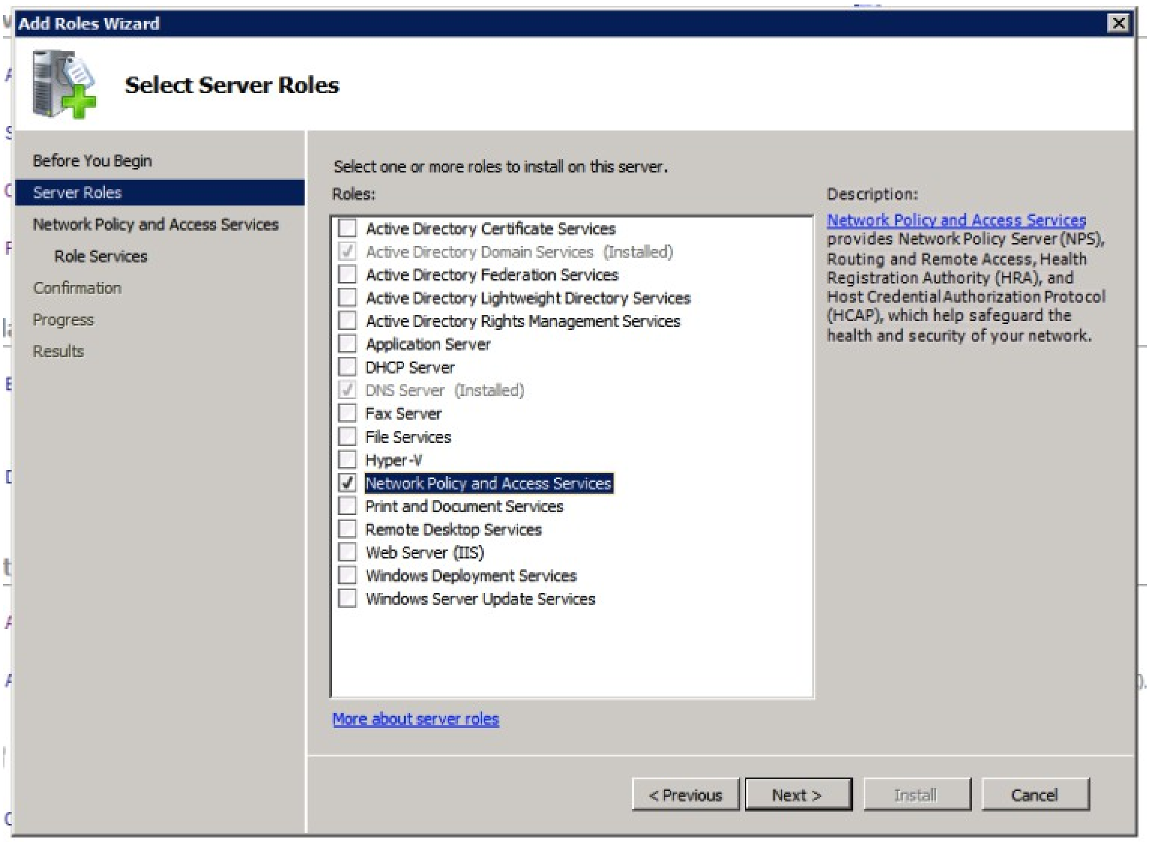
Running eduroam on NPS with Windows 2008 R2 Enterprise

The network policy server is the RADIUS server as part of Windows server editions. These instructions assume a basic setup of an Active Directory.

Installation of NPS

In the “initial configuration” or “Server Manager” look for “Roles” and click “Add Roles”.



Select one or more roles to install on this server.

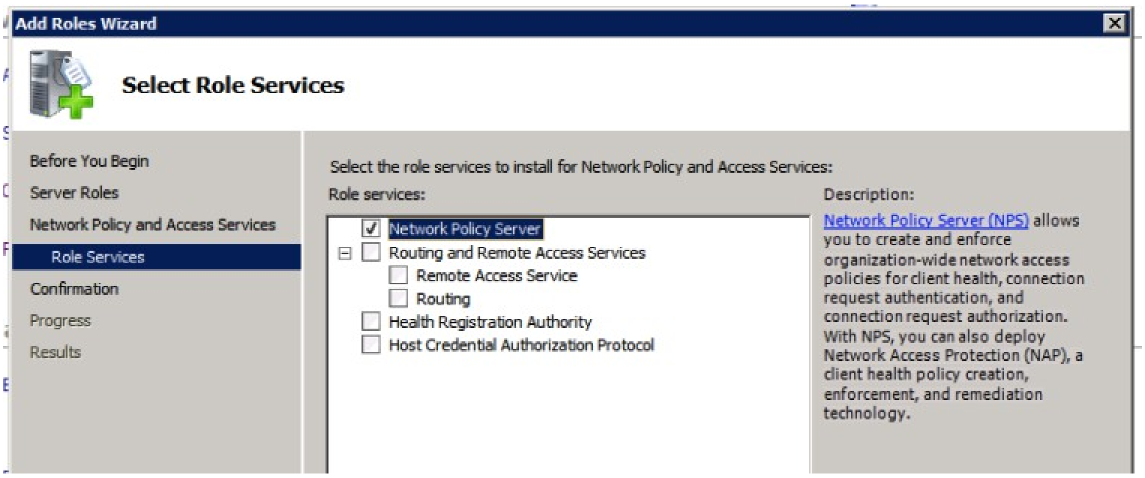
Roles:

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

Description:

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

Select the “Network Policy and Access Services” option and click “Next >”. After reading the introduction to NPS, continue to the role services to install:



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

Role services:

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

Description:

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

Select only the “Network Policy Server” component, and click “Next >” again.

You will see a summary of