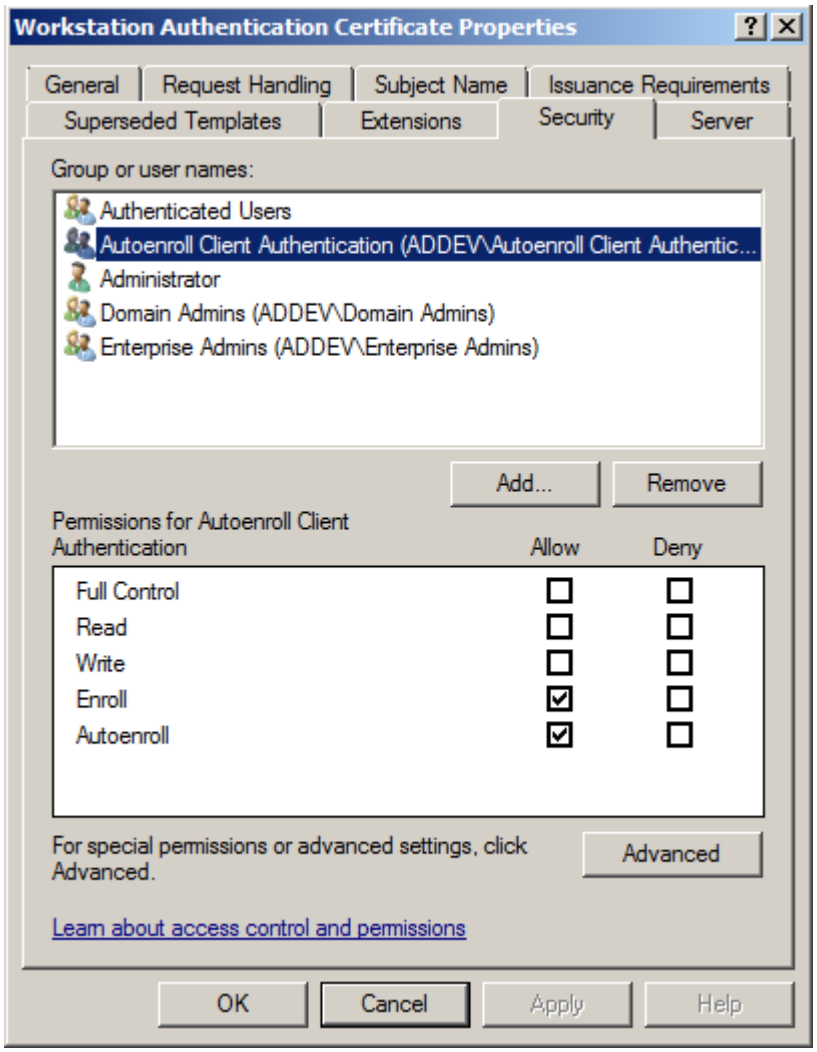
- Right click on the **Workstation Authentication** certificate template and select **Duplicate Template.**
- Click on the **General** tab, in the **Template** display name, type *Workstation Authentication Certificate.*



- Click on the **Subject Name** tab, ensure to select **Built from this Active Directory Information**. Under Subject name format select **Common Name.** Ensure that DNS name is the only option selected under **Include this information in subject alternate name**



- Click on the **Security** tab, click on the **Add** button and add **AutoEnroll Client Authentication Certificate** group, assign **Enroll** and **Autoenroll** permissions and click **OK**



- Close **Certificates Templates** snap-in

You should remote any of the other security groups that have permissions to enroll and/or autoenroll this certificate template.

Adding the Certificate Templates to the Certificate Authority

After you have configured or created new certificate templates, you have to add them to the certificate authority to enable enrollment.

- From the **Certificate Authority** snap-in, right click on **Certificate Templates**, select **New – Certificate Template to Issue**.

Select following certificate templates: **Workstation Authentication Certificate** and **2012 Server Authentication Certificate** and click **OK**.

Add the NPS Server account to the AutoEnroll Server Authentication Certificate group

- Open **Active Directory Users and Computers** from **Administrative Tools**
- Double click on **AutoEnroll Server Authentication Certificate** group.
- Click on the **Member** tab and click **Add**.
- In the **Select Users, Contacts, Computers, or Groups** dialog box, in the **Enter the object names to select** add *ADDEVSRV01* computer account and click **OK**.

Add client computer accounts to the AutoEnroll Client Authentication Certificate group

- Double click on **AutoEnroll Client Authentication Certificate** group.
- Click on the **Member** tab and click **Add**.
- In the **Select Users, Contacts, Computers, or Groups** dialog box, in the **Enter the object names to select** add *ADDEVWKS01* computer account and click **OK**.

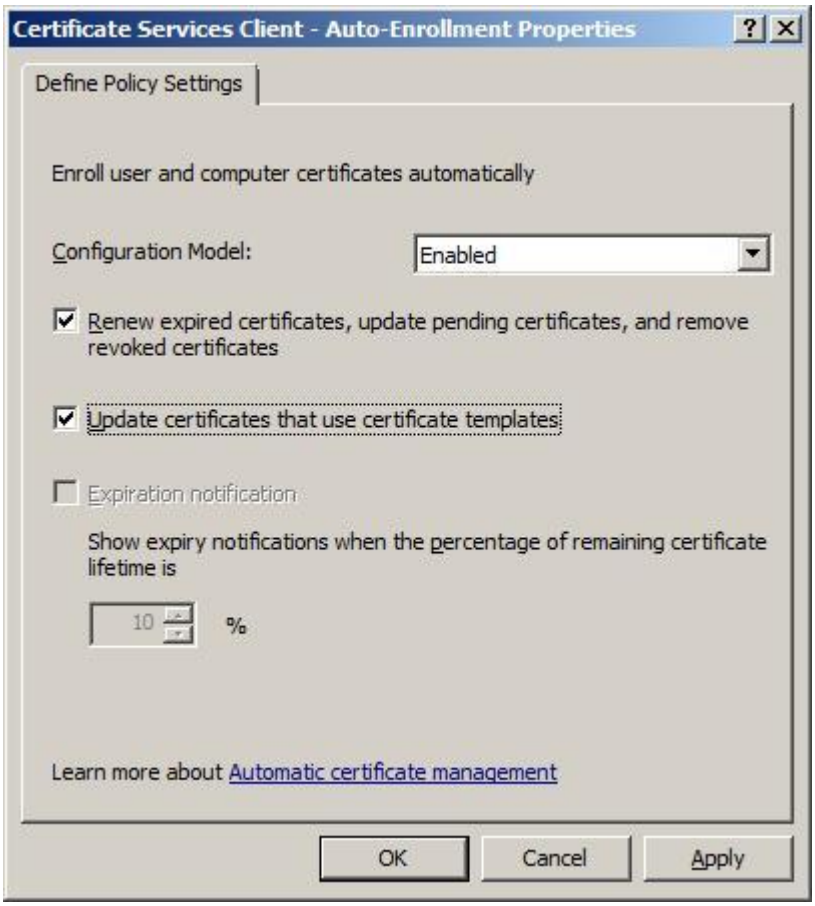
Add client computer accounts to the Wired Computers VLAN 10

- Double click on **Wired Computers VLAN 10** group.
- Click on the **Member** tab and click **Add**.
- In the **Select Users, Contacts, Computers, or Groups** dialog box, in the **Enter the object names to select** add *ADDEVWKS01* computer account and click **OK**.

Create a GPO for NPS Server certificate enrollment

- Open **Group Policy Management** from **Administrative Tools.**
- Expand Domain, expand Group Policy Objects, and select **New Group Policy Objects**.
- On the **New – Group Policy** dialog box, type *Autoenroll Server Certificate* and click **OK**

- Right click on **Autoenroll Server Certificate**, select **GPO Status**, and select **User Configuration Settings Disabled**
- Right click on **Autoenroll Server Certificate** and select **Edit.**
- Expand **Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies.**
- In the right pane, double click on **Certificate Services Client – Auto-enrollment**
- On the **Certificate Services Client – Auto-enrollment Properties** dialog box, select **Enroll Certificates Automatically**, select **Renew expired certificates** and select **Update certificates that use certificate templates** and click **OK.**



- Close Group Policy Editor
- Link group policy to the organizational unit which contains the computer account of your NPS server.
- On the **NPS server**, open command prompt and run launch **gpupdate.exe** or restart the server.

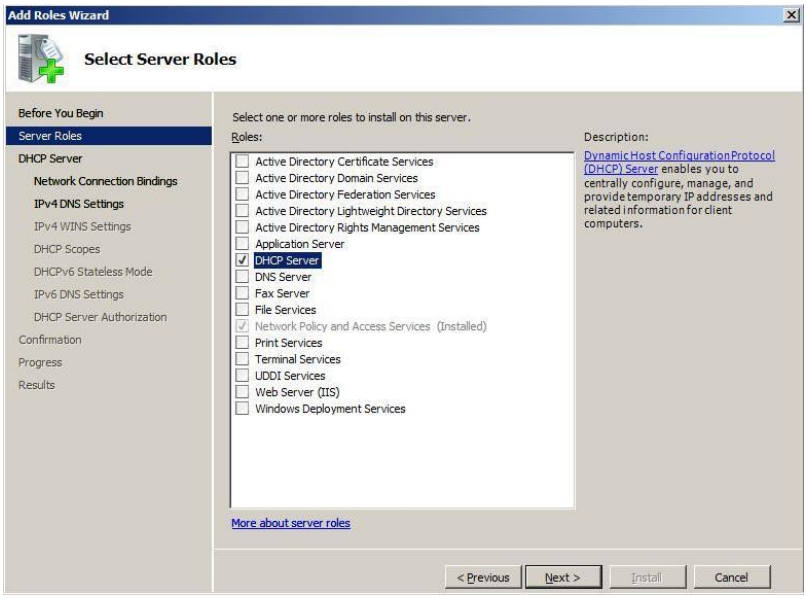
Install and Configure your DHCP Server

Client computers on our network will receive an IP address based on the VLAN where the client computer is a member of. In our lab, we will create a scope for VLAN 10.

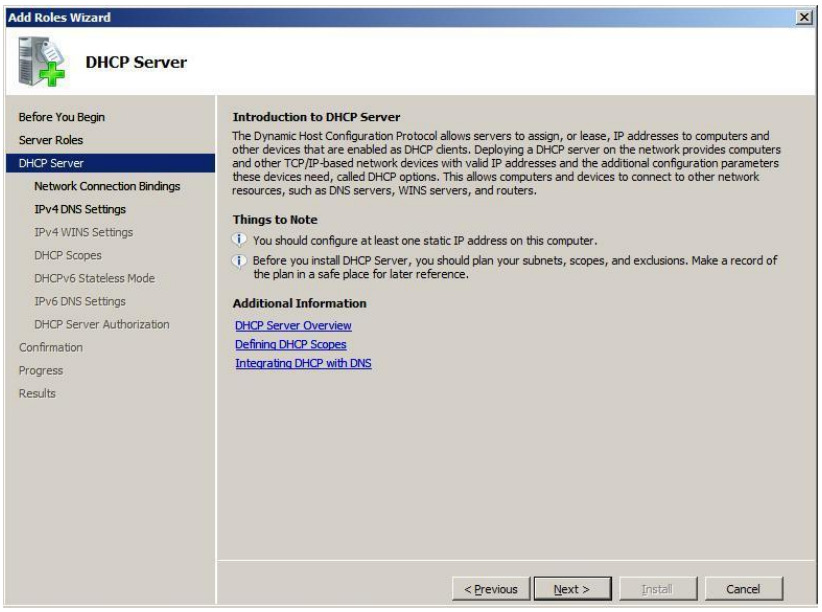
- Install the DHCP Server Role
- Configure your DHCP Server with a scope for VLAN 10
- Configure your DHCP Server with a scope for VLAN 20
- Configure your DHCP Server with a scope for VLAN 99
- Configure your DHCP Server with a scope for VLAN 100

Install the DHCP Server role

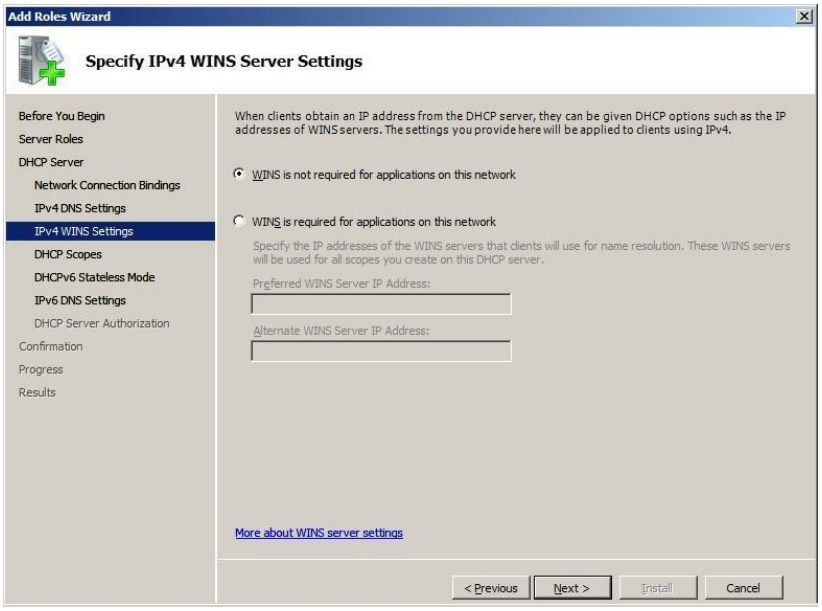
- Open **Server Manager** from the **Administrative Tools**, expand **Roles** and select **Add Roles**
- On the **Select Server Role** page, select **DHCP Server** and click **Next**



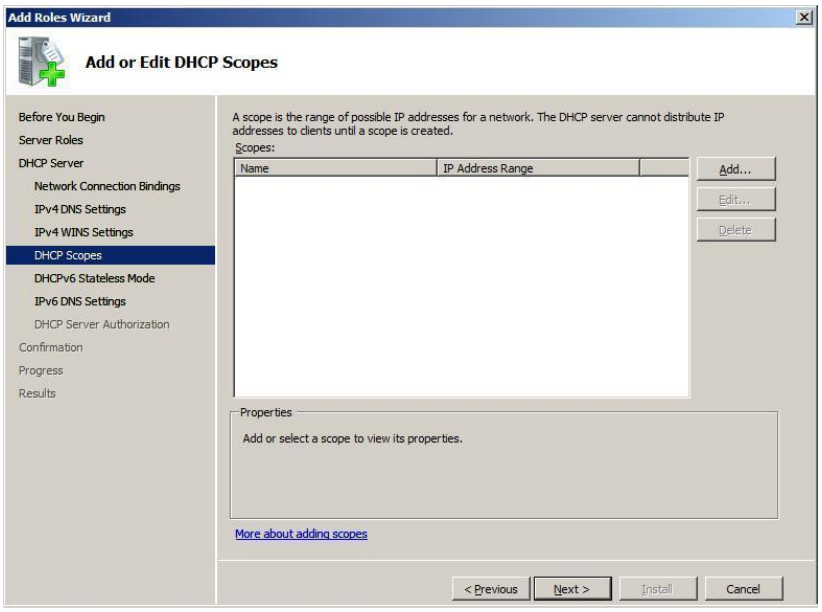
- On the **DHCP Server** page, select **Next**



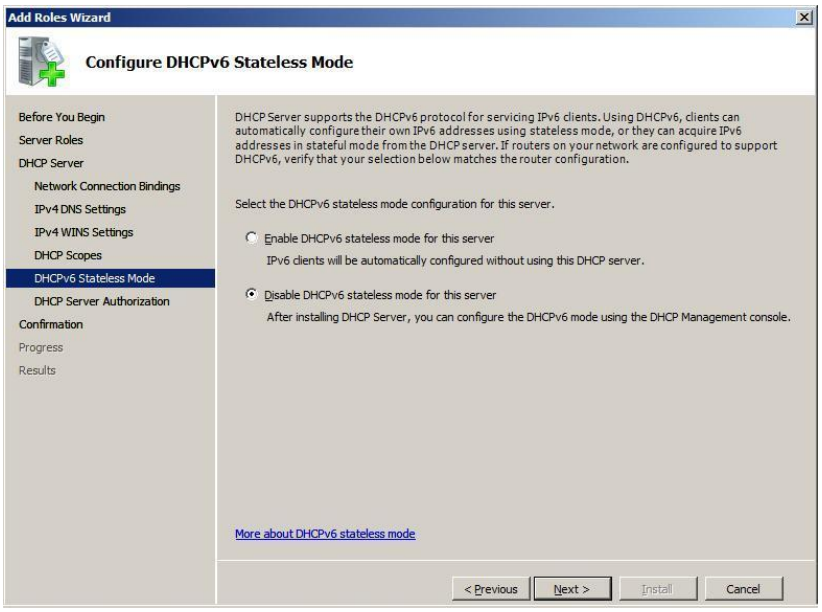
- On the **Select Network Connection Binding** page, select the **Network Connection** and click **Next**
- On the **Specify IPv4 DNS Server Settings** page, type the IP address of your preferred DNS server and click **Next**
- On the **Specify IPv4 WINS Server Settings** page, select **WINS is not required** and click **Next**



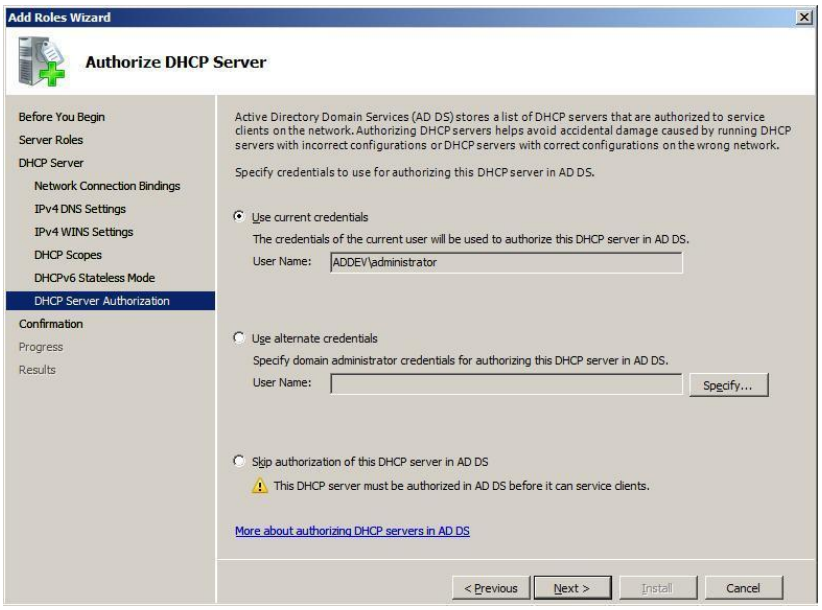
- On the **Add or Edit DHCP Scopes** page, click **Next**



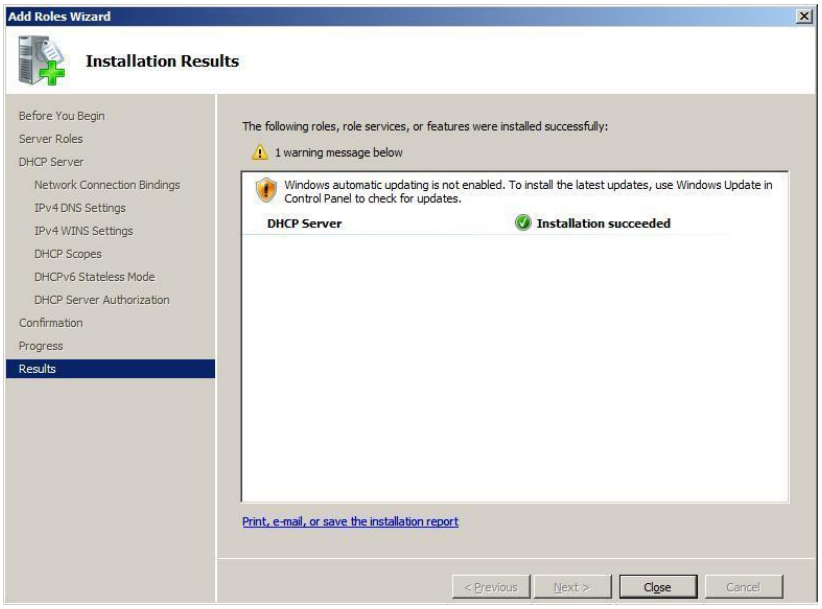
- On the **Configure DHCPv6 Stateless Mode** page, select **Disable** and click **Next**



- On the **Authorize DHCP Server** page, select use **Current Credentials** and click **Next**

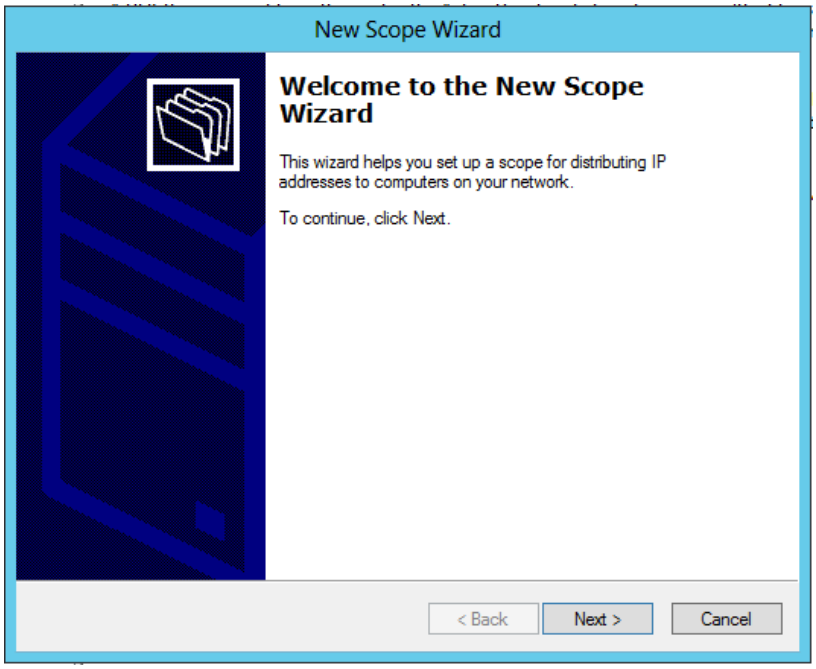


- On the **Confirm Installation Selection** page, click **Install**
- On the **Installation Results** page, click **Close**

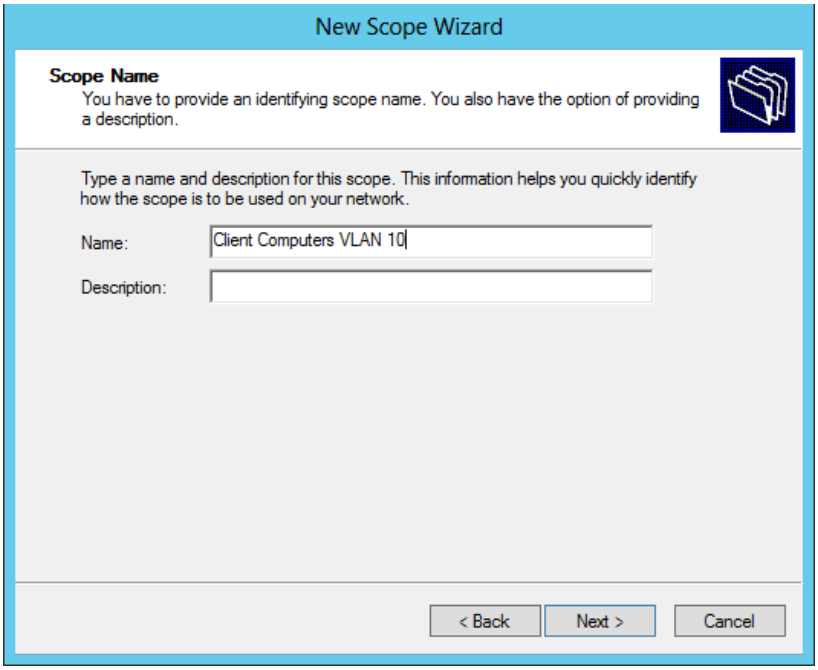


Configure DHCP Server with a scope for VLAN 10

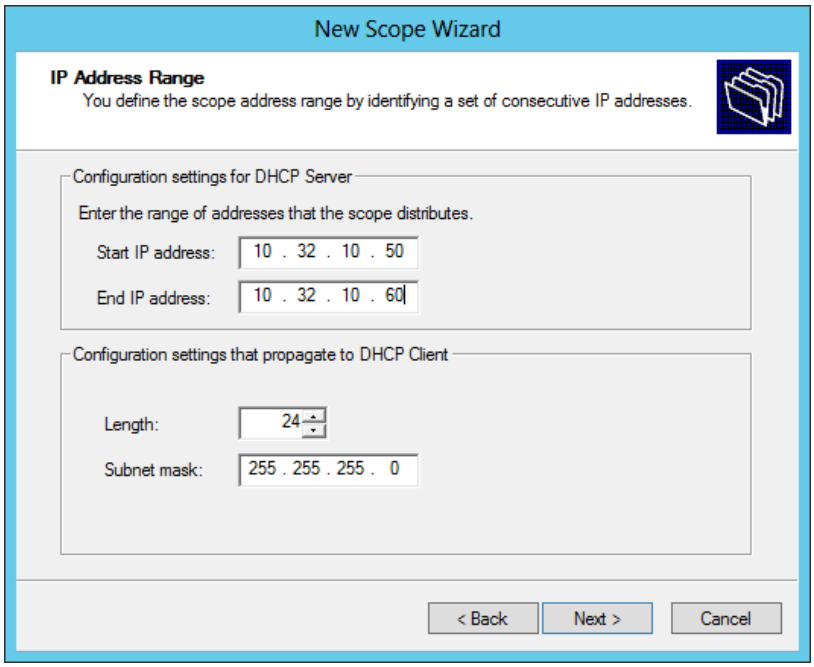
- Open **DHCP Console** from **Administrative Tools**
- Right click on **IPv4** and select **New Scope**
- On the **Welcome to the New Scope Wizard** page, click **Next**



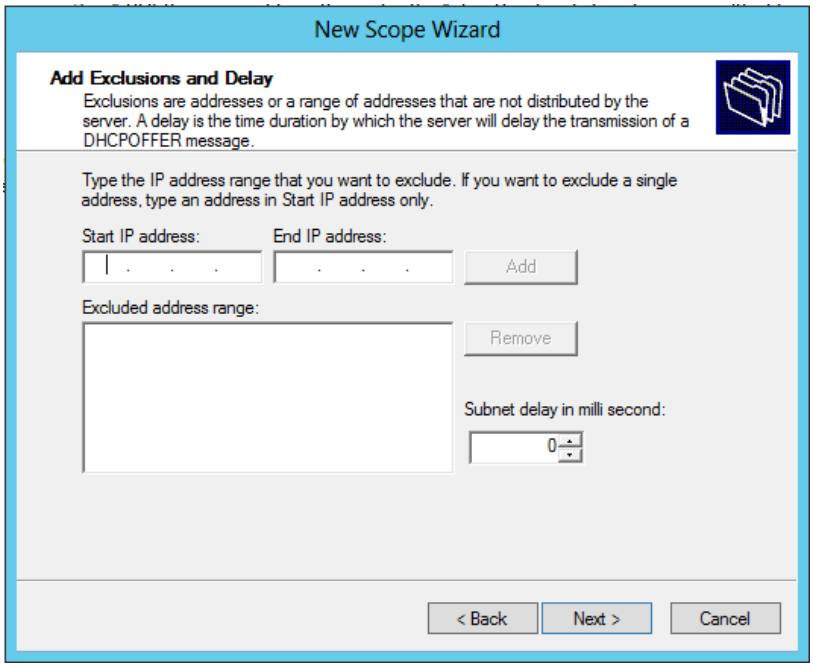
- On the **Scope Name** page, type a name for the scope and click **Next**



- On the **IP Address Range** page, specify Start and End IP address. Also specify the correct subnet mask and click **Next**

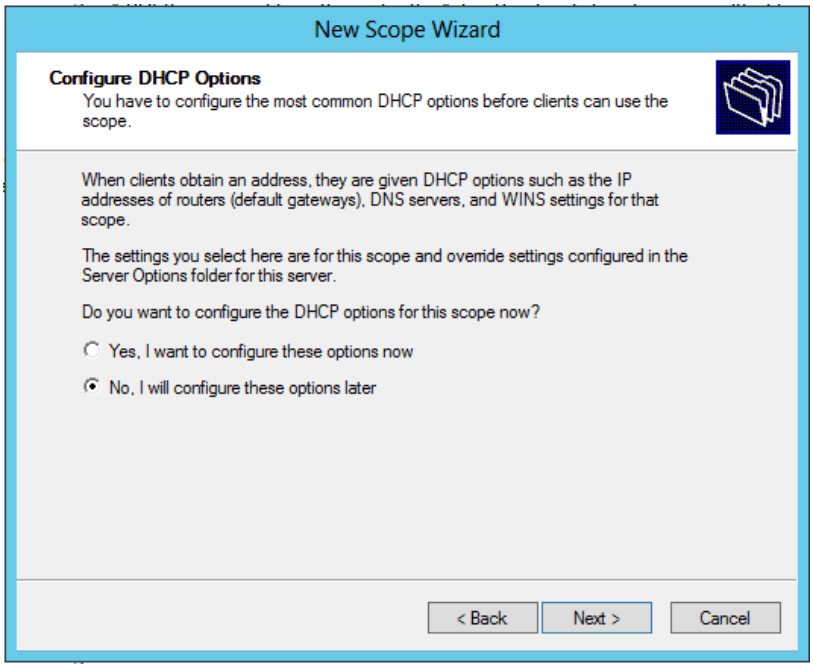


- On the **Add Exclusions** page, click **Next**

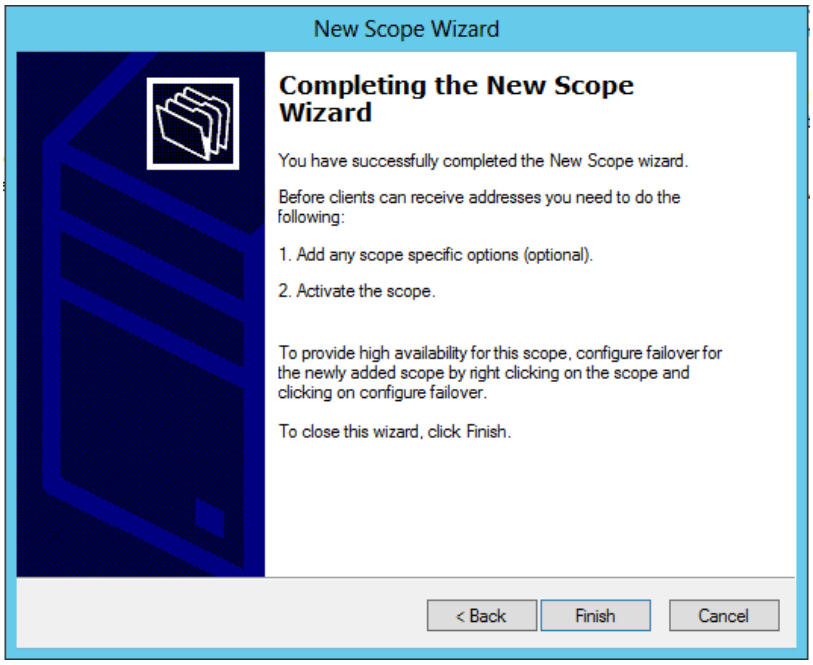


- On the **Lease Duration** page, specify a lease duration and click **Next**

- On the **Configure DHCP Option** page, select **No, I will configure these options later** and click **Next**



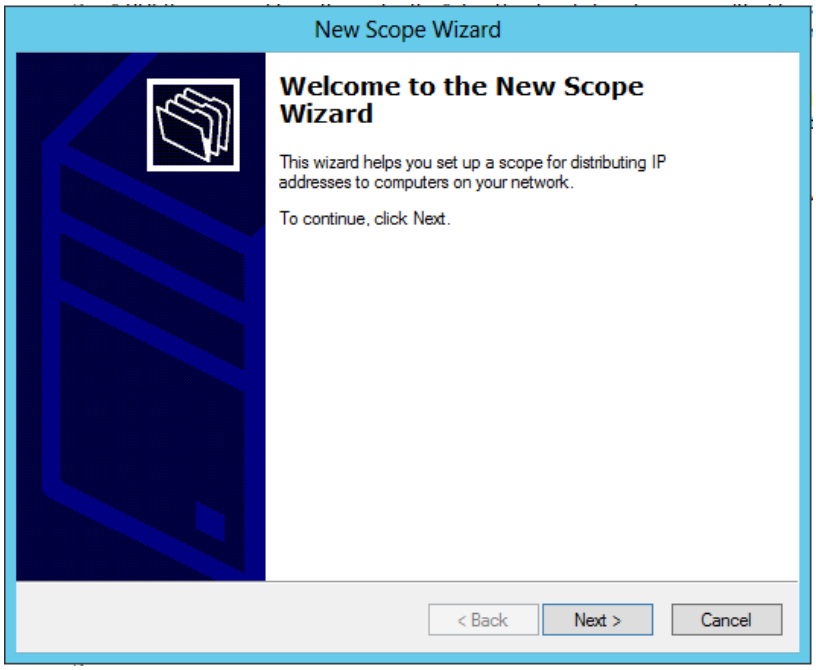
- On the **Completing the New Scope Wizard** page, click **Finish**



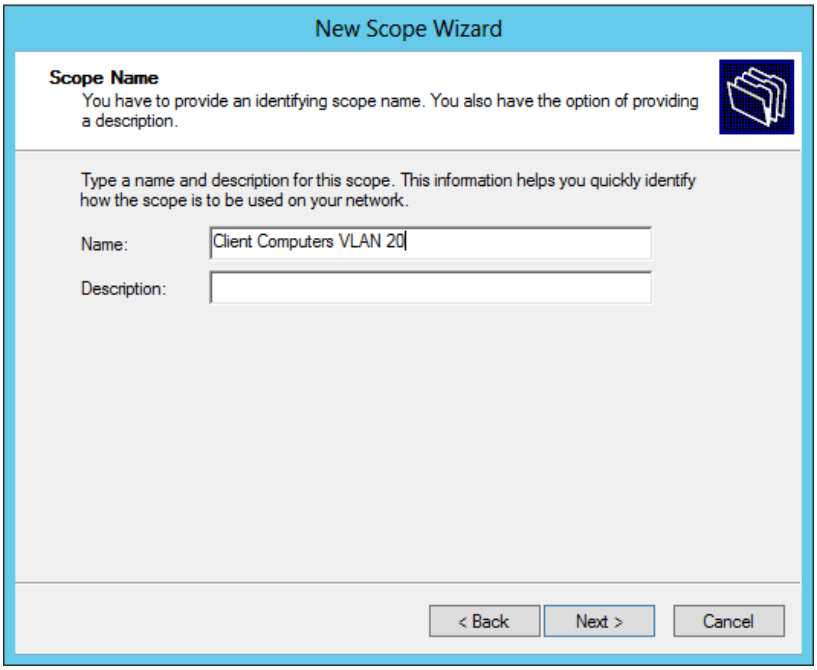
- Expand Scope, right click on **Scope Options** and select **Configure Options**
- On the **Scope Option**s dialog box, select the following: 003 Router 10.32.10.254, 006 DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click **OK**
- Right click on the **Scope** and select **Activate**

Configure DHCP Server with a scope for VLAN 20

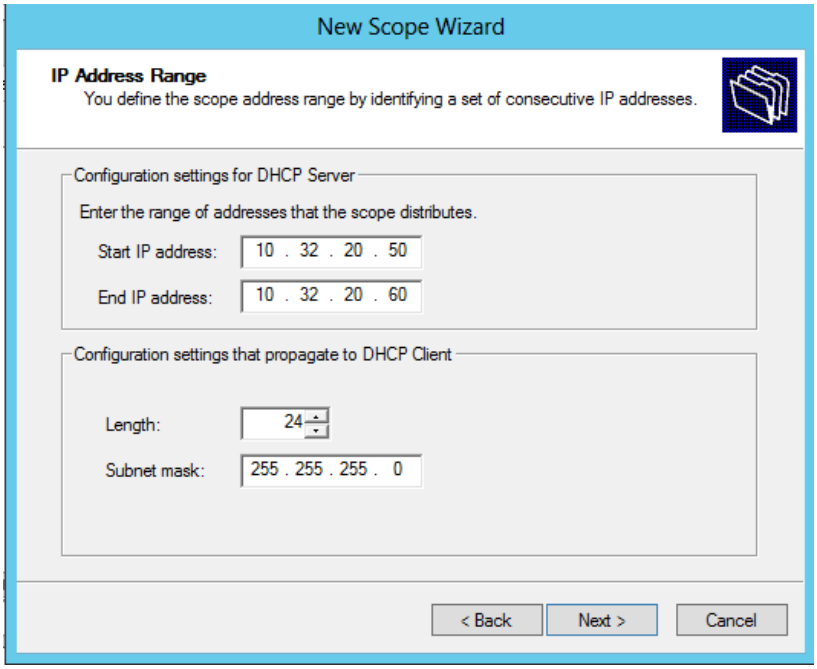
- Open **DHCP Console** from **Administrative Tools**
- Right click on **IPv4** and select **New Scope**
- On the **Welcome to the New Scope Wizard** page, click **Next**



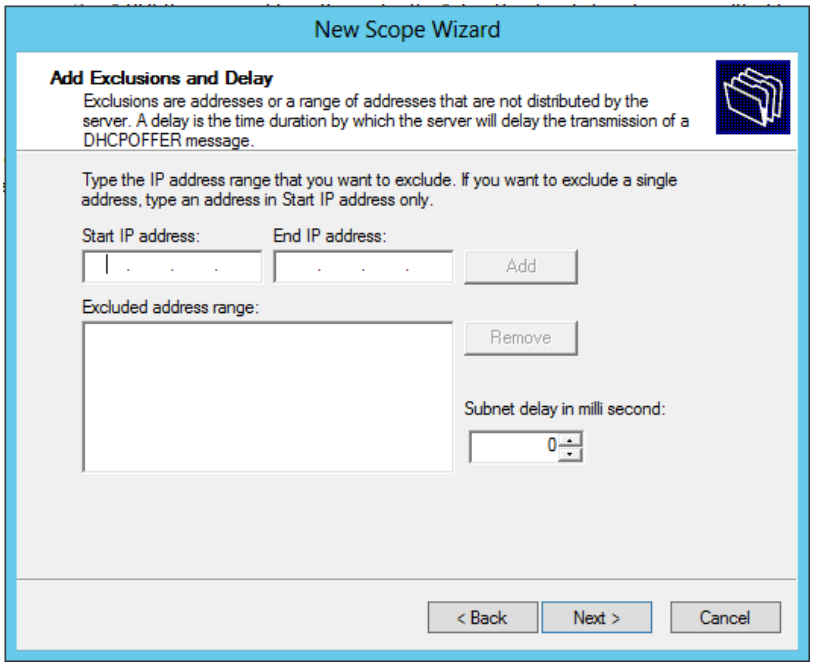
- On the **Scope Name** page, type a name for the scope and click **Next**



- On the **IP Address Range** page, specify Start and End IP address. Also specify the correct subnet mask and click **Next**

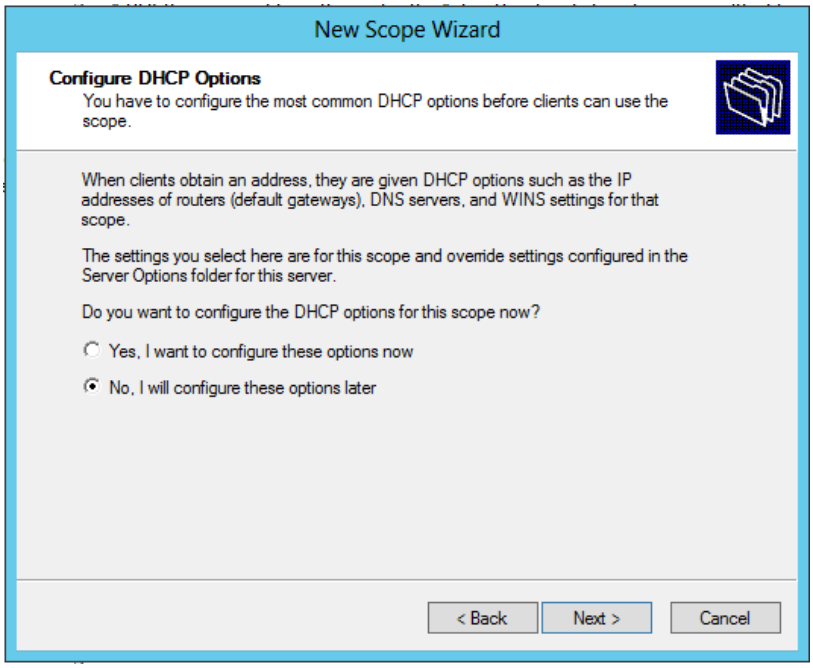


- On the **Add Exclusions** page, click **Next**

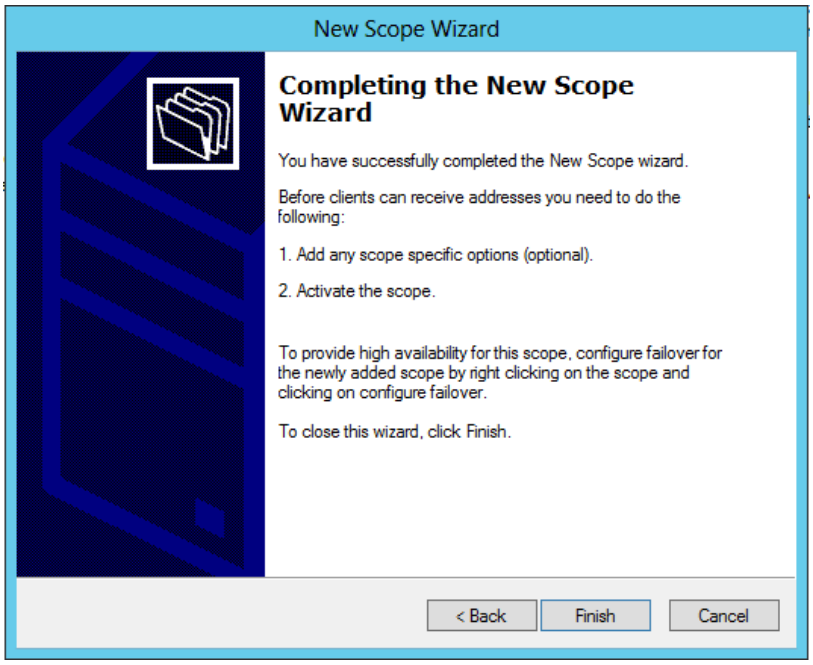


- On the **Lease Duration** page, specify a lease duration and click **Next**

- On the **Configure DHCP Option** page, select **No, I will configure these options later** and click **Next**



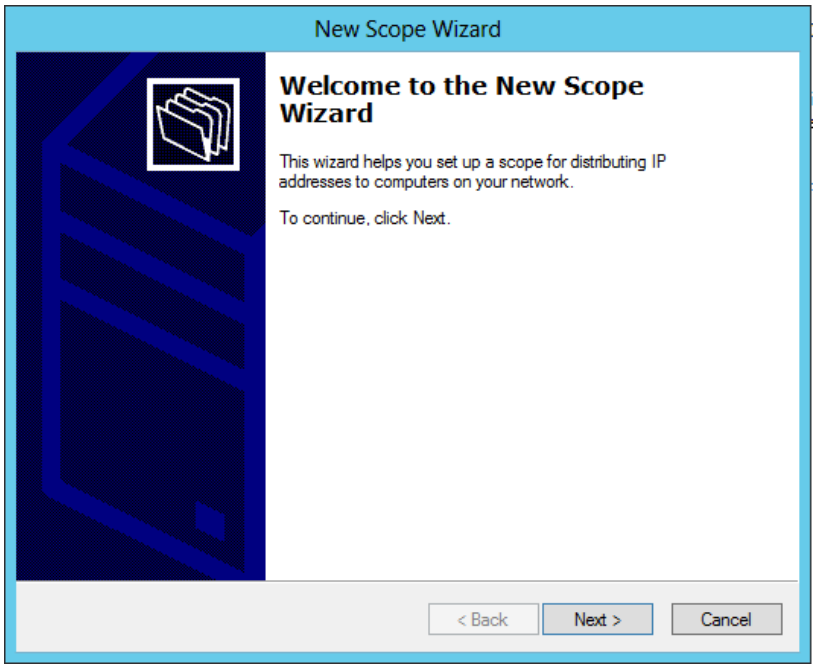
- On the **Completing the New Scope Wizard** page, click **Finish**



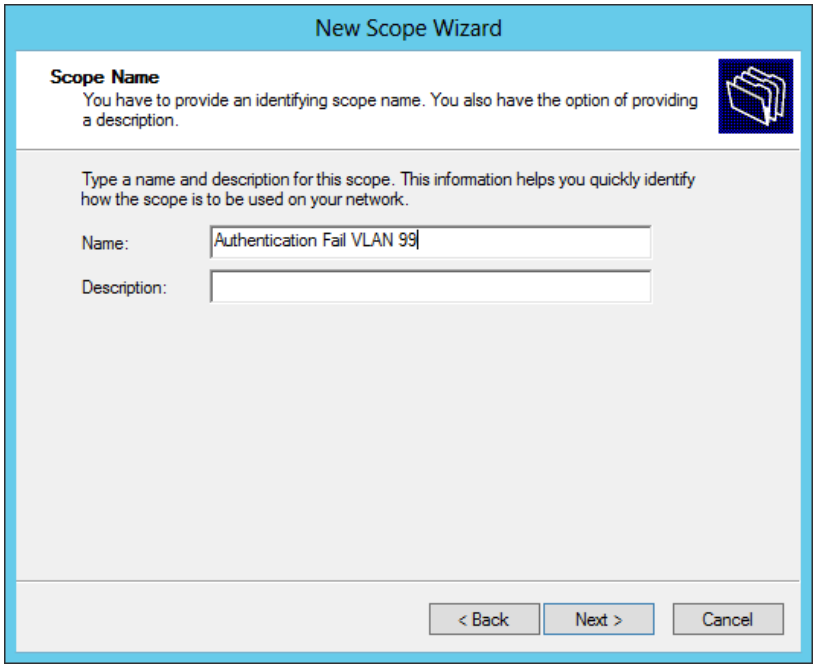
- Expand Scope, right click on **Scope Options** and select **Configure Options**
- On the **Scope Option**s dialog box, select the following: 003 Router 10.32.20.254, 006 DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click **OK**
- Right click on the **Scope** and select **Activate**

Configure DHCP Server with a scope for VLAN 99 (Authentication Fail VLAN)

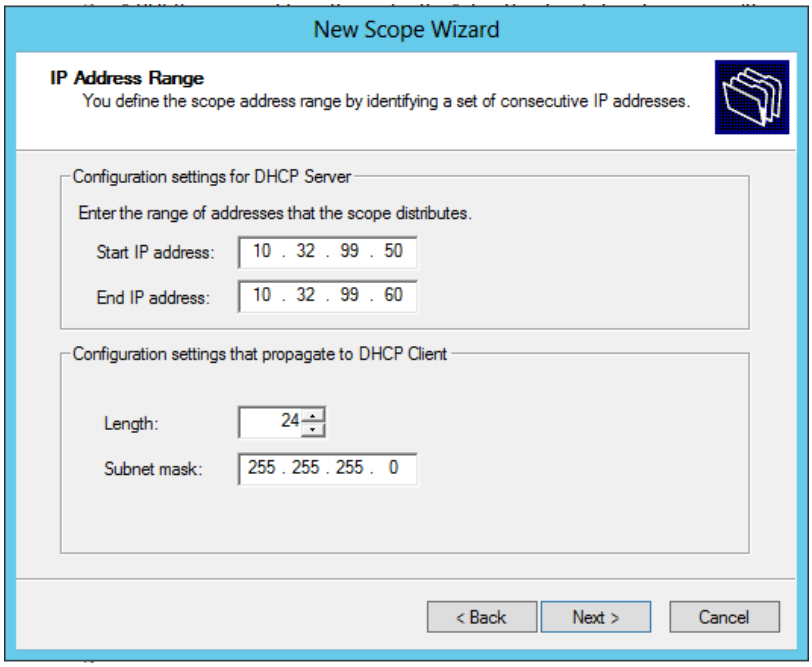
- Open **DHCP Console** from **Administrative Tools**
- Right click on **IPv4** and select **New Scope**
- On the **Welcome to the New Scope Wizard** page, click **Next**



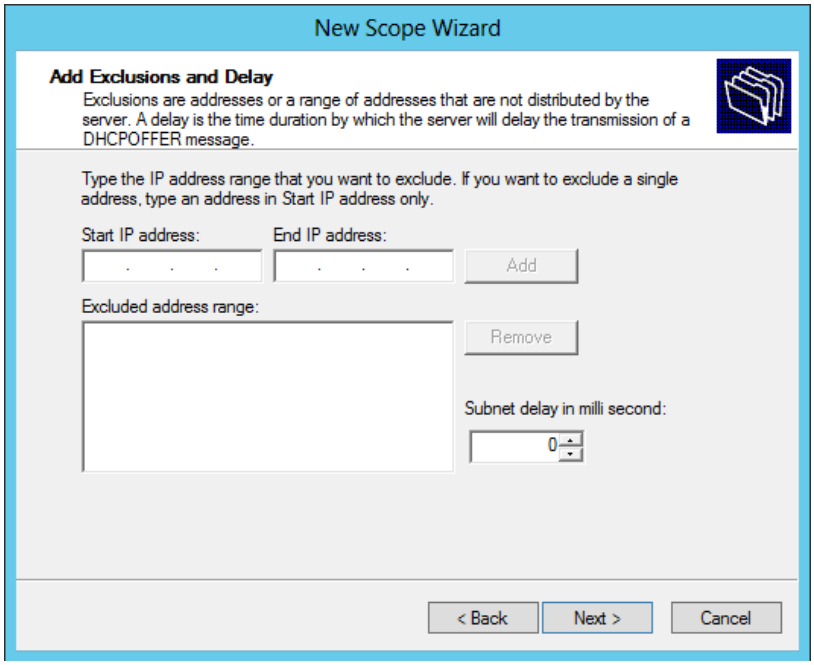
- On the **Scope Name** page, type a name for the scope and click **Next**



- On the **IP Address Range** page, specify Start and End IP address. Also specify the correct subnet mask and click **Next**

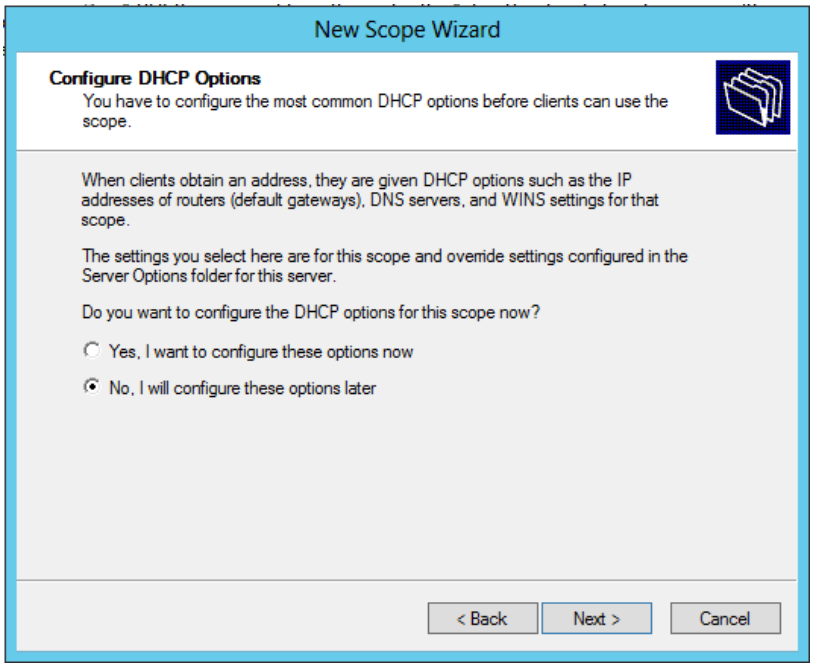


- On the **Add Exclusions** page, click **Next**

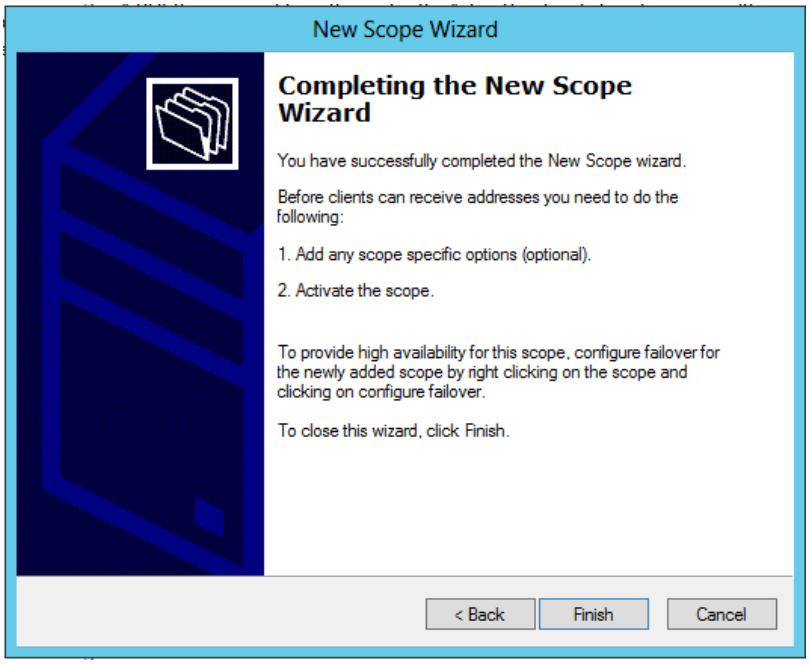


- On the **Lease Duration** page, specify a lease duration and click **Next**

- On the **Configure DHCP Option** page, select **No, I will configure these options later** and click **Next**



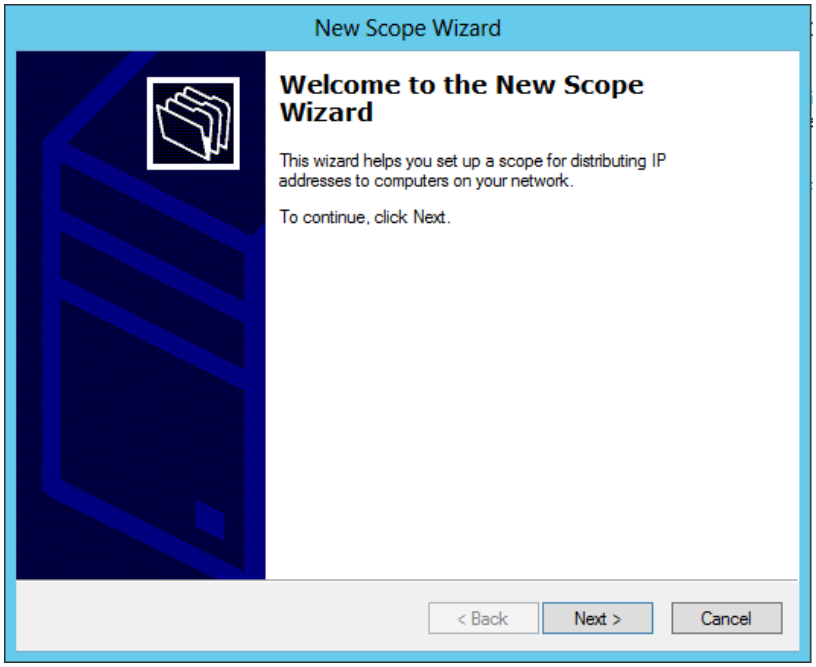
- On the **Completing the New Scope Wizard** page, click **Finish**



- Expand Scope, right click on **Scope Options** and select **Configure Options**
- On the **Scope Option**s dialog box, select the following: 003 Router 10.32.99.254, 006 DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click **OK**
- Right click on the **Scope** and select **Activate**

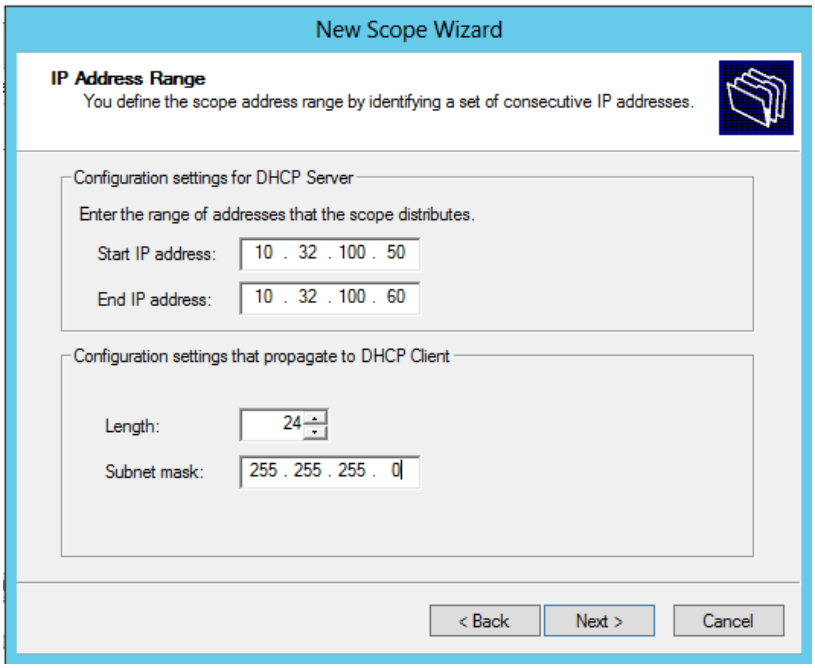
Configure DHCP Server with a scope for VLAN 100 (Guest VLAN)

- Open **DHCP Console** from **Administrative Tools**
- Right click on **IPv4** and select **New Scope**
- On the **Welcome to the New Scope Wizard** page, click **Next**

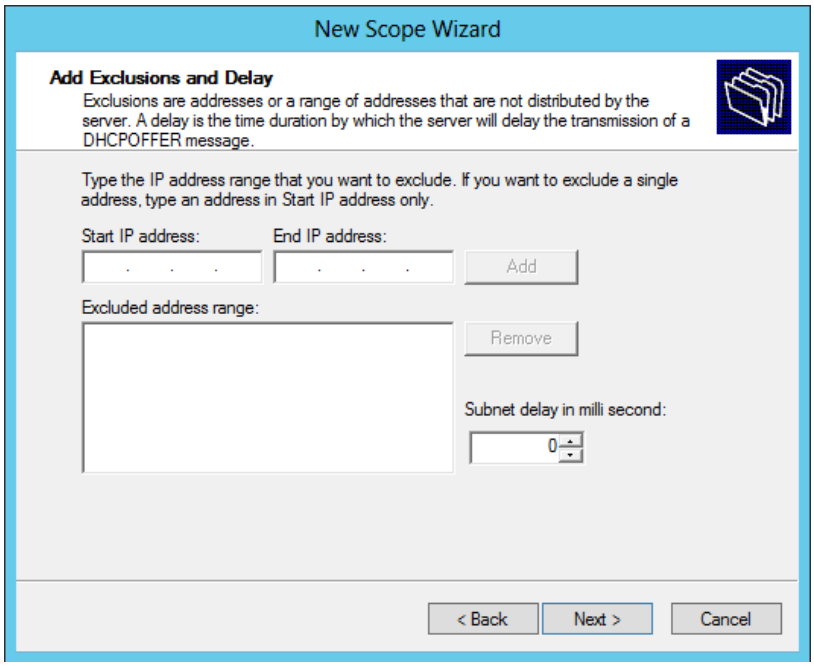


- On the **Scope Name** page, type a name for the scope and click **Next**

- On the **IP Address Range** page, specify Start and End IP address. Also specify the correct subnet mask and click **Next**

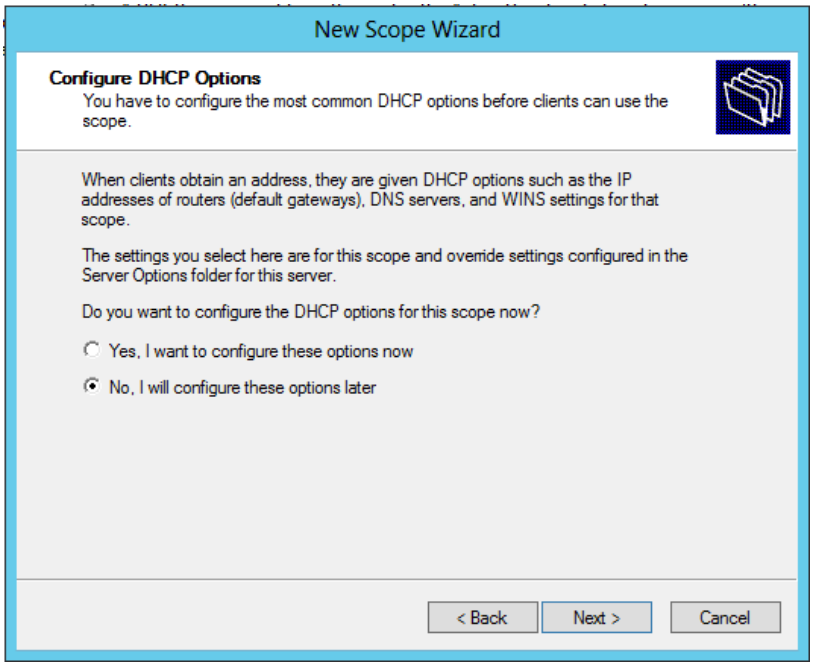


- On the **Add Exclusions** page, click **Next**



- On the **Lease Duration** page, specify a lease duration and click **Next**

- On the **Configure DHCP Option** page, select **No, I will configure these options later** and click **Next**



- On the **Completing the New Scope Wizard** page, click **Finish**

- Expand Scope, right click on **Scope Options** and select **Configure Options**
- On the **Scope Option**s dialog box, select the following: 003 Router 10.32.100.254, 006 DNS Server 10.32.5.3, 015 DNS Domain Name addev.local and click **OK**
- Right click on the **Scope** and select **Activate**

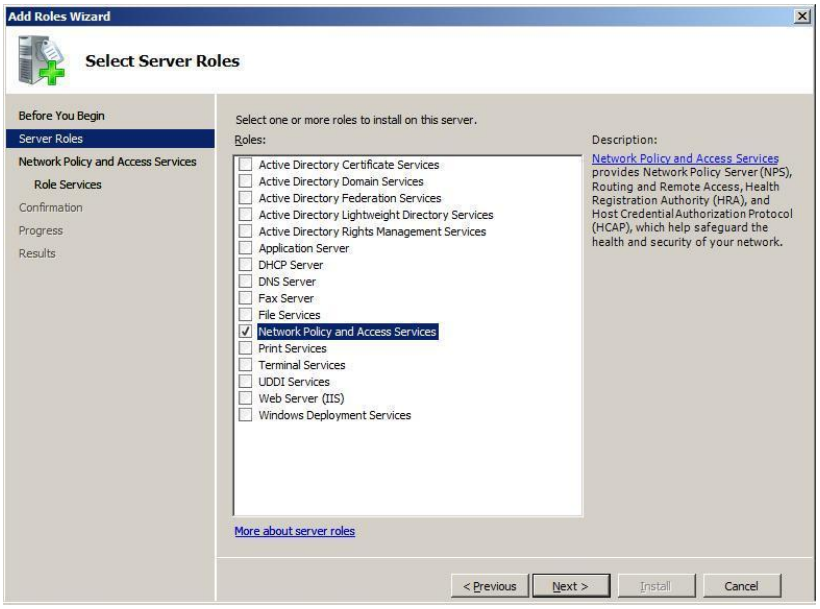
Install and configure your NPS Server

The task of the NPS server is the talk with the switch. The NPS server will be configured as a RADIUS server, whereas the switch will be configured as a RADIUS client. Afterwards, we need to create a Connection Request Policy which allows a connection between the switch and the NPS server. Next step is to create Network Policies where we can provide more details on how the client on the network needs to be authenticated.

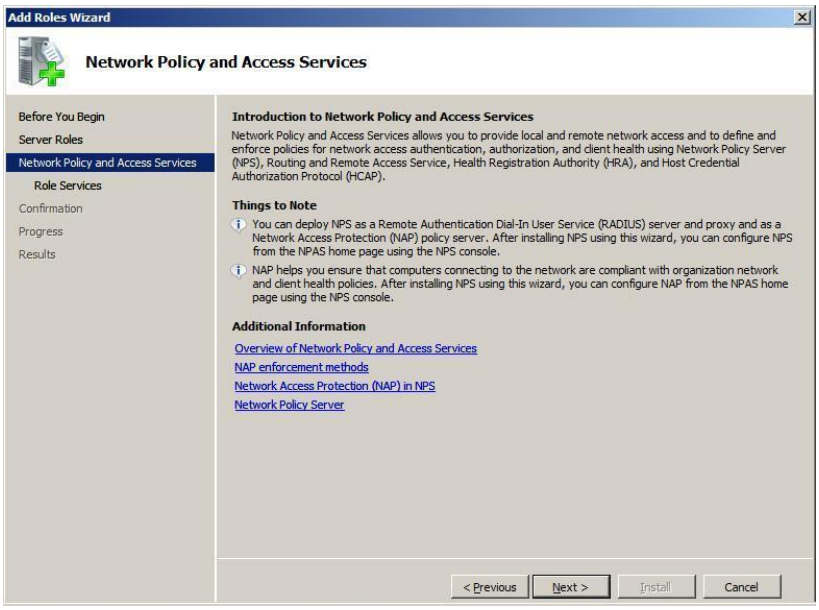
- Install the NPS Server Role
- Configure RADIUS Clients on NPS Server
- Configure Connection Request Policy
- Configure a Network Policy for EAP-TLS
- Configure a Network Policy for PEAP-EAP-MSCHAPv2
- Configure a Network Policy for PEAP-EAP-TLS

Install the NPS Server Role

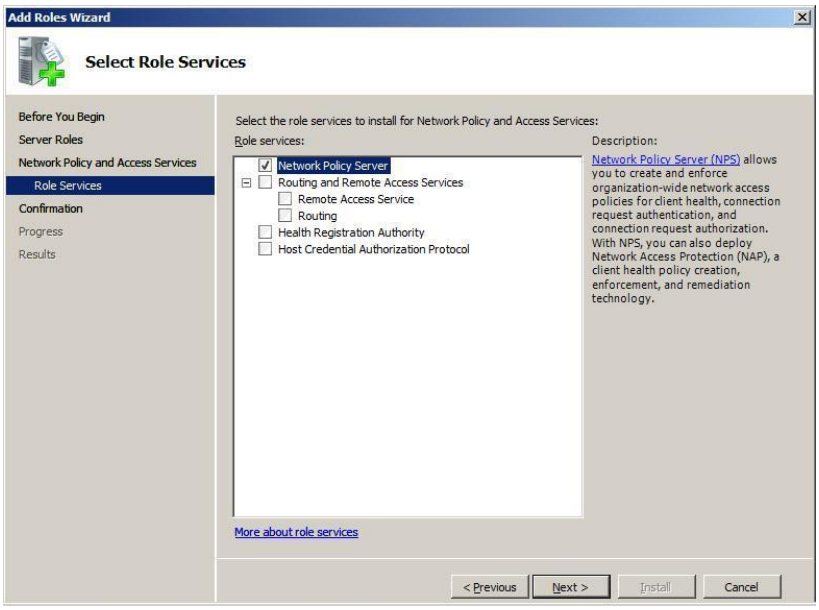
- Open **Server Management** from **Administrative Tools**
- On the **Select Server Role** page, select **Network Policy and Access Services**, and click **Next**



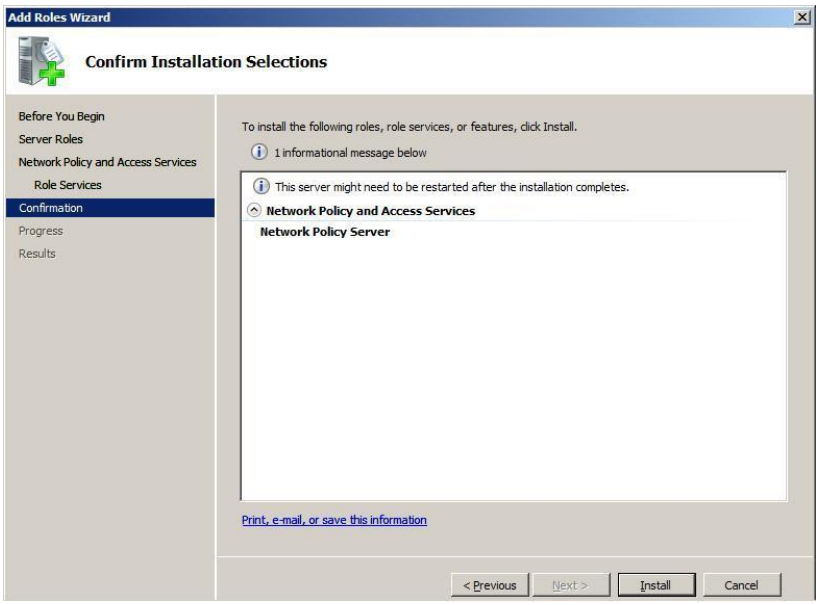
- On the **Network and Access Services** page, click **Next**



- On the **Select Role Services** page, select **Network Policy Server**



- On the **Confirm Installation Selections** page, click **Install**

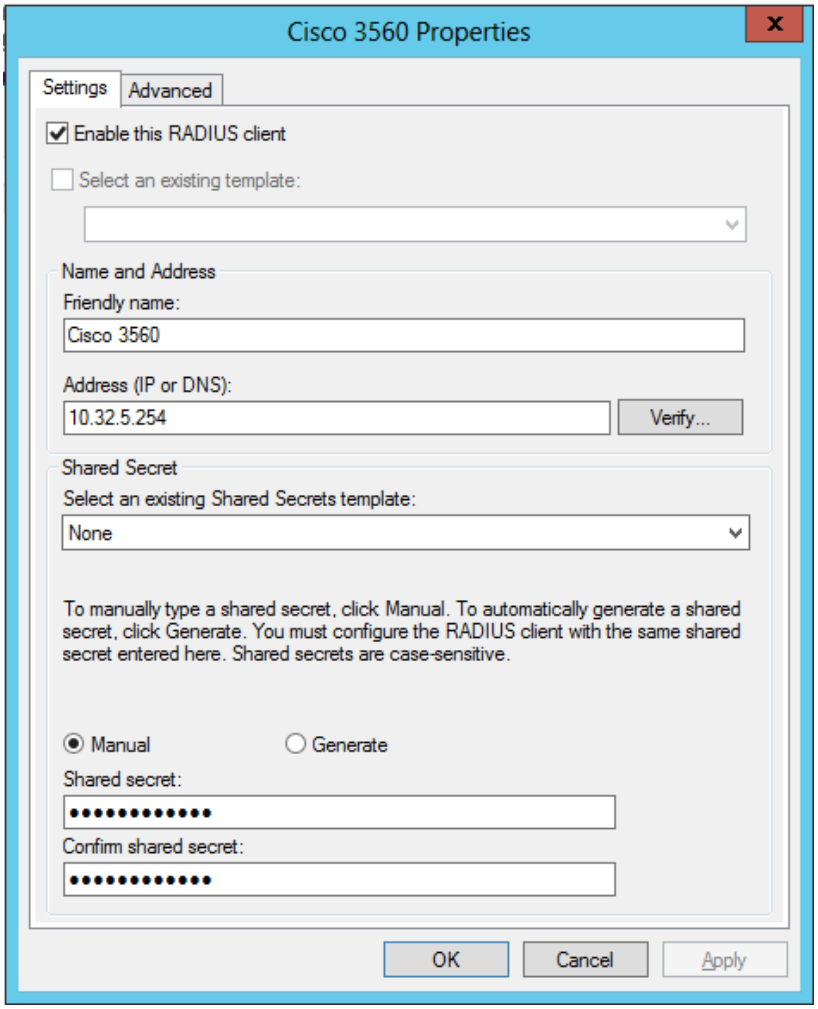


Configure Accounting

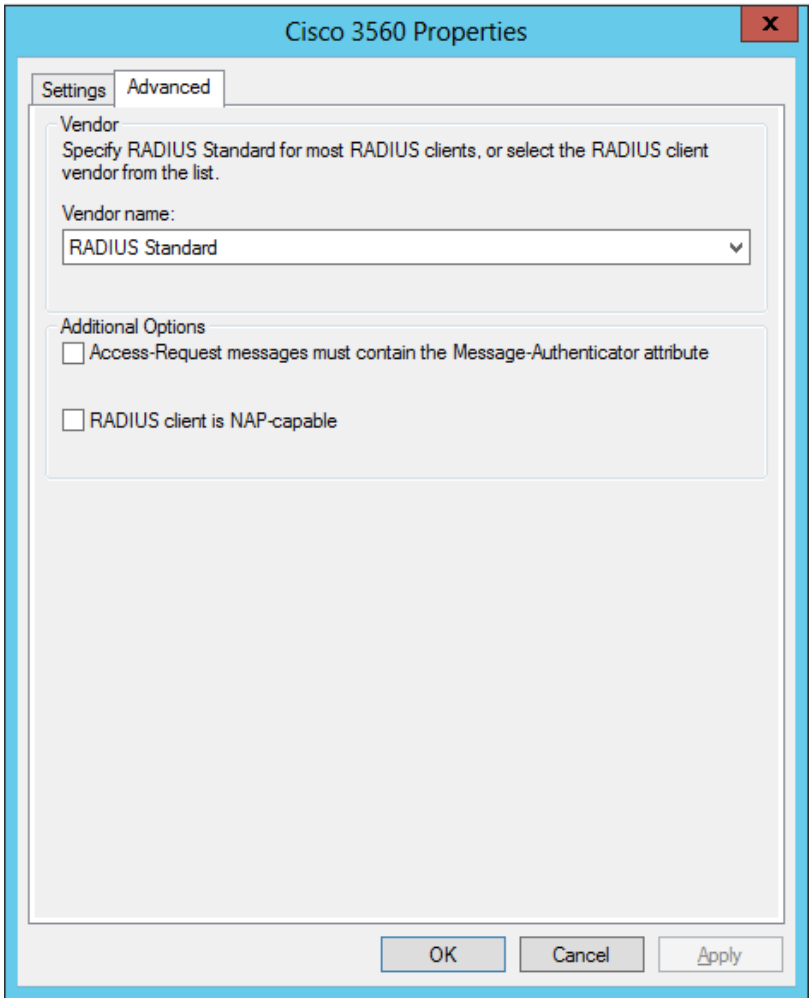
- From the **Network Policy Server** console, click on **Accounting**
- Select **Configure Local File Logging**
- On the **Log File** tab, select **IAS** as format and click **OK**

Configure RADIUS Clients on NPS Server

- Open **Network Policy Server** from **Administrative Tools**
- Expand RADIUS Clients and Servers, right click on **RADIUS Clients** and select **New RADIUS Client**
- On the **New RADIUS Client** dialog box, specify a friendly name and IP address
- From the **Vendor** list box, select **Cisco** and **s**pecify a **Shared Secret**



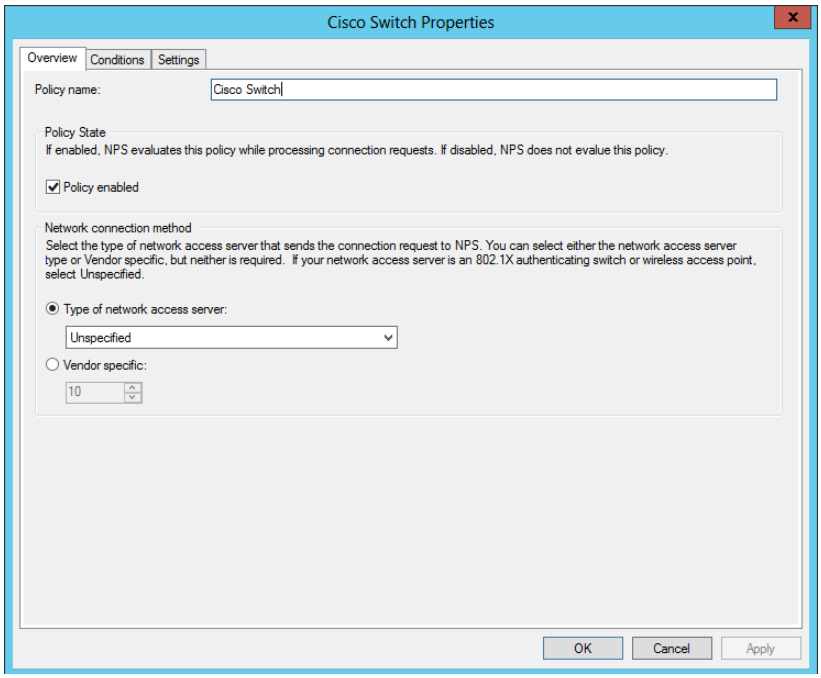
- Click on **Advanced**, uncheck or check the required options



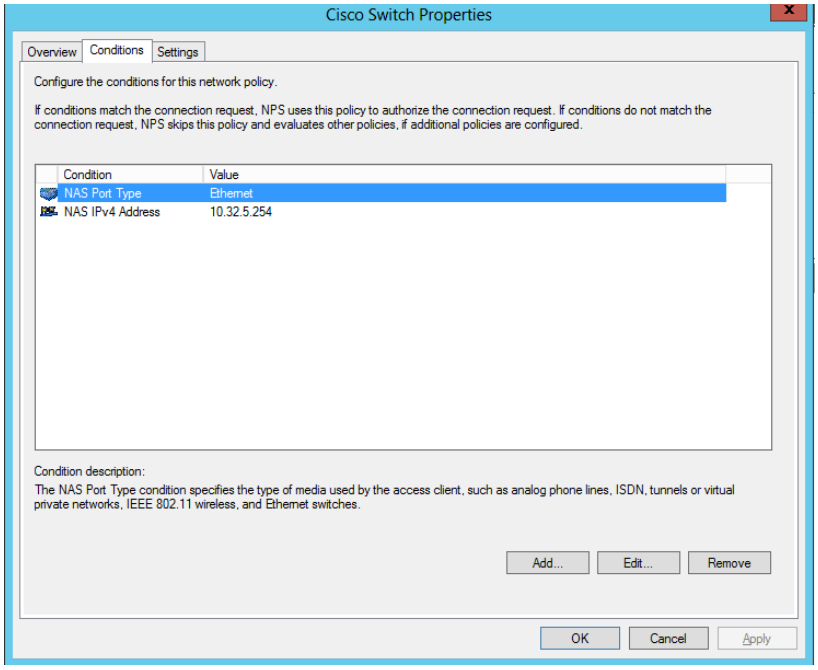
- Click **OK**

Configure a Connection Request Policy

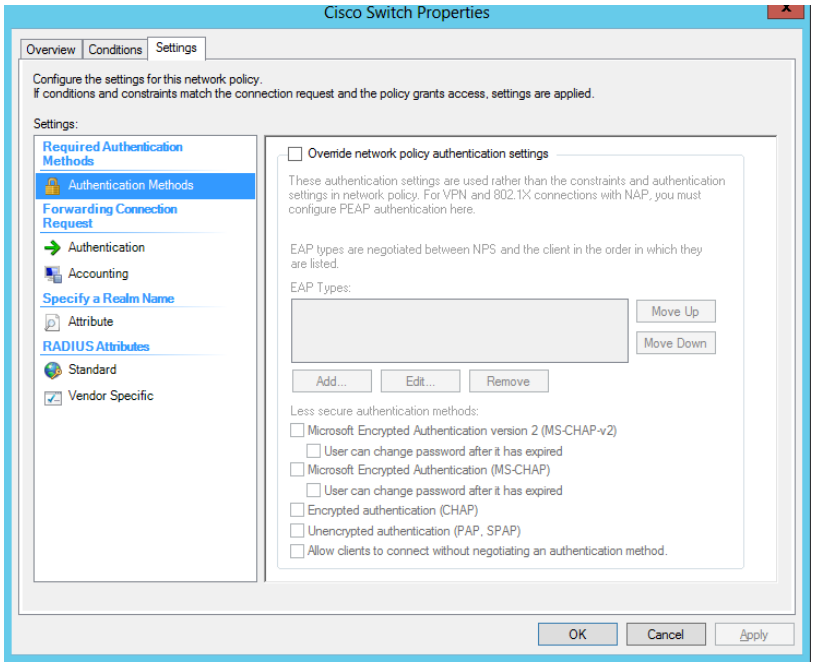
- From the **Network Policy Server** Console, right click on **Connection Request Policies** and select **New**
- On the **Specify Connection Request Policy Name and Connection Type** page, type a name for the policy and click **Next**



- On the **Specify Conditions** page, click **Add**. Select **NAS Port Type (Ethernet)**
- On the **Select conditions** dialog box, select **NAS IPv4 Address** and click **Add**
- On the **NAS IPv4 Address** dialog box, type the management IP address of the switch.



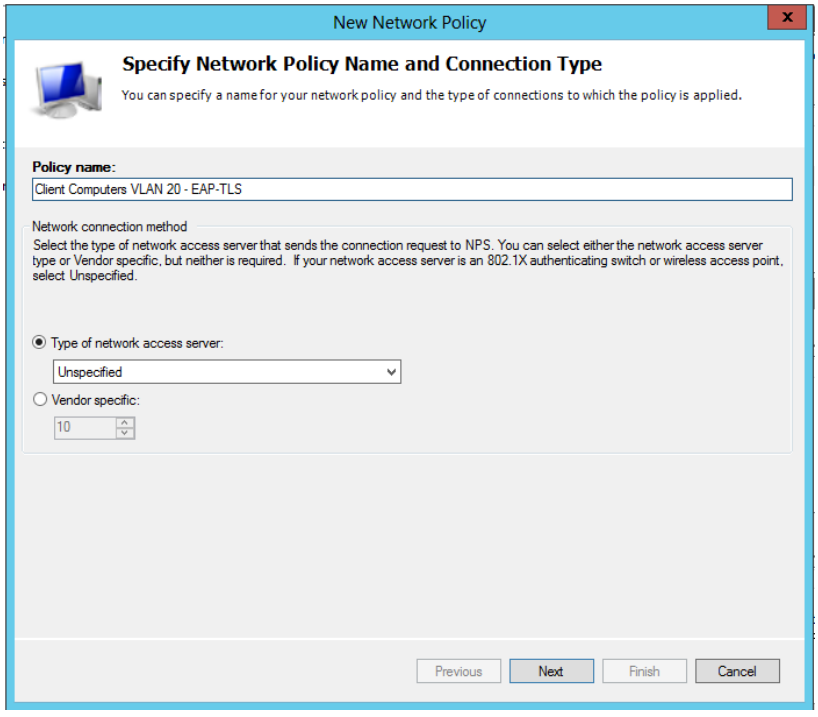
- Click **OK** and click **Next**
- On the **Specify Connection Request Forwarding** page, select **Authenticate requests on this server** and click **Next**
- On the **Specify Authentication Methods** page, click **Next**



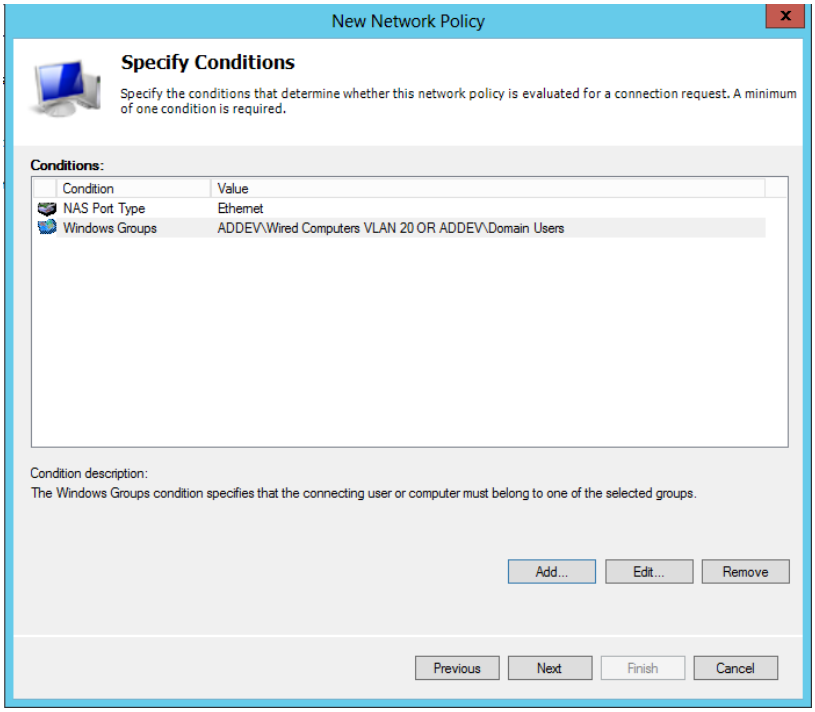
- On the **Configure Settings** page, click **Next**
- On the **Completing Connection Request Policy Wizard** page, click **Finish**

Configure a Network Policy for EAP-TLS

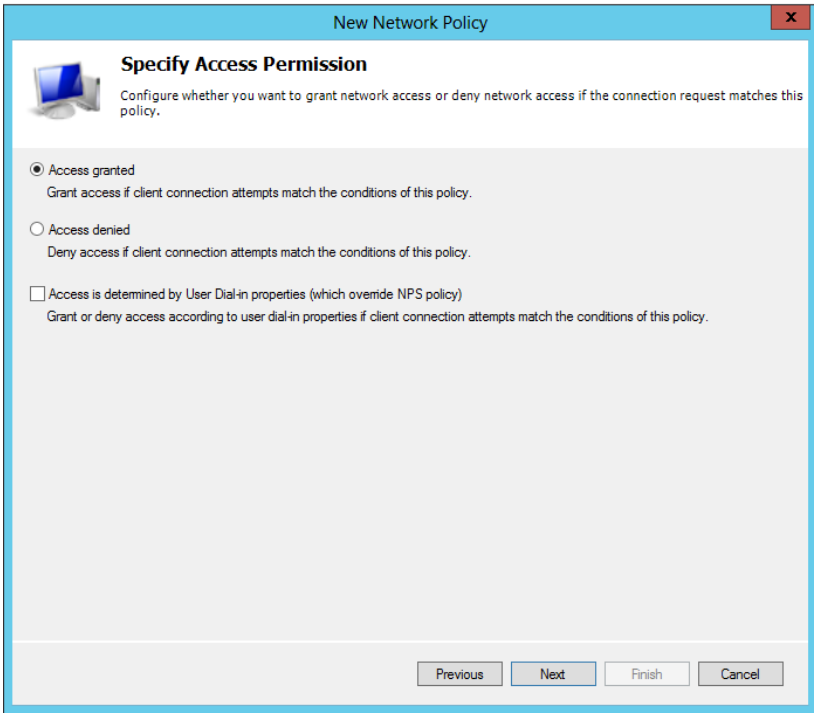
- From the **Network Policy Server Console**, right click on **Network Policies** and select **New**
- On the **Specify Network Policy Name and Connection Type** page, type a name for your policy and click **Next**



- On the **Specify Conditions** page, click **Add**
- From the **Select Conditions** dialog box, select **NAS Port Type (Ethernet)** and click **Add**
- From the **Select Condition** dialog box, add the following Windows Groups *Domain Computers, Domain Users* , and click **Next**

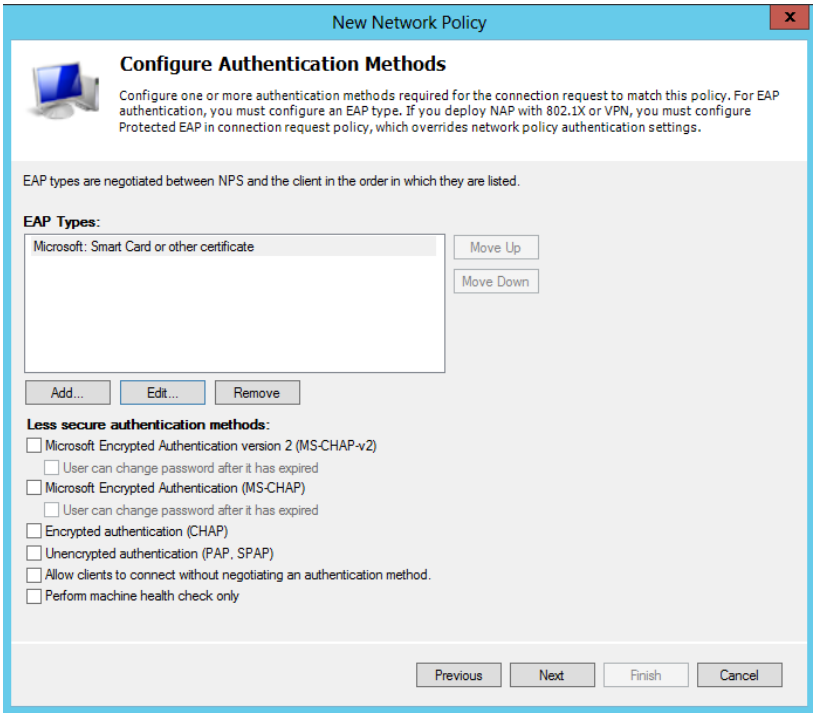


- On the **Specify Access Permissions** page, select **Access Granted** and click **Next**

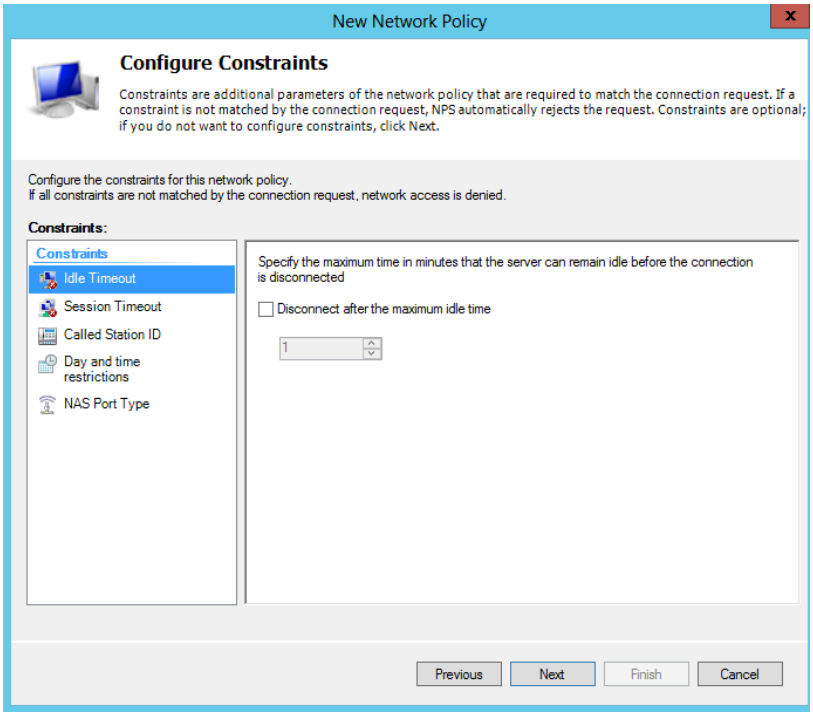


- On the **Configure Authentication Methods** page, clear MS-CHAP, clear MS-CHAP-v2 and click **Add**

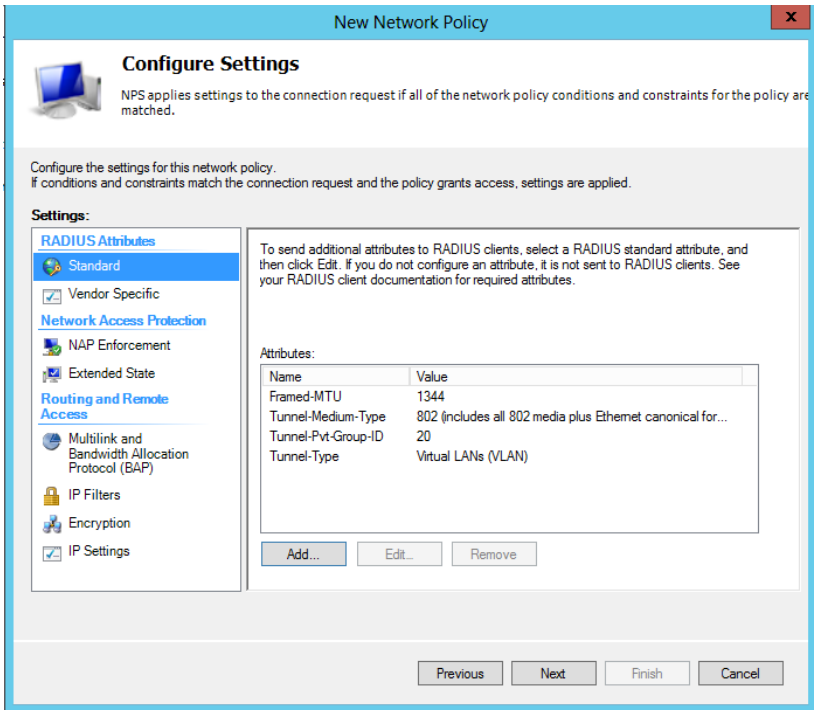
- On the **Select EAP** dialog box, select **Microsoft: Smart card or other Certificate** and click **OK**



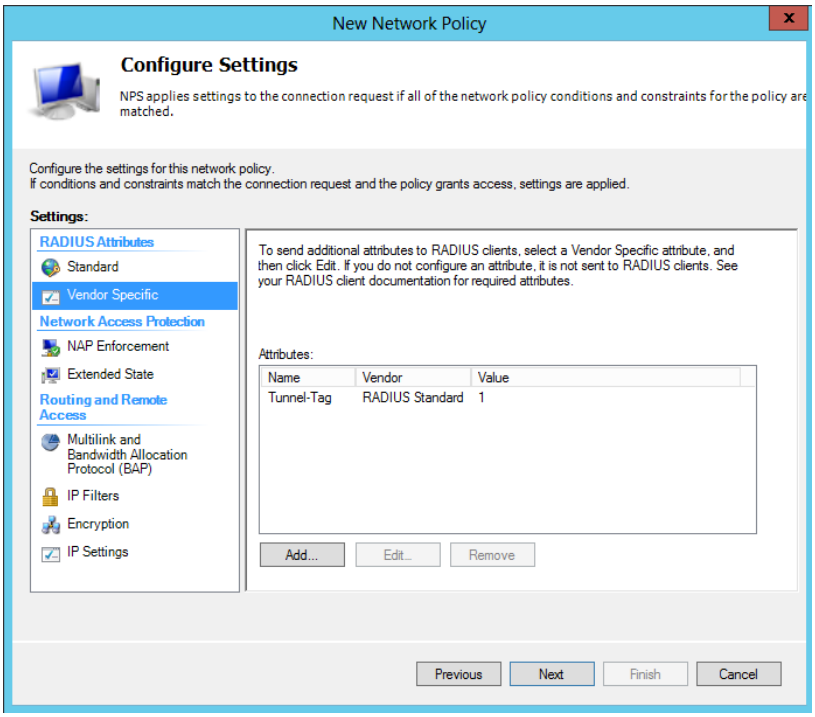
- On the **Configure Constraints** page, click **Next**



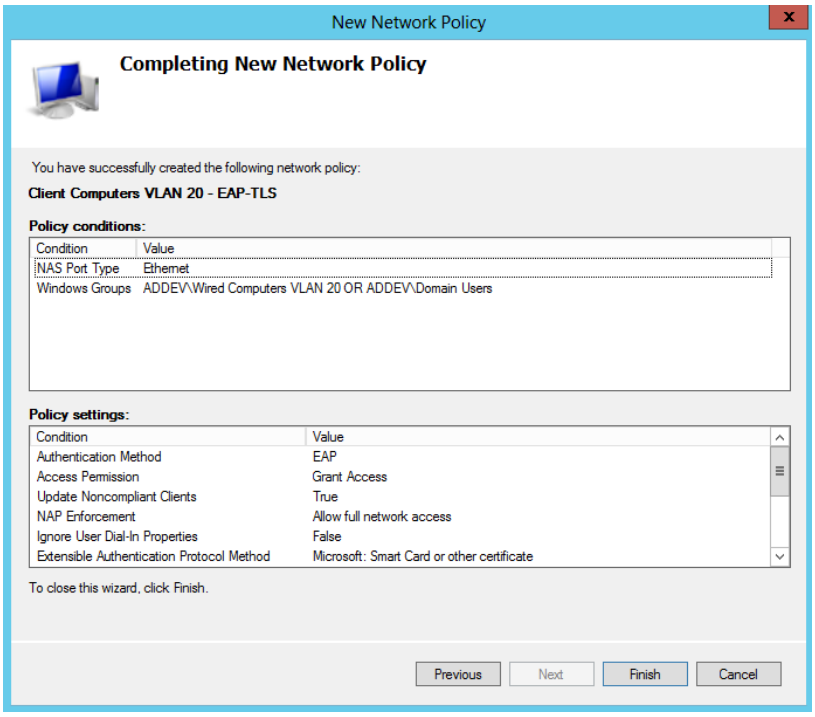
- On the **Configure Settings** page, add the following **Standard Attributes**



- Click on **Vendor Specific** attributes and add **Microsoft Tunnel-Tag** equal to 1, click **OK** and click **Next**

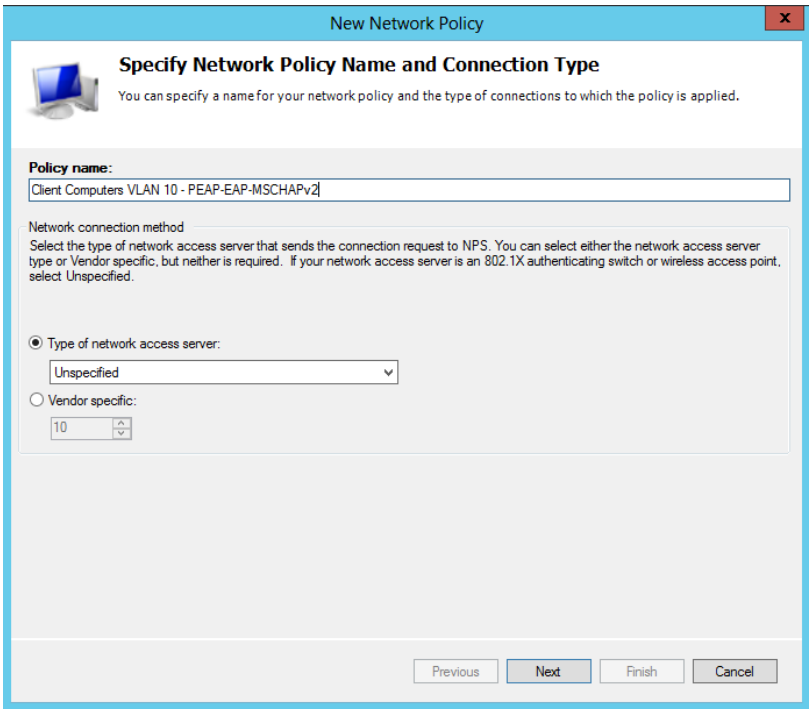


- On the **Completing New Network Policy** page, click **Finish**



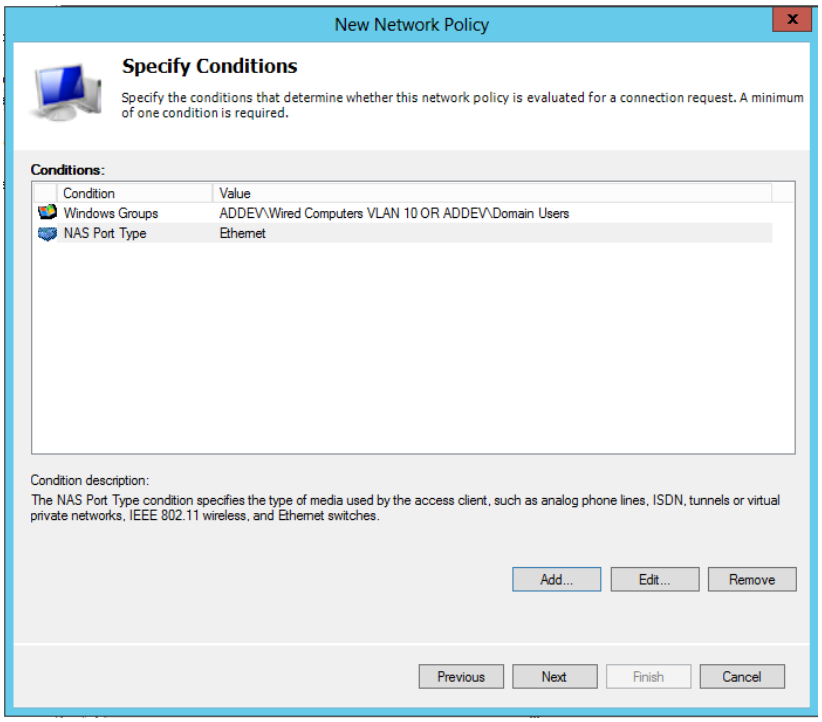
Configure a Network Policy for PEAP-EAP-MSCHAPv2

- From the **Network Policy Server Console**, right click on **Network Policies** and select **New**
- On the **Specify Network Policy Name and Connection Type** page, type a name for your policy and click **Next**

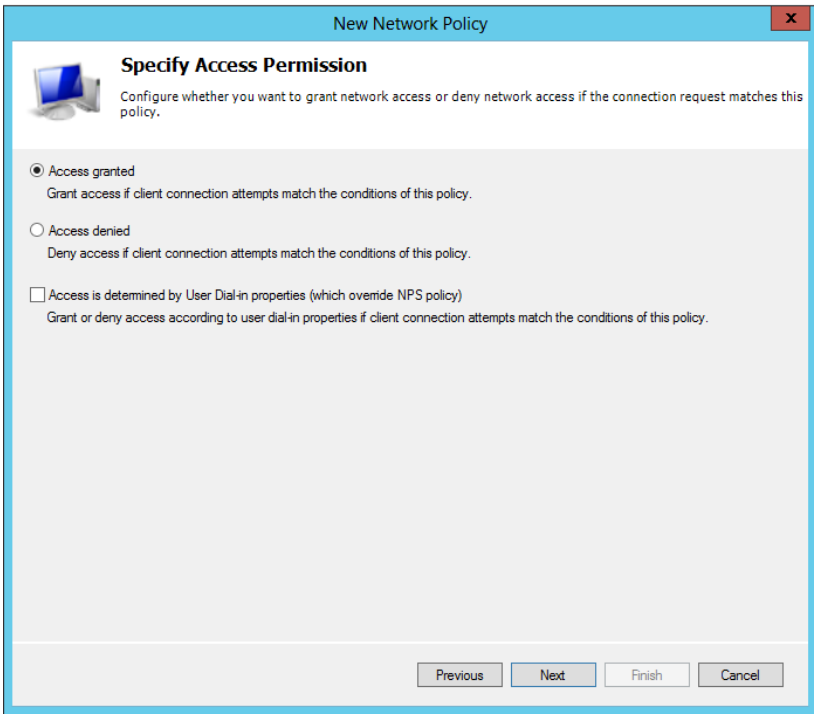


- On the **Specify Conditions** page, click **Add**

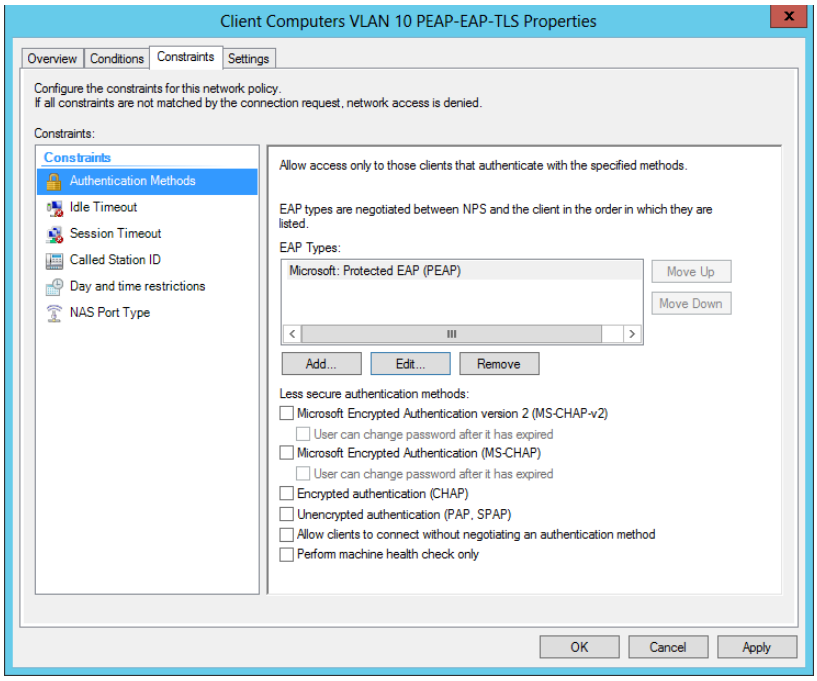
- From the **Select Conditions** dialog box, select **NAS Port Type (Ethernet)** and click **Add**
- From the **Select Condition** dialog box, add the following Windows Groups *Domain Computers*, *Domain Users* and click **Next**



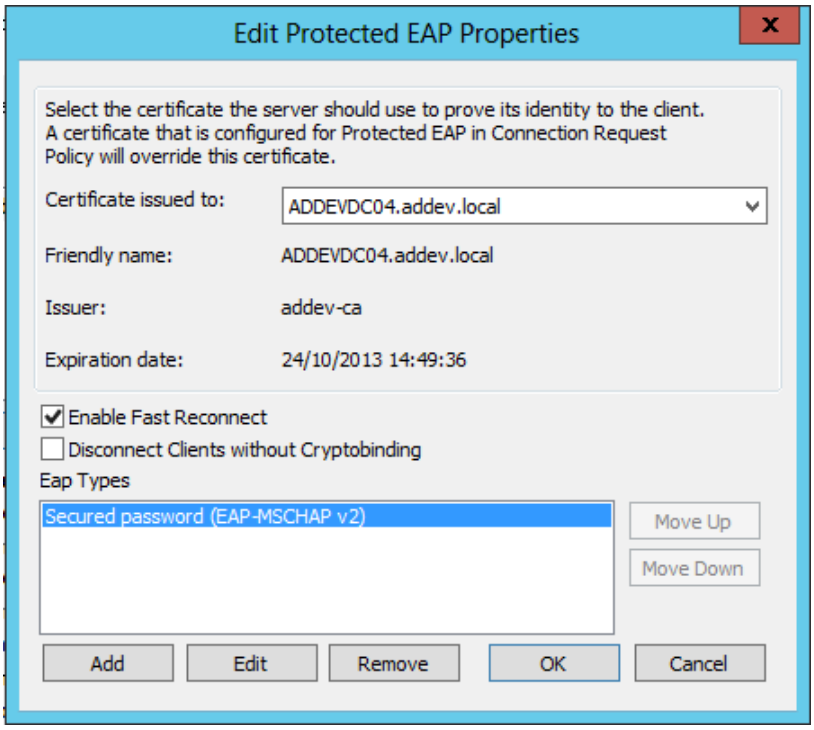
- On the **Specify Access Permissions** page, select **Access Granted** and click **Next**



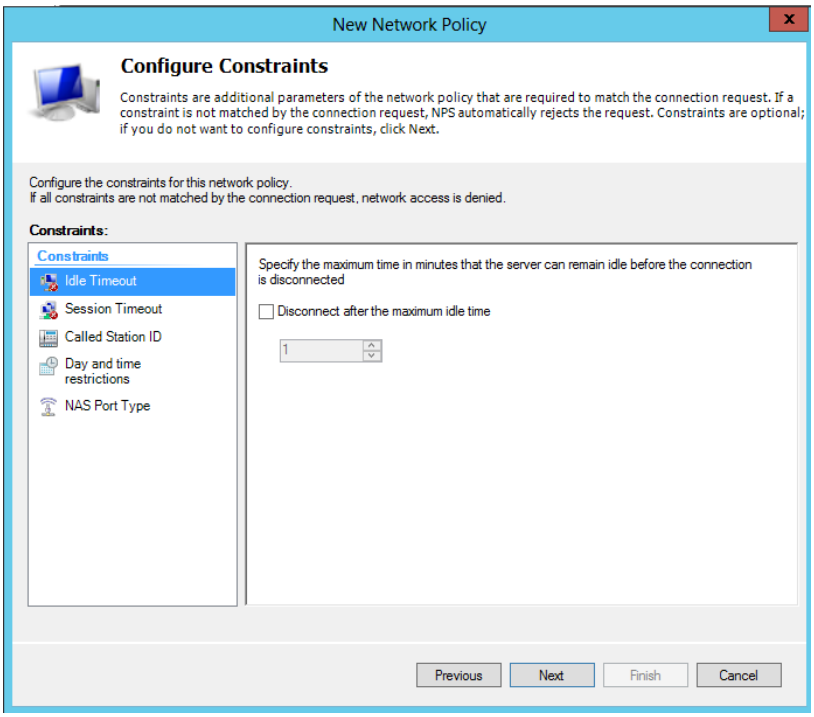
- On the **Configure Authentication Methods** page, clear MS-CHAP, clear MS-CHAP-v2 and click **Add**
- On the **Select EAP** dialog box, select **Microsoft: Protected EAP (PEAP)**



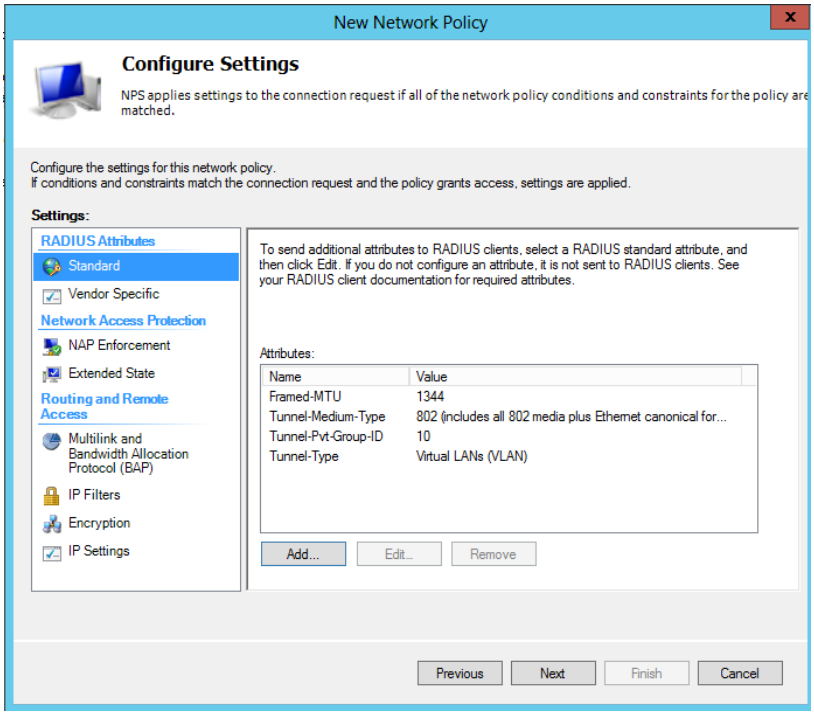
- Configure settings as below and click **OK**



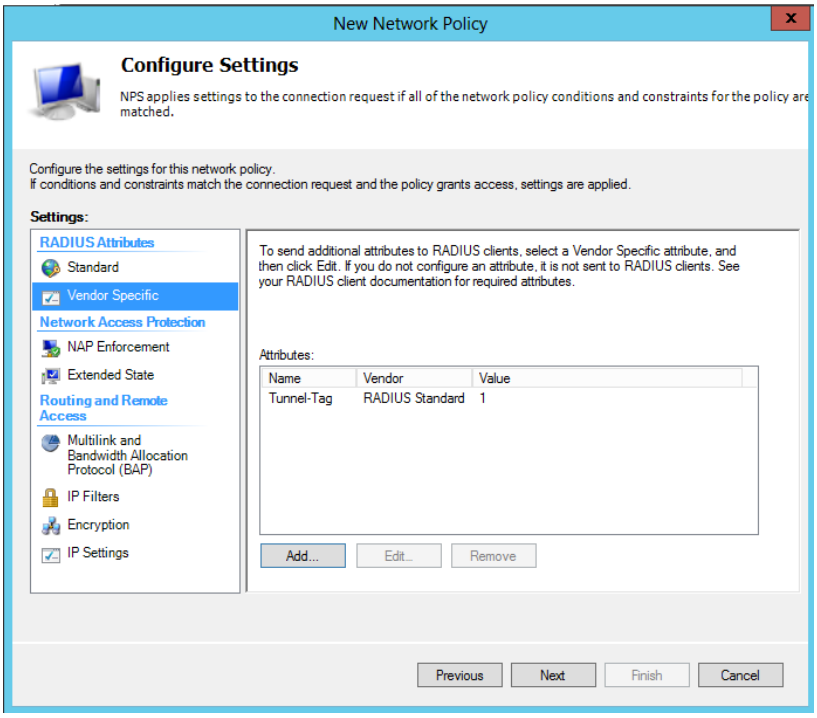
- On the **Configure Constraints** page, click **Next**



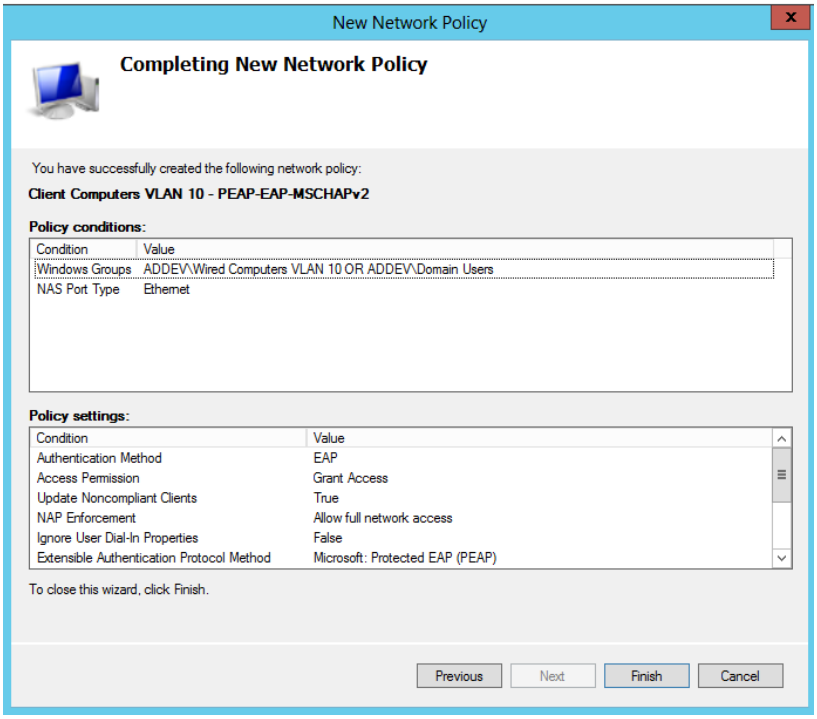
- On the **Configure Settings** page, add the following **Standard Attributes**



- Click on **Vendor Specific** attributes and add **Microsoft Tunnel-Tag** equal to 1, click **OK** and click **Next**

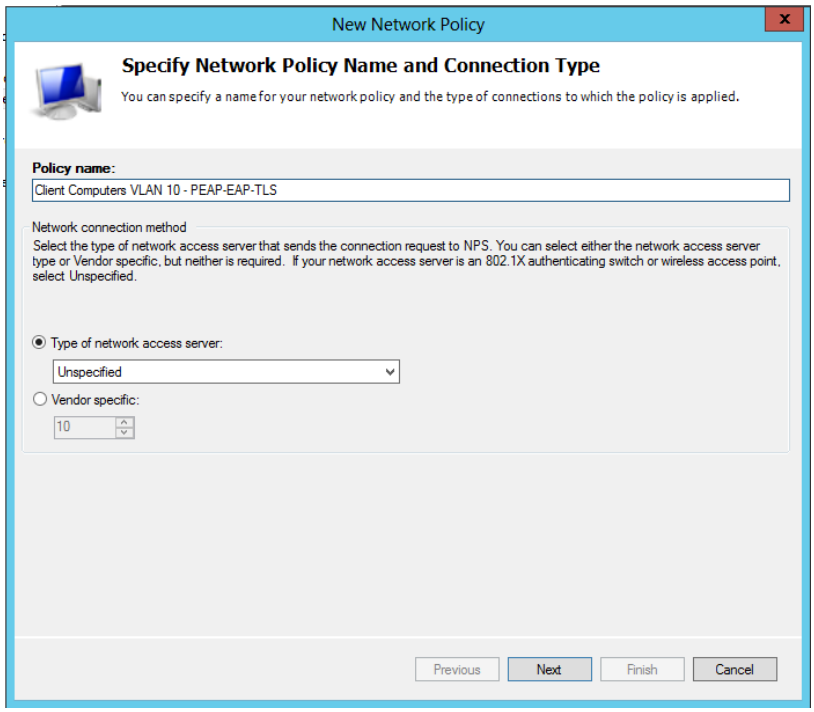


- On the **Completing New Network Policy** page, click **Finish**

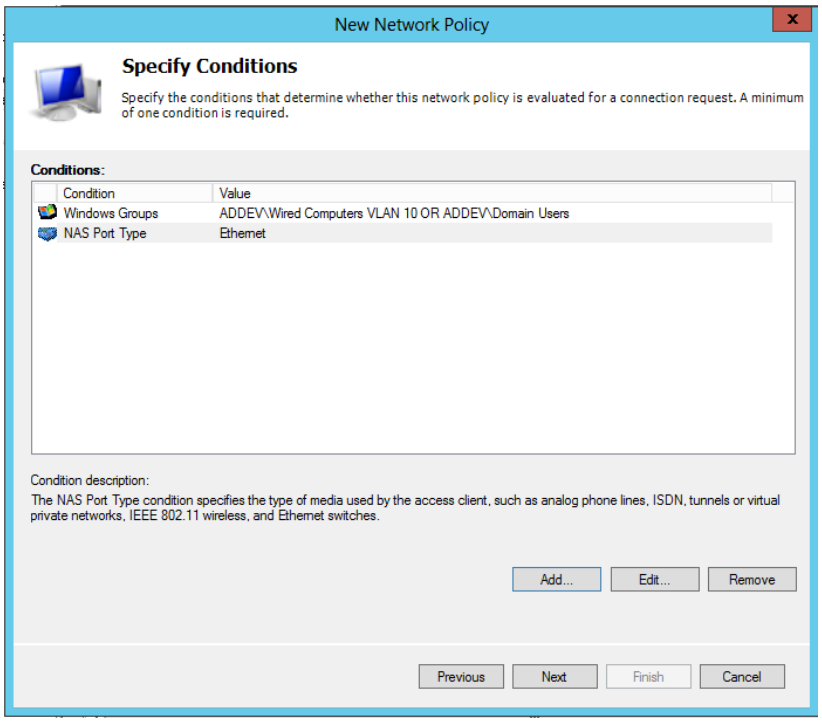


Configure a Network Policy for PEAP-EAP-TLS

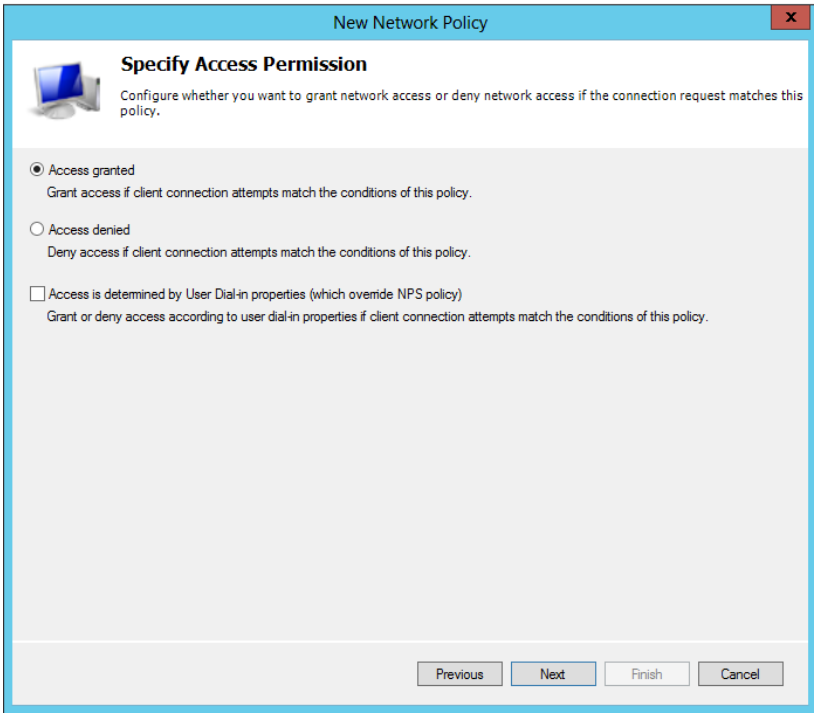
- From the **Network Policy Server Console**, right click on **Network Policies** and select **New**
- On the **Specify Network Policy Name and Connection Type** page, type a name for your policy and click **Next**



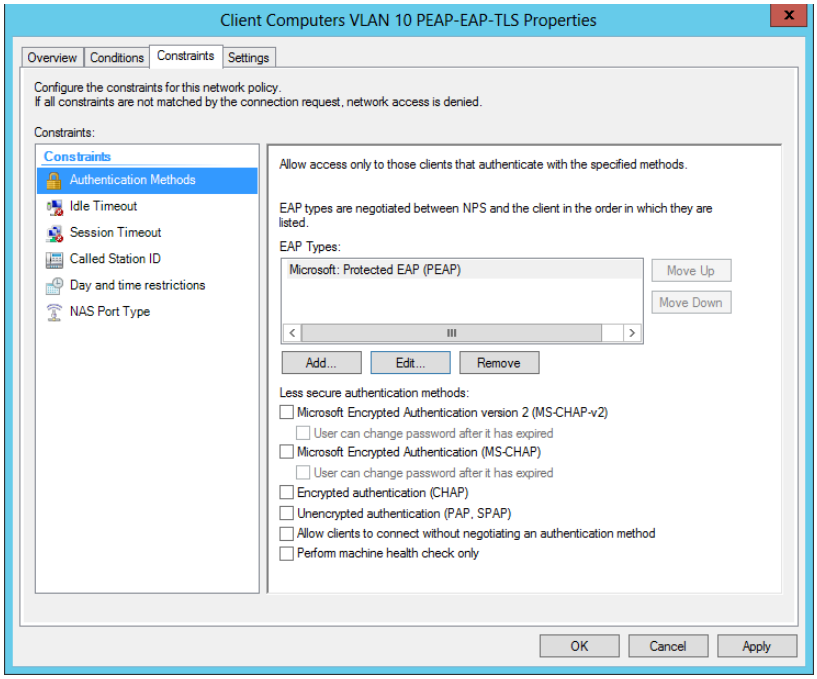
- On the **Specify Conditions** page, click **Add**
- From the **Select Conditions** dialog box, select **NAS Port Type (Ethernet)** and click **Add**
- From the **Select Condition** dialog box, add the following Windows Groups *Domain Computers*, *Domain Users* and click **Next**



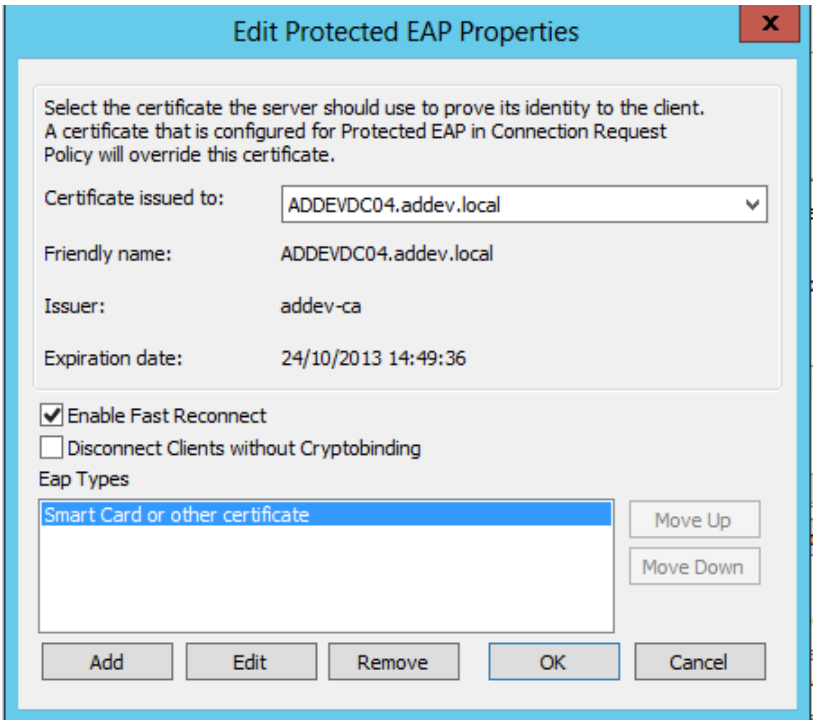
- On the **Specify Access Permissions** page, select **Access Granted** and click **Next**



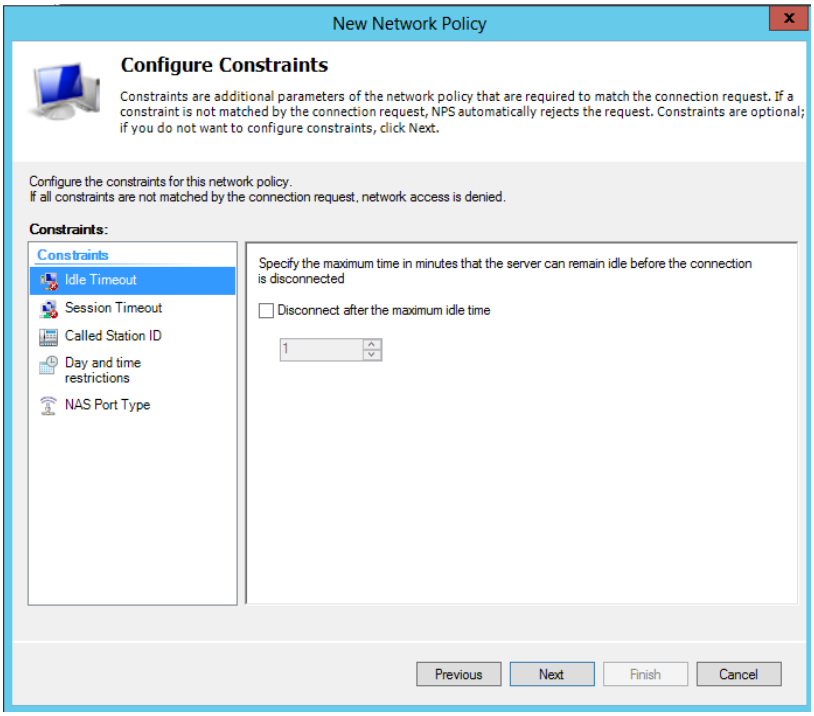
- On the **Configure Authentication Methods** page, clear MS-CHAP, clear MS-CHAP-v2 and click **Add**
- On the **Select EAP** dialog box, select **Microsoft: Protected EAP (PEAP)**



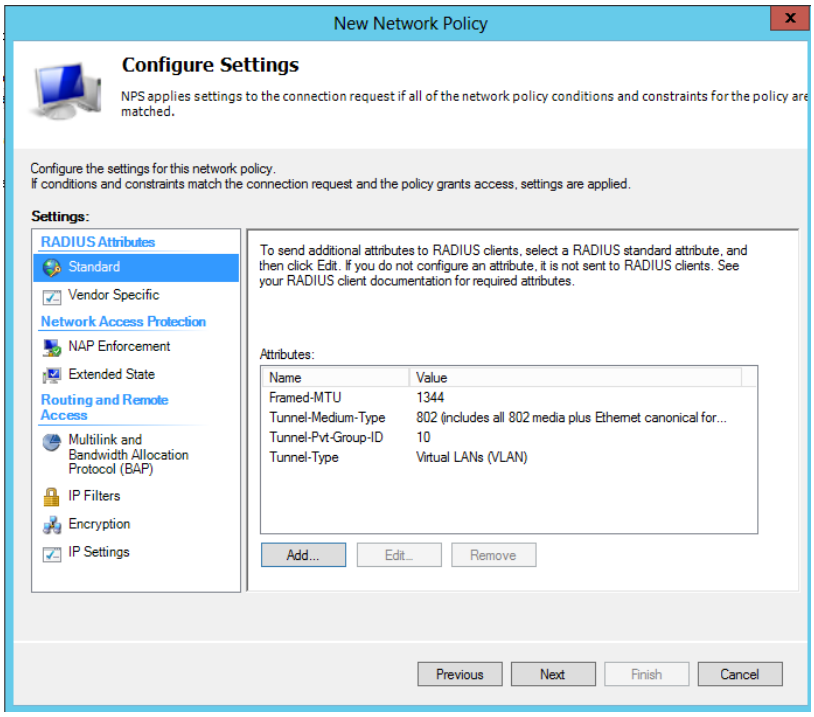
- Configure settings as below and click **OK**



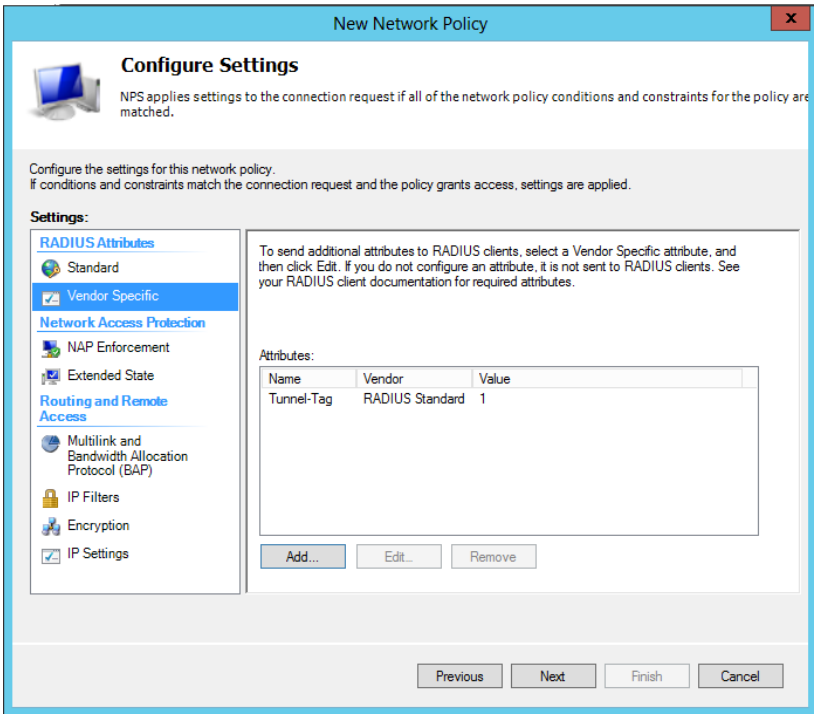
- On the **Configure Constraints** page, click **Next**



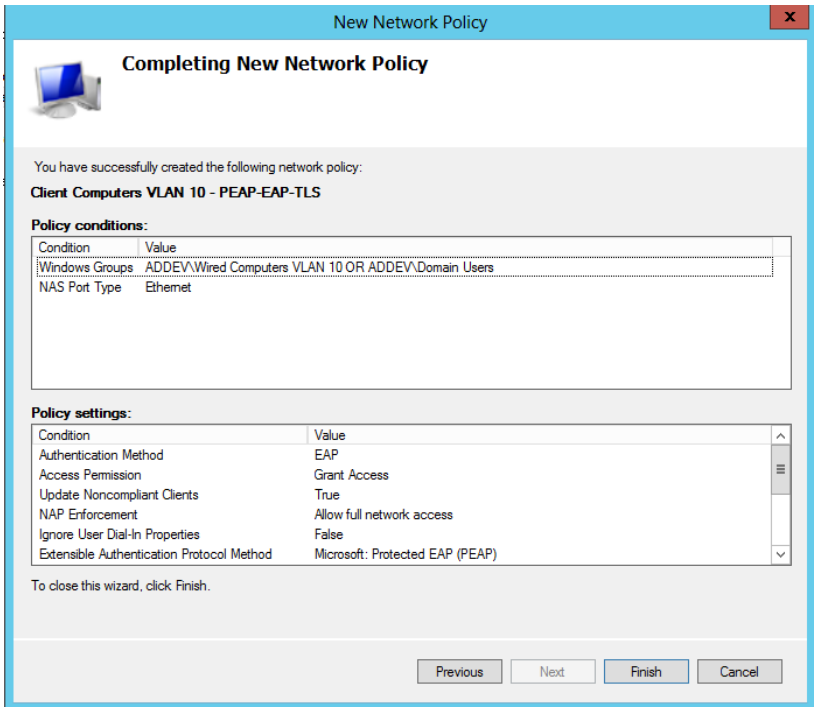
- On the **Configure Settings** page, add the following **Standard Attributes**



- Click on **Vendor Specific** attributes and add **Microsoft Tunnel-Tag** equal to 1, click **OK** and click **Next**



- On the **Completing New Network Policy** page, click **Finish**

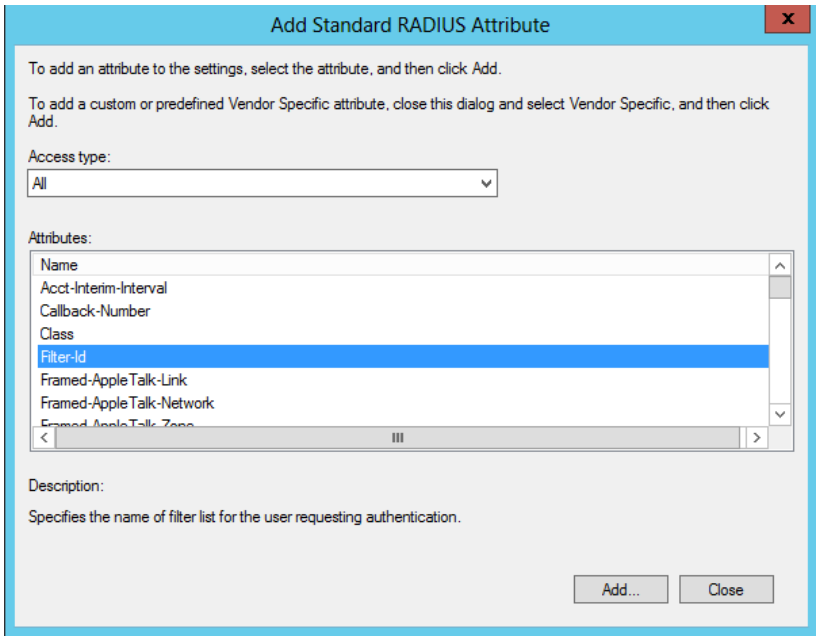


Configure your policy with Filter-Id ACL

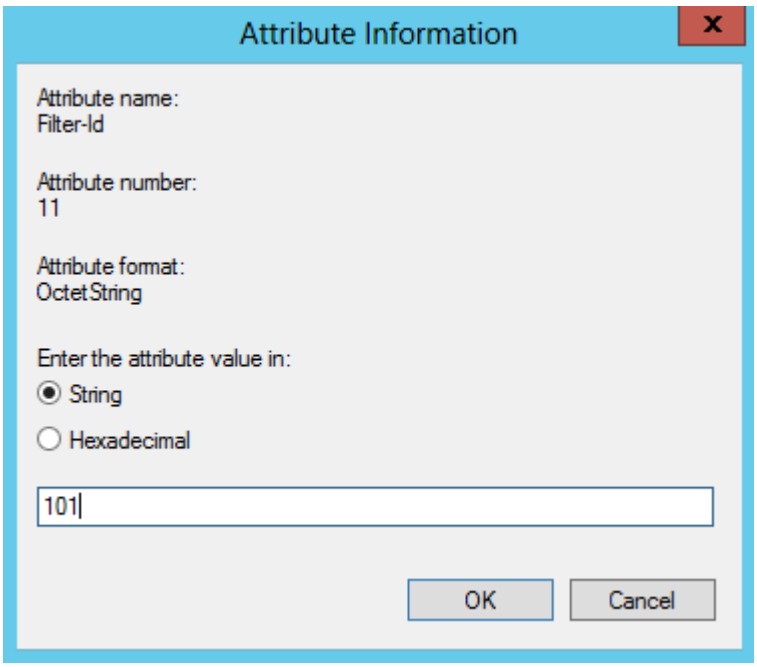
```
addevsw01(config)#access-list 101 deny tcp any host 10.32.5.3 eq www
addevsw01(config)#access-list 101 permit ip any any
```

You need to add the RADIUS attribute into your Network Policy.

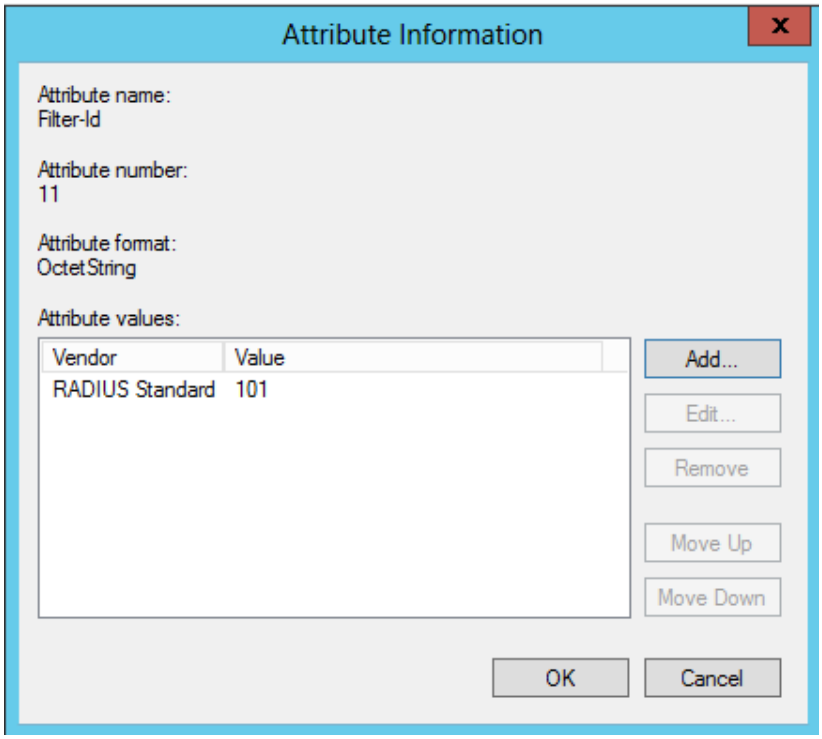
- Open **Network Policy Server** from **Administrative Tools**
- Right click on the **Network Policy**, select **Properties** and click **Settings**
- On the **Add Standard RADIUS Attribute** page, select **Filter-Id** and click **Add**



- On the **Attribute Information** page, click **String** and type the ACL number



- Click **OK**



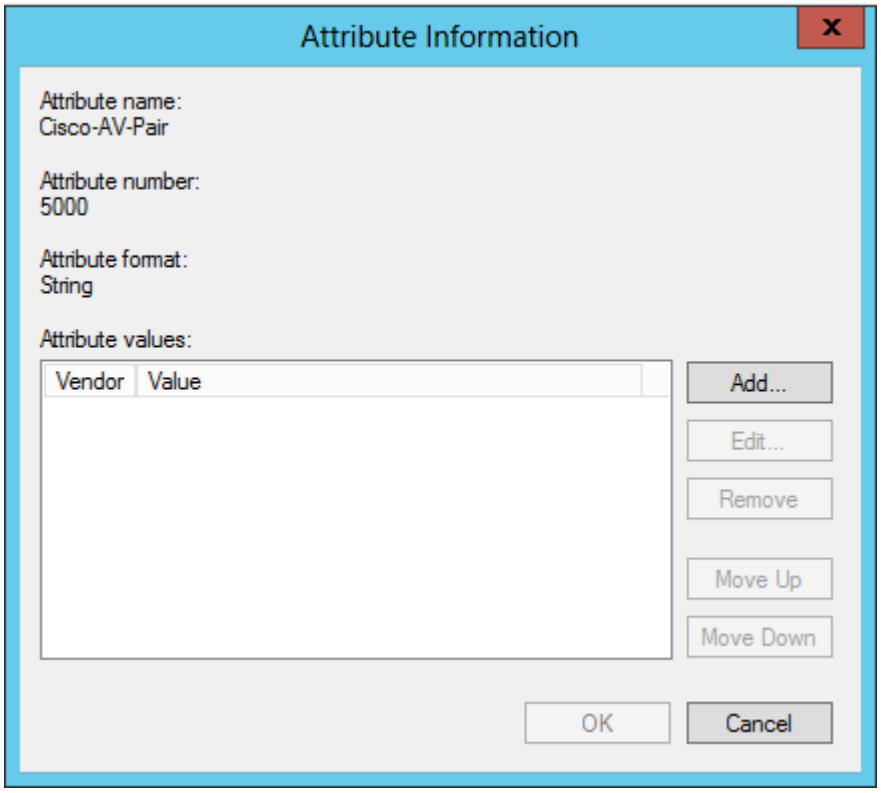
- Click **OK**

Configure your policy with Cisco-AV-Pair ACL

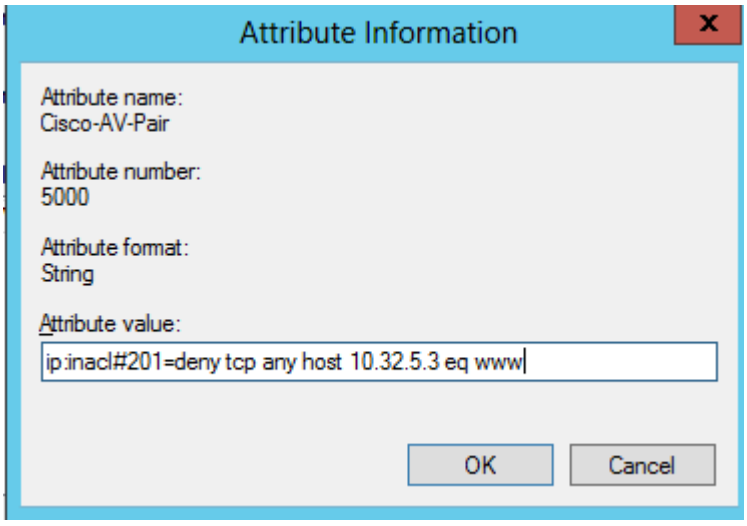
```
ip:inacl#201=deny tcp any host 10.32.5.3 eq www
ip:inacl#201=permit ip any any
```

You need to add the Vendor attribute into your Network Policy.

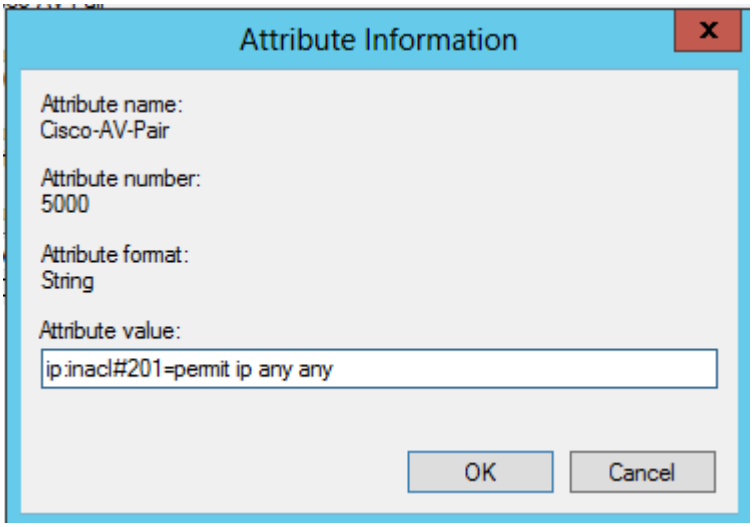
- Open **Network Policy Server** from **Administrative Tools**
- Right click on the **Network Policy**, select **Properties** and click **Settings**
- On the **Add Vendor Specific Attribute** page, select **Cisco** and click on **Cisco-AV-Pair** and click **Add**



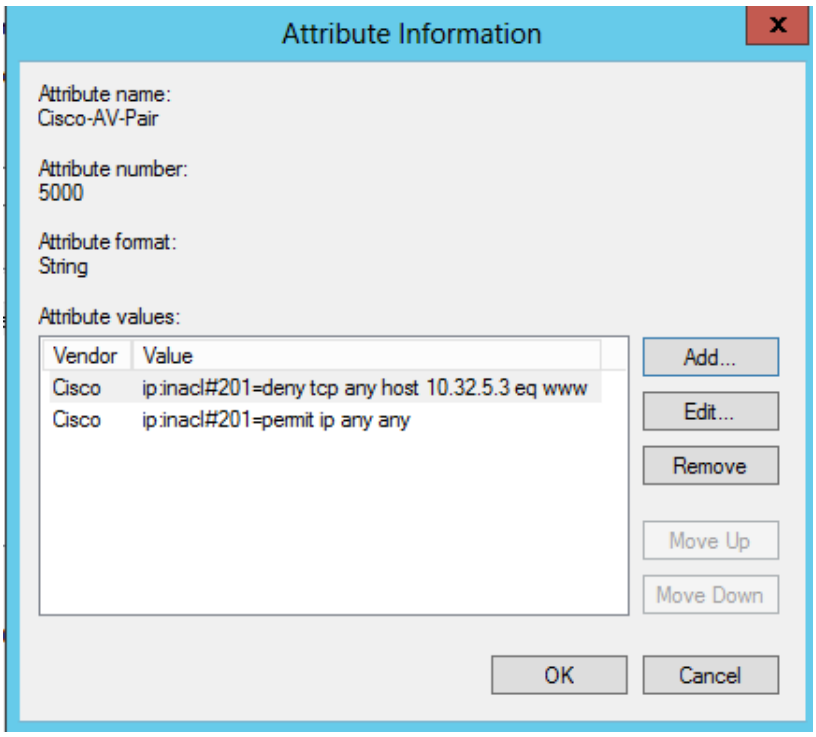
- In the **Attribute value** box, type your ACL



- Click **OK**
- In the **Attribute value** box, type your ACL



- Click **OK**



- Click **OK**, click **Close** and click **OK**

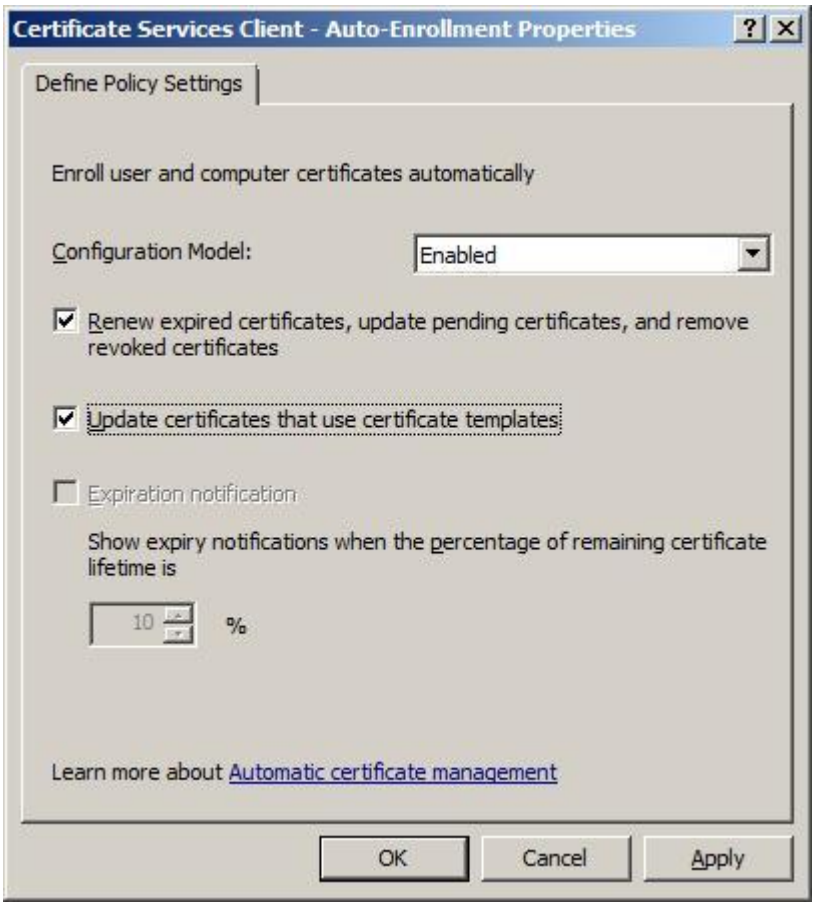
Create a Secure Baseline GPO for Windows 7 client Computers

- Configure Windows 7 client computers for certificate enrollment
- Configure Windows 7 client computers to enable Wired Authentication
- Configure Windows 7 client computers for 802.1x authentication via Group Policies and PEAP-EAP-TLS

- Configure Windows 7 client computers for 802.1x authentication via Network Sharing Center and PEAP-EAP-MSCHAPv2
- Configure Windows 7 client computers for 802.1x authentication via Network Sharing Center and EAP-TLS
- Configure Windows 7 client computers for 802.1x authentication via Network Sharing Center and PEAP-EAP-TLS

Configure Windows 7 client computers for certificate enrollment

- Open **Group Policy Management** from **Administrative Tools**
- Expand, **Domain | Group Policy Objects | Group Policy**, and select **New Group Policy Object**. Type *Secure Baseline Client Computers*
- Right click on *Secure Baseline Client Computers*, select **GPO Status** and select **User Configuration Settings Disabled**.
- Right click on **Secure Baseline Client Computers** and select **Edit**.
- Expand **Computer Configuration | Policies | Windows Settings | Security Settings** | **Public Key Policies**, double click on **Certificate Services Client-Auto Enrollment.**
- On **the Certificate Services Client-Auto Enrollment** dialog box, select **Enabled**.



- Select **Renew expired certificates**, select **Update certificates** and click **OK**.

Configure Windows 7 client computers to enable Wired Authentication

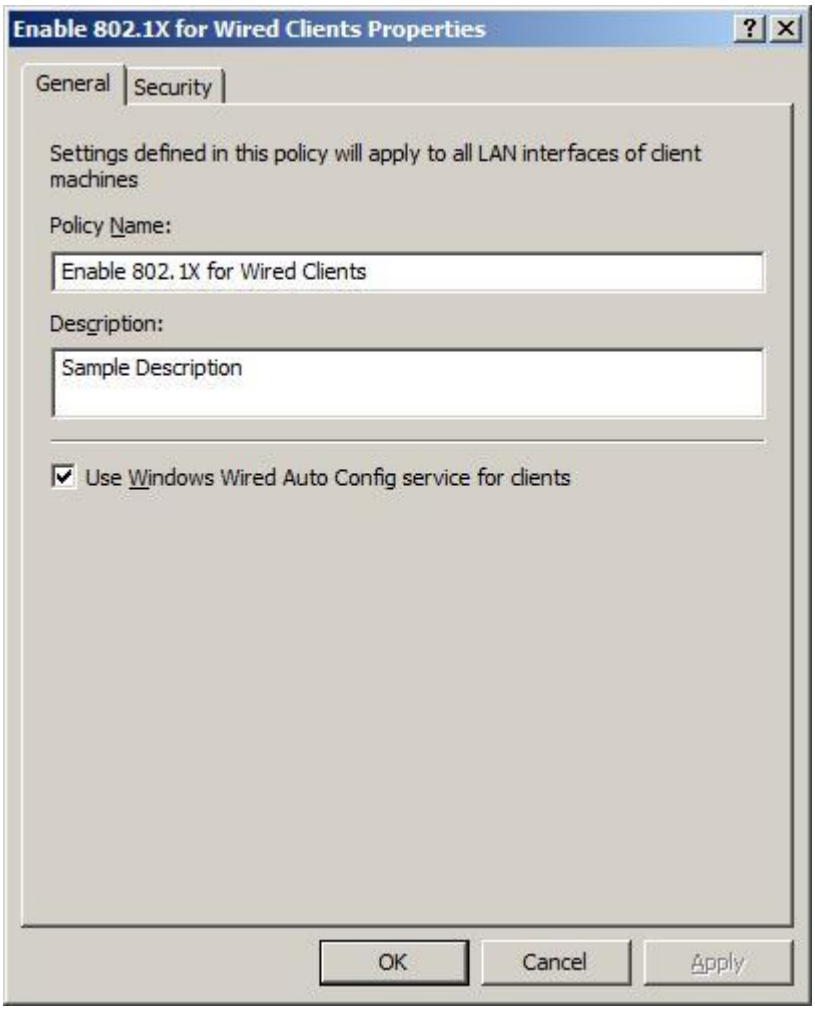
Before we can configure a Windows 7 client computer with 802.1x authentication, we need to enable the Authentication tab, which is part of the local area connection. This Authentication tab will be displayed when the Wired AutoConfig service is started.

- Select **System Services,** right click on **WiredAutoConfig**, and select **Properties**.
- Select **Define this Policy Setting**, and change service startup mode to **Automatic**.

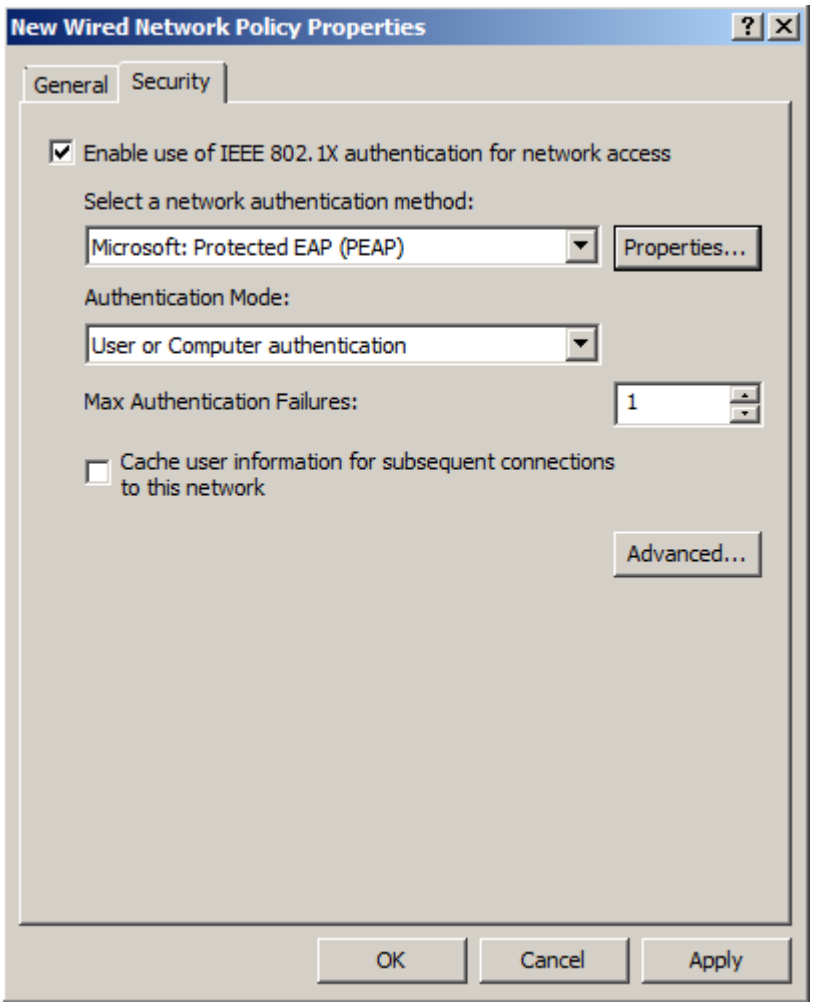
- Click **OK**.

Configure Windows 7 client computers for 802.1x authentication via Group Policy and PEAP-EAP-TLS

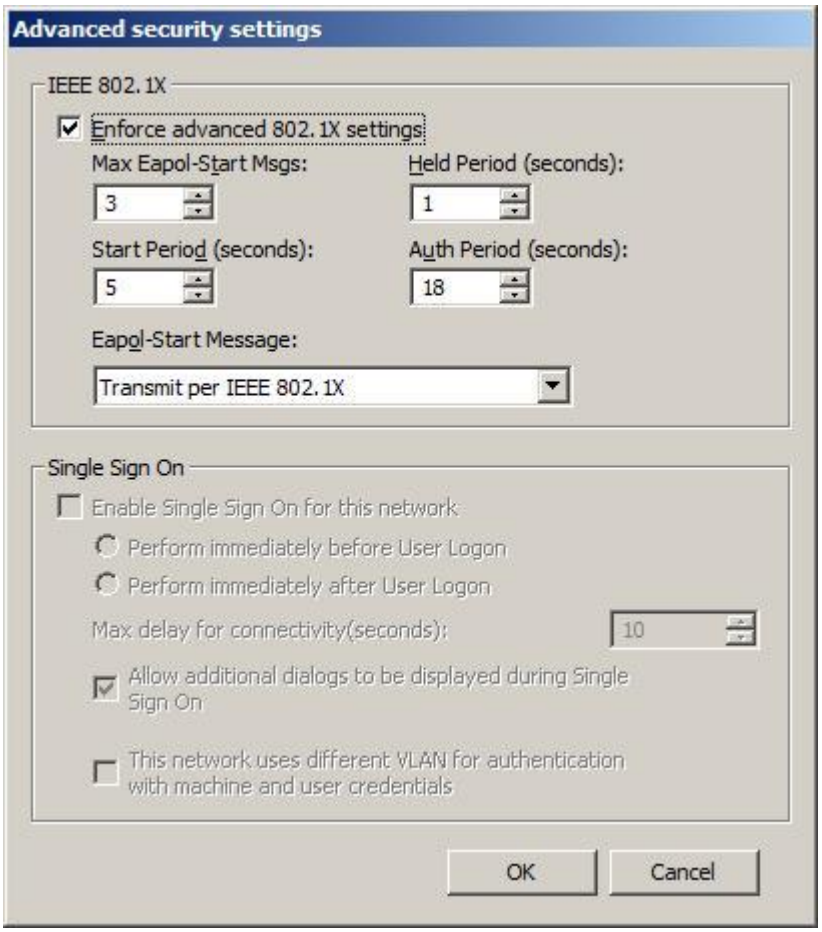
- Right click on **Wired Network Policies** and select **Create a New Windows Vista Policy.**
- On the **New Vista Wired Network Policy Properties** dialog box, type a policy name



- Click on the **Security** tab. **Select Enable use of IEEE 802.1x authentication for network access.**
- From **the Select a network authentication method** list box, select **Smart Card or certificate.**
- On the **Authentication Mode** list box, select **User or Computer authentication**.



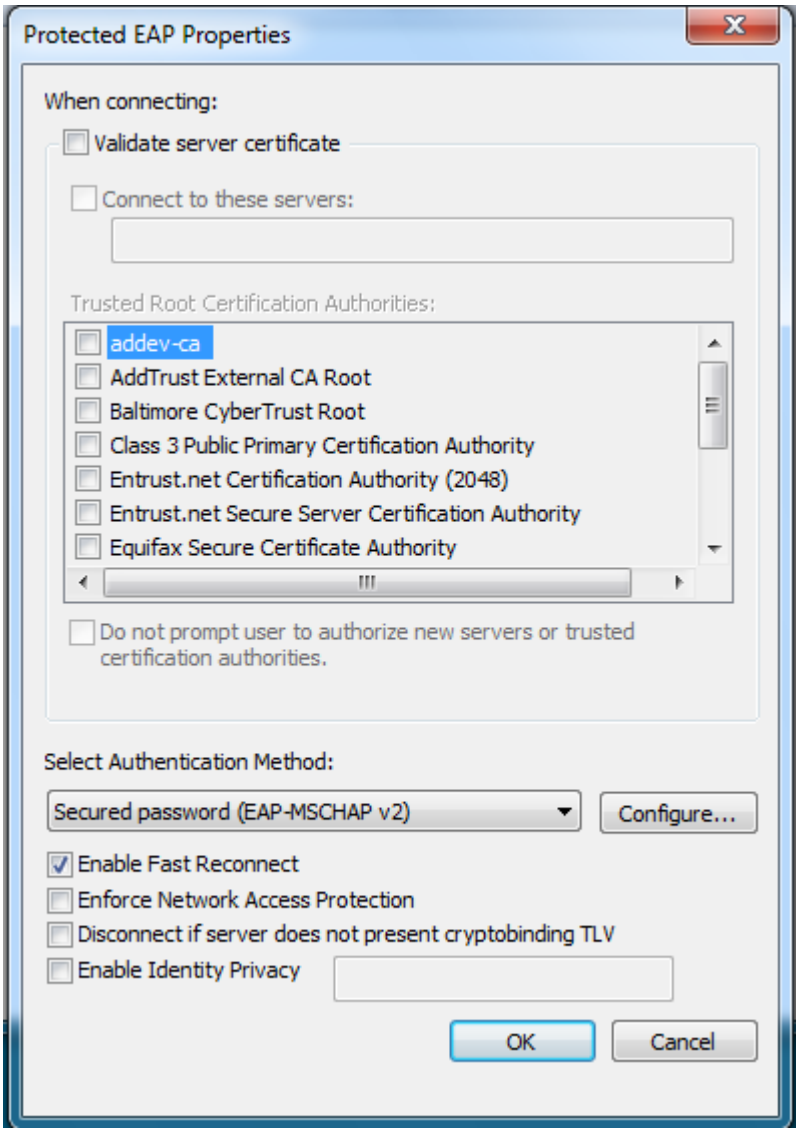
- Select **Enforce advanced 802.1X settings** and click **OK**.
- Click on **Advanced** and select **Enforce advanced 802.1X settings**



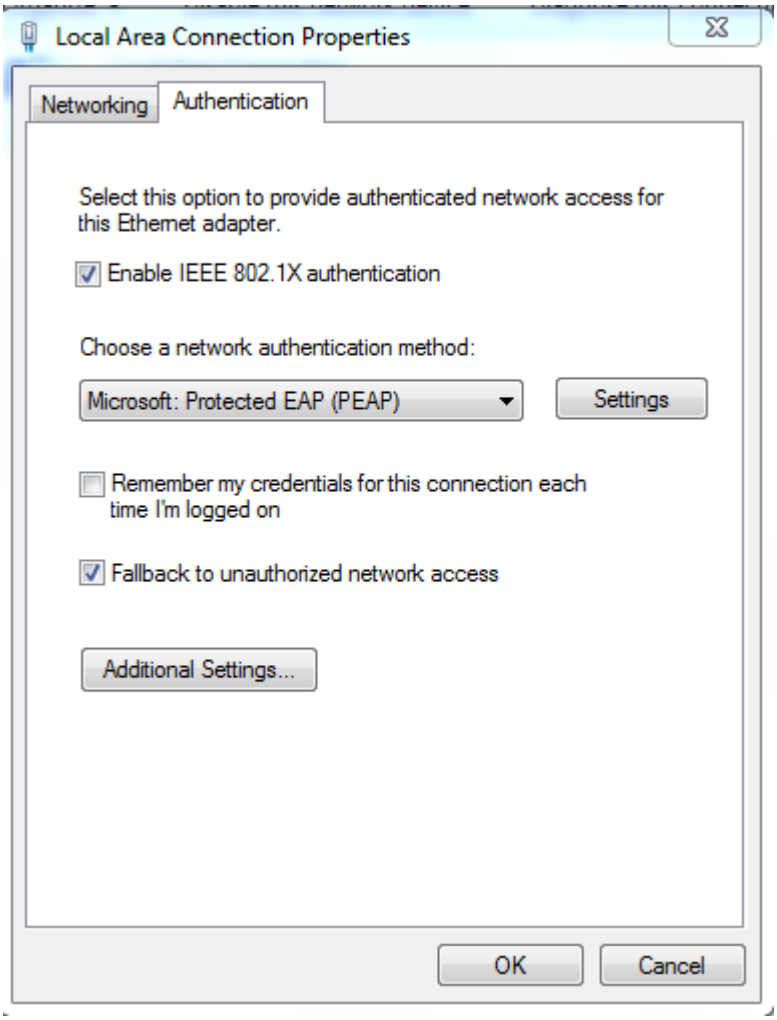
- Click **OK** and Click **OK**
- Close Group Policy Editor.
- Link GPO to the OU of your workstations
- Restart client computer or launch gpupdate.exe

Configure Windows 7 client computers for 802.1x authentication via Network and Sharing Center for PEAP-EAP-MSCHAPv2

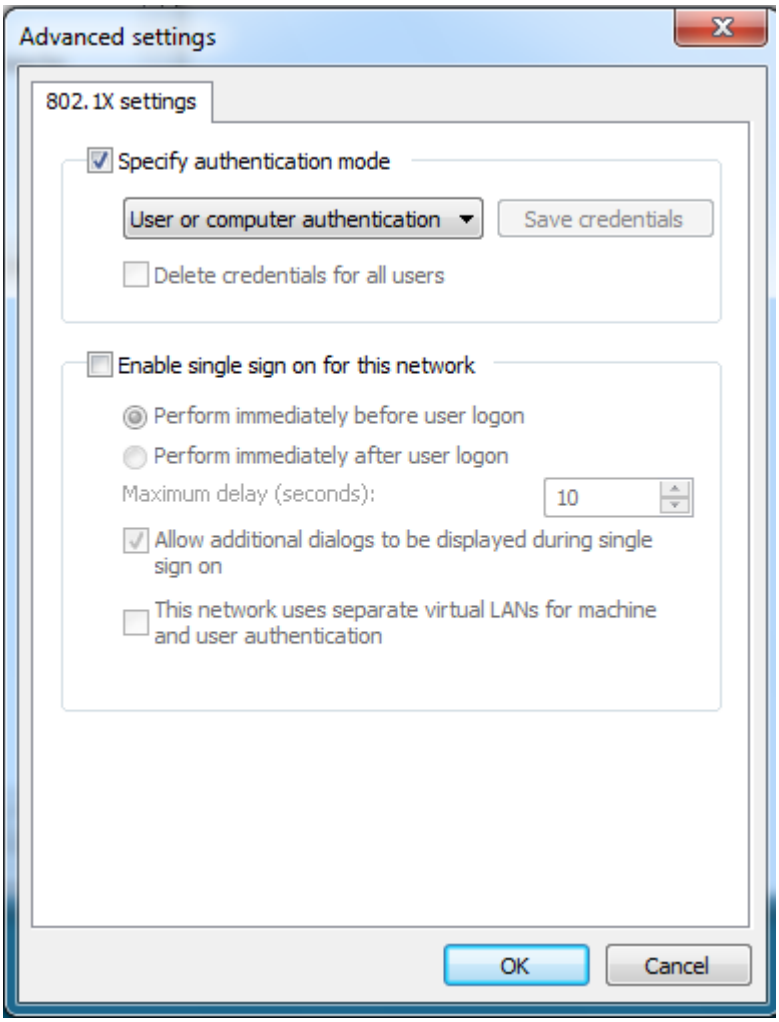
- Open **Network and sharing Center**, and select **Change adapter settings**
- Right click on **Local Area Connection** and select **Properties**
- Select **Authentication** tab and select **Enable IEEE 802.1X authentication**
- On the **Choose a network authentication method** list box, select **Microsoft: Protected EAP (PEAP)**
- Click on **Settings** and select **Secured Password (EAP-MSCHAPv2)**



- Click **OK**
- Clear **Remember my credentials for this connection each time I'm logged on** and enable **Fallback to unauthorized network access**



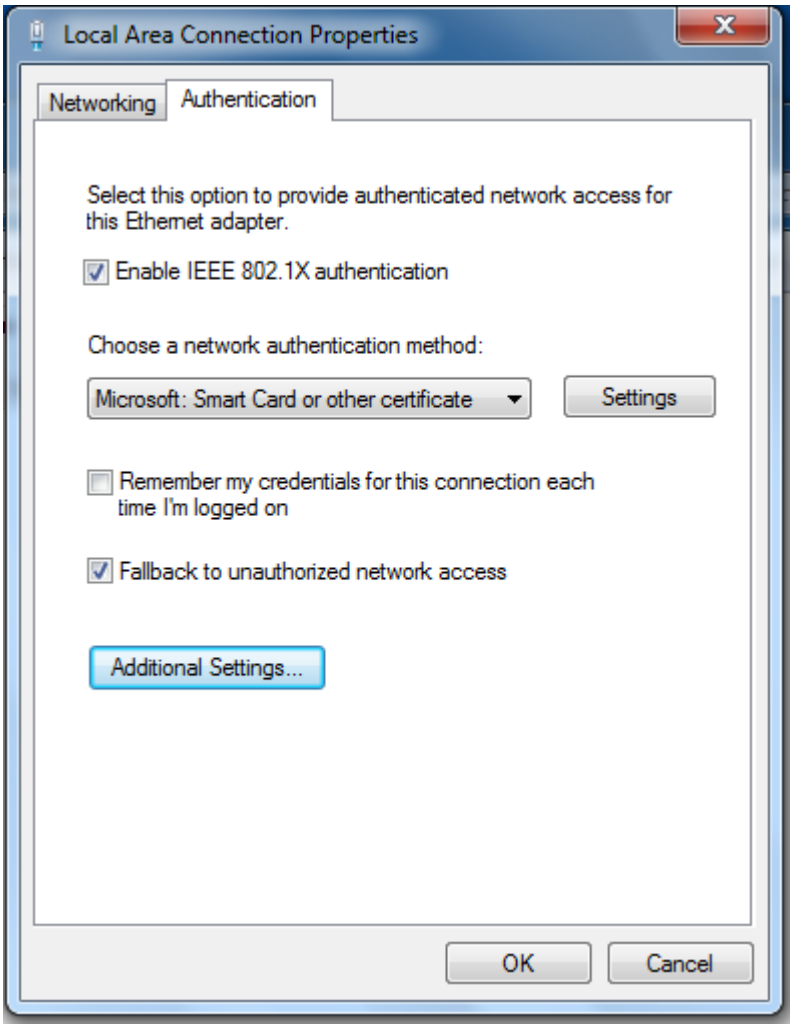
- Click **Additional Settings**, select **Specify authentication mode** and select **Computer authentication** from the list



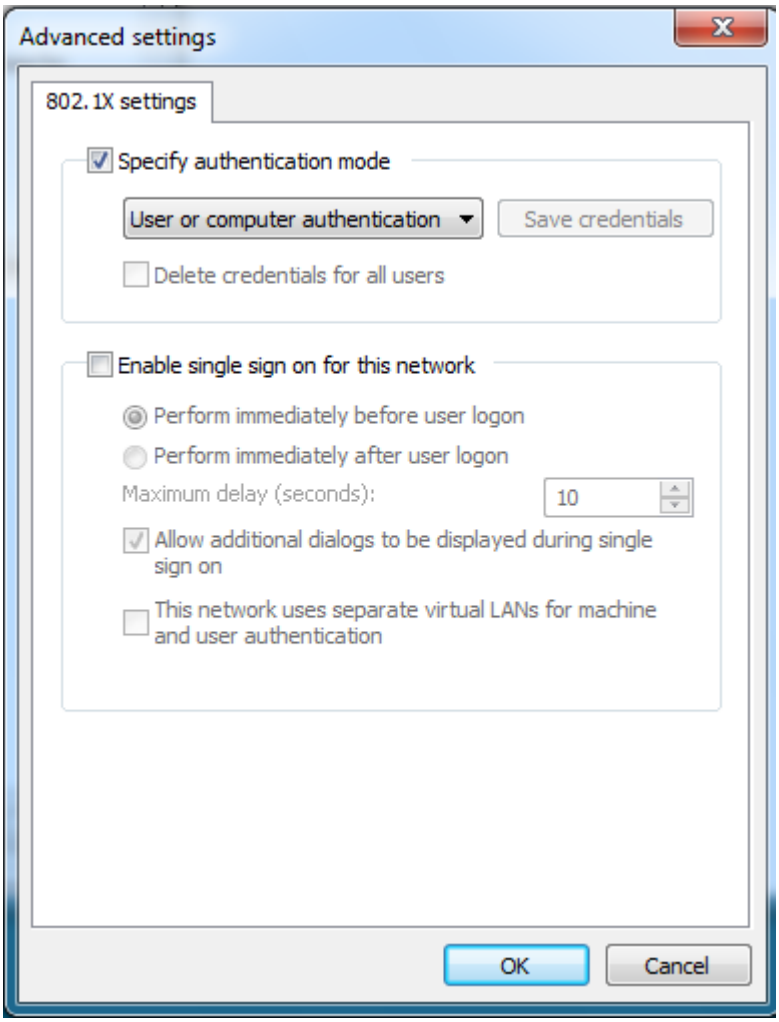
- Click **OK**

Configure Windows 7 client computers for 802.1x authentication via Network and Sharing Center for EAP-TLS

- Open **Network and sharing Center**, and select **Change adapter settings**
- Right click on **Local Area Connection** and select **Properties**
- Select **Authentication** tab and select **Enable IEEE 802.1X authentication**
- On the **Choose a network authentication method** list box, select **Microsoft: Smart Card or other Certificate**
- Clear **Remember my credentials for this connection each time I'm logged on** and enable **Fallback to unauthorized network access**



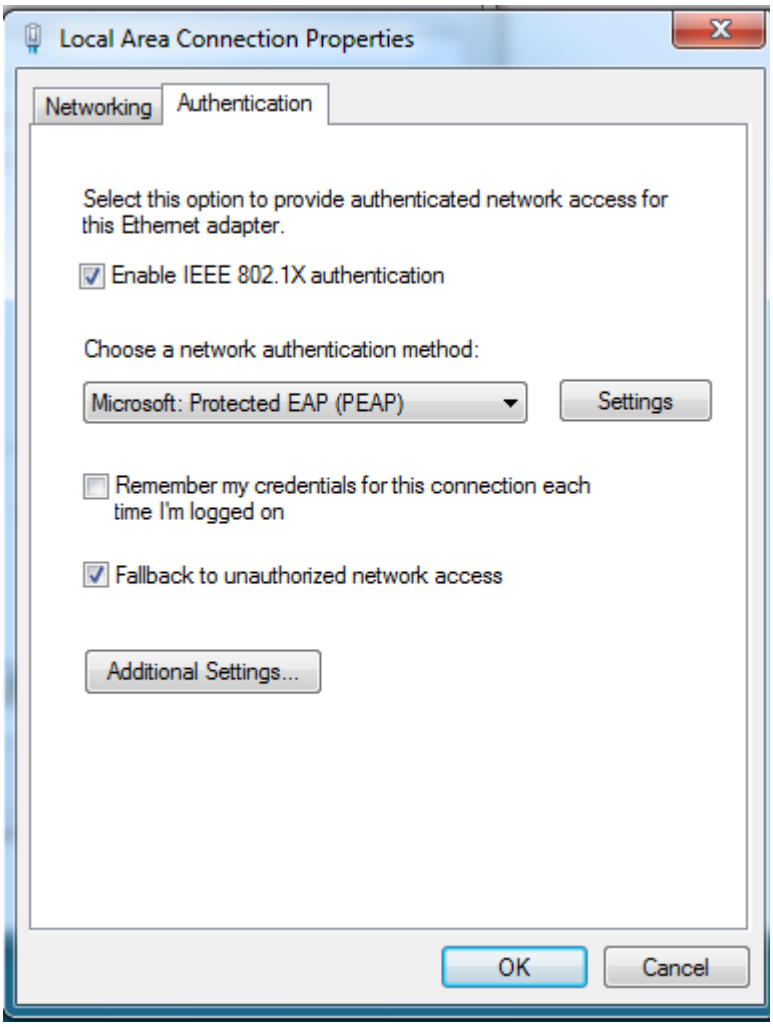
- Click **Additional Settings**, select **Specify authentication mode** and select **Computer authentication** from the list



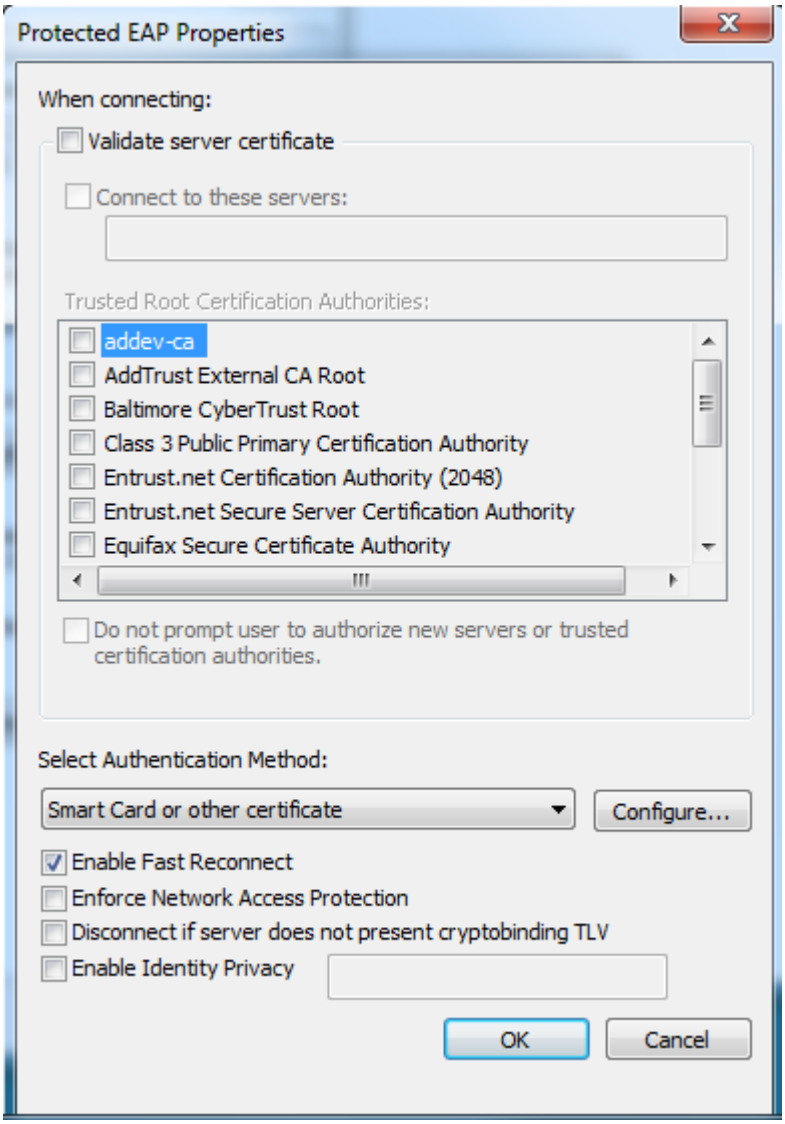
- Click **OK**

Configure Windows 7 client computers for 802.1x authentication via Network and Sharing Center for PEAP-EAP-TLS

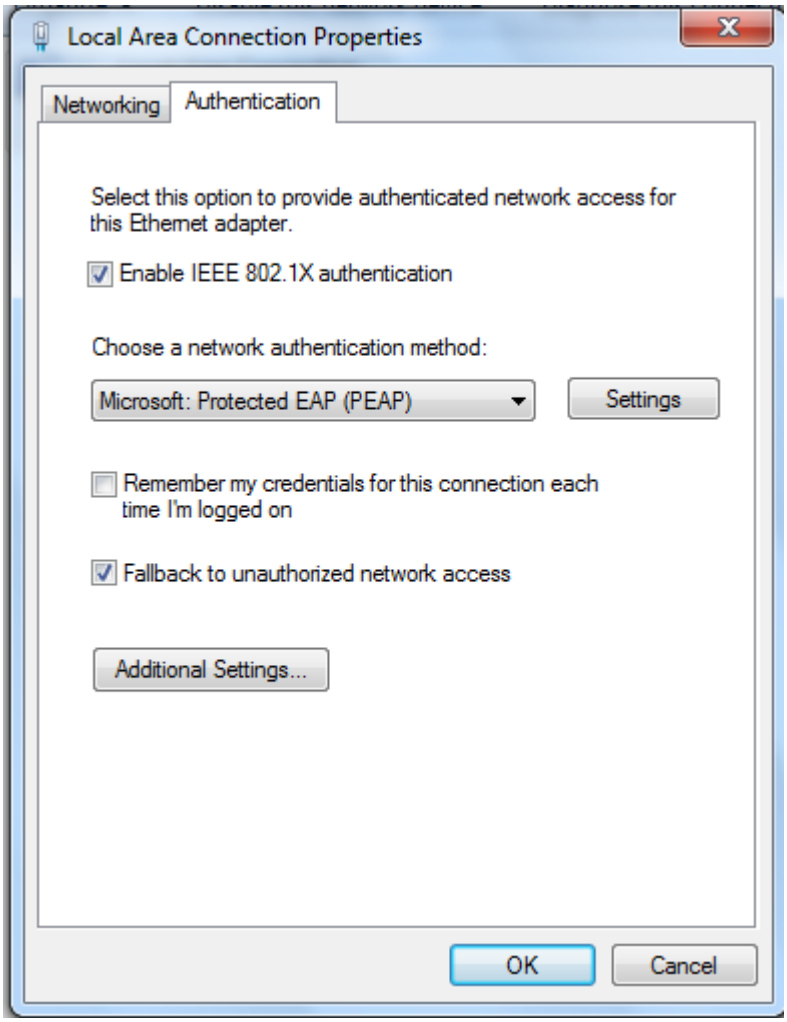
- Open **Network and sharing Center**, and select **Change adapter settings**
- Right click on **Local Area Connection** and select **Properties**
- Select **Authentication** tab and select **Enable IEEE 802.1X authentication**
- On the **Choose a network authentication method** list box, select **Microsoft: Protected EAP (PEAP)** and click **Settings**



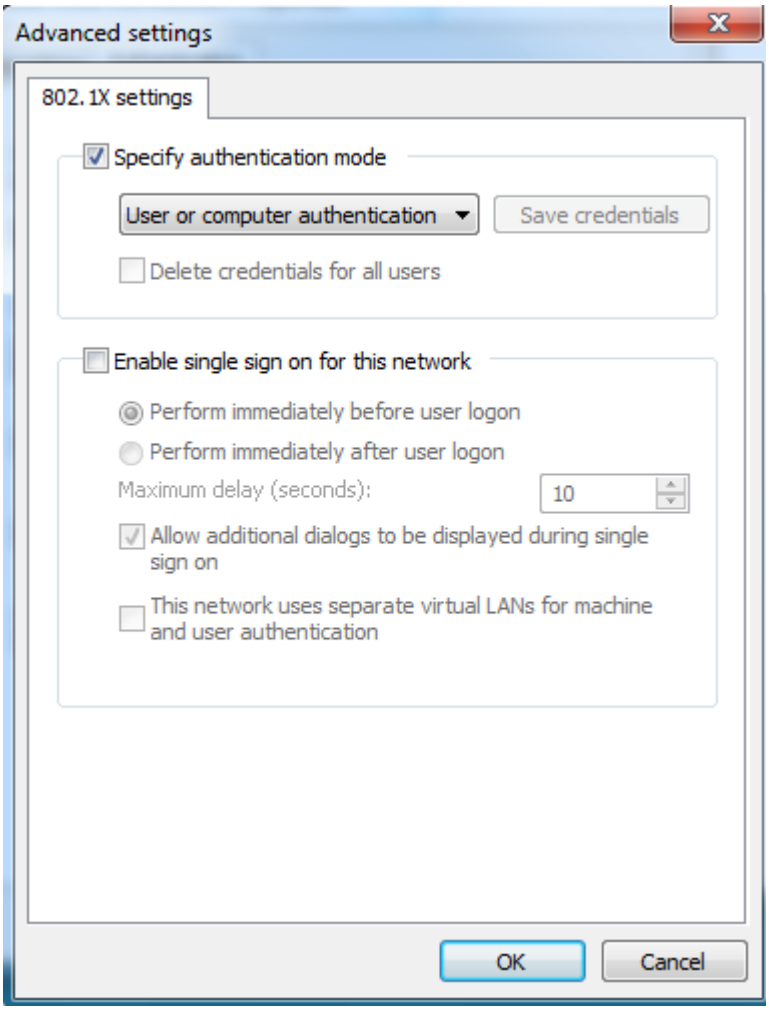
- From the **Select Authentication Method** list box, select **Smart Card or other certificate** and click **OK**



- Clear **Remember my credentials for this connection each time I'm logged on** and enable **Fallback to unauthorized network access**



- Click **Additional Settings**, select **Specify authentication mode** and select **User or Computer authentication** from the list



- Click **OK**

Configuring Catalyst 3560 for 802.1x authentication Task List

The next step is to configure the switch to support port-based authentication.

- Enabling 802.1x authentication on the switch
- Configuring switch-to-RADIUS server communication
- Configure Guest VLAN
- Configure Restricted VLAN
- Enabling periodic re-authentication
- Display statistics and status

Configuring 802.1x authentication on the switch

```
addevsw01#config t
addevsw01(config)#aaa new-model
addevsw01(config)#aaa authentication dot1x default group radius
```

```
addevsw01(config)#aaa authorization network default group radius
addevsw01(config)#dot1x system-auth-control
addevsw01(config)#interface fa 0/2
addevsw01(config-if)#switchport mode access
addevsw01(config-if)#authentication port-control auto
```

Configuring switch-to-RADIUS server communication

```
addevsw01(config)#radius-server host 10.32.5.15 auth-port 1812
acct-port 1813 key accessdenied
```

Configure Guest VLAN

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event no-response action
authorize vlan 100
```

Configure Restricted VLAN

```
addevsw01(config)#interface fa0/2
addevsw01(config-if)#authentication event fail action authorize
vlan 99
```

Enabling periodic re-authentication

```
addevsw01(config)#int fa 0/2
addevsw01(config-if)#authentication periodic
addevsw01(config-if)#authentication timer reauthenticate 4800
```

Display Statistics and Status

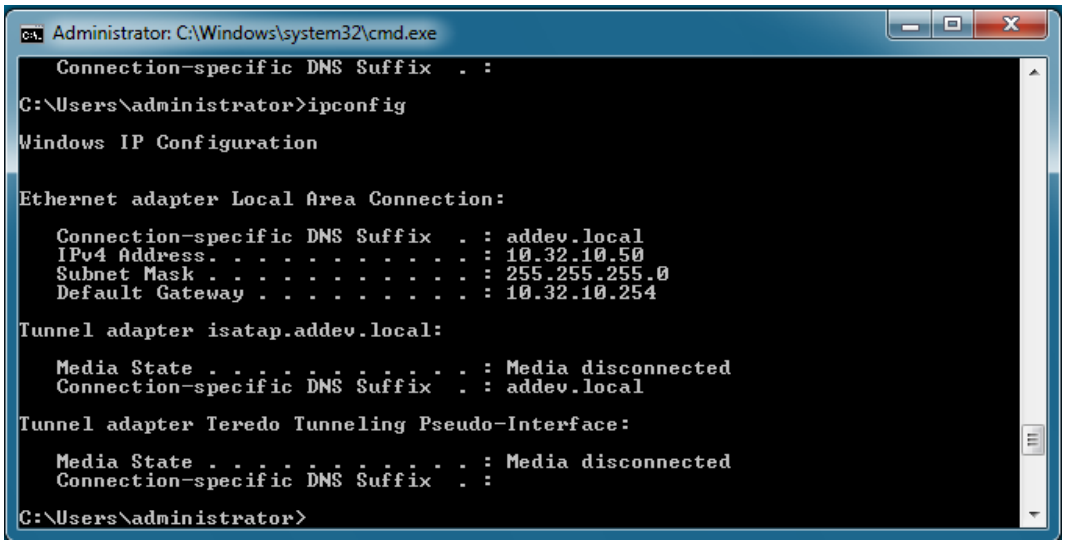
```
addevsw01#show dot1x int fa 0/2
```

How to test

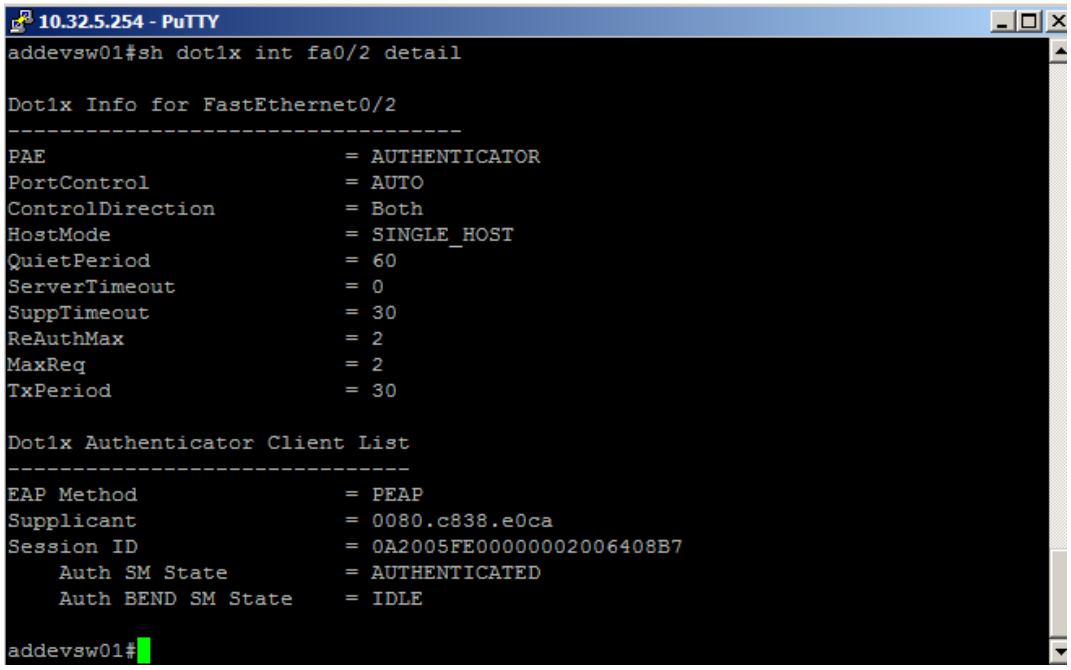
Power-on your Windows 7 client computer and configure the correct authentication method. When restart your Windows 7 client, the client sends an authentication request. If authentication is successful, the client computer receives an IP address from your DHCP server. If the client computer is a member of Wired Computers VLAN 10, the client receives an IP address from the network range 10.32.10.50-60.

If authentication fails, the client becomes a member of VLAN 99 and receives an IP address in the range of 10.32.99.50-60

If the client computer is successfully authenticated, you receive an IP address from VLAN 10



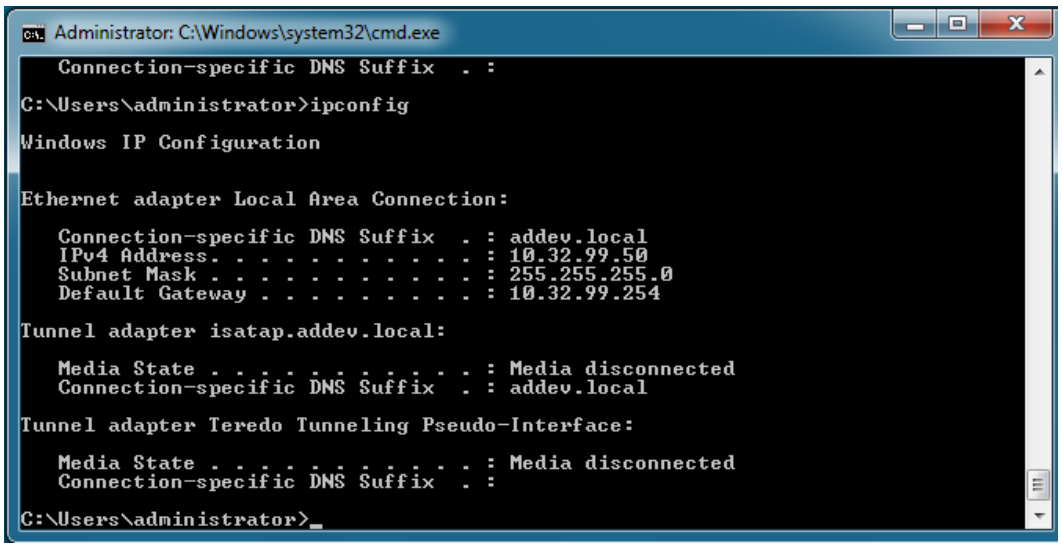
After authorization, you receive following message for PEAP-EAP-TLS authentication:



VLAN database

```
addevsw01#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Gi0/1
5    native-vlan                       active    Fa0/1
10   VLAN0010                          active    Fa0/2
99   VLAN0099                          active
100  VLAN0100                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

addevsw01#
```

If the client computer fails authentication, you receive an IP address from VLAN 99



If the authentication method is not compatible, the client becomes a member of the authentication fail VLAN

```
*Mar  1 02:10:12.453: %AUTHMGR-5-START: Starting 'dot1x' for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionID 0A2005F
E0000000300764D22
*Mar  1 02:10:16.966: %DOT1X-5-FAIL: Authentication failed for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionID 0A200
5FE0000000300764D22
*Mar  1 02:10:16.966: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (0080.c838.e0ca) on Interface Fa
0/2 AuditSessionID 0A2005FE0000000300764D22
*Mar  1 02:10:19.231: %DOT1X-5-FAIL: Authentication failed for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionID 0A200
5FE0000000300764D22
*Mar  1 02:10:19.231: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (0080.c838.e0ca) on Interface Fa
0/2 AuditSessionID 0A2005FE0000000300764D22
*Mar  1 02:11:51.849: %DOT1X-5-FAIL: Authentication failed for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionID 0A200
5FE0000000300764D22
*Mar  1 02:11:51.849: %AUTHMGR-7-RESULT: Authentication result 'timeout' from 'dot1x' for client (0080.c838.e0ca) on Interface
 Fa0/2 AuditSessionID 0A2005FE0000000300764D22
*Mar  1 02:11:51.849: %AUTHMGR-5-VLANASSIGN: VLAN 99 assigned to Interface Fa0/2 AuditSessionID 0A2005FE0000000300764D22
*Mar  1 02:11:52.864: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
*Mar  1 02:11:52.889: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (0080.c838.e0ca) on Interface Fa0/2 AuditSessionI
D 0A2005FE0000000300764D22
*Mar  1 02:11:52.889: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client (0080.c838.e0ca) on Interface Fa0/
2 AuditSessionID 0A2005FE0000000300764D22
*Mar  1 02:12:21.872: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
addevsw01#
```

Per User ACL

```
addevsw01#sh access-lists
Extended IP access list 101
    10 deny tcp any host 10.32.5.3 eq www
    20 permit ip any any
Extended IP access list Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348
    20 permit udp any any range bootps 65347
    30 deny ip any any
Extended IP access list FastEthernet0/2#IP2 (per-user)
    10 deny tcp any host 10.32.5.3 eq www
    20 permit ip any any (8 matches)
addevsw01#
```

Appendix A: Security Groups

Group	Description
Autoenroll Server Authentication Certificate	Members of this group receive a certificate with the purpose of server authentication
Autoenroll Client Authentication Certificate	Members of this group receive a certificate with the purpose of client authentication
Wired Computers VLAN 10	Members of this group are placed into VLAN 10
Wired Computers VLAN 20	Members of this group are placed into VLAN 20

Appendix B: Switch Configuration

```
sh run
Building configuration...

Current configuration : 3581 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname addevsw01
!
boot-start-marker
boot-end-marker
!
!
!
username cisco password 0 cisco
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
!
!
!
aaa session-id common
system mtu routing 1500
ip routing
ip domain-name addev.local
!
!
!
!
!
crypto pki trustpoint TP-self-signed-1081864448
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1081864448
 revocation-check none
 rsakeypair TP-self-signed-1081864448
!
!
crypto pki certificate chain TP-self-signed-1081864448
 certificate self-signed 01
  3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31303831 38363434 3438301E 170D3933 30333031 30303031
  30315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 30383138
  36343434 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100BF82 23C594F7 C1F04979 E31E819E CFA7B323 F1D827C3 64211110 15FD804F
  9DC25434 E0E63342 95253F16 5A721C51 EAA30216 8B8320A7 C7573A55 684B9F77
  42CB097A 3F8C2A13 21B0C676 51C7B00C C5D781EF 03AA038E BC3E8946 7AE41C17
  9F3A6698 2921AE8F D2C84E5F 8D436AEC 8046208A DB718804 5061306E 921D0A44
  4D0F0203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603
  551D1104 19301782 15616464 65767377 30312E61 64646576 2E6C6F63 616C301F
```

```
  0603551D 23041830 1680149F 143D56F9 389C6F81 F05B0DAE 8B693799 98893530
  1D060355 1D0E0416 04149F14 3D56F938 9C6F81F0 5B0DAE8B 69379998 8935300D
  06092A86 4886F70D 01010405 00038181 00851ACE F2C9718D 5DBA2B67 DF48378D
  704D9DCD 2D6D49FF F3321FA1 42901F2A CFD3B18D 13064E95 B116D74C E943DA73
  53741A11 5FC49F57 4D566F5E A838163D 6408D122 F3A8FE7F D99F6422 AA67F077
  25E8D40D 54915FEA 16309073 79A433C7 B45C2E08 B30198F3 83784498 0788ACFD
  1F67D8B0 C537D680 744EAFD0 FBF60449 AD
      quit
dot1x system-auth-control
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
!
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/2
 switchport mode access
 authentication event fail action authorize vlan 99
 authentication event no-response action authorize vlan 100
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate 60
 dot1x pae authenticator
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface GigabitEthernet0/1
!
interface Vlan1
 no ip address
!
interface Vlan5
 ip address 10.32.5.254 255.255.255.0
!
interface Vlan10
 ip address 10.32.10.254 255.255.255.0
 ip helper-address 10.32.5.15
!
```

```
interface Vlan99
 ip address 10.32.99.254 255.255.255.0
 ip helper-address 10.32.5.15
!
interface Vlan100
 ip address 10.32.100.254 255.255.255.0
 ip helper-address 10.32.5.15
!
ip http server
ip http secure-server
!
!
!
logging esm config
access-list 101 deny   tcp any host 10.32.5.3 eq www
access-list 101 permit ip any any
!
!
radius server addevdc01
 address ipv4 10.32.5.15 auth-port 1812 acct-port 1813
 key accessdenied
!
!
!
!
line con 0
line vty 0 4
 password cisco
 transport input ssh
line vty 5 15
 password cisco
 transport input ssh
!
end

addevsw01#
```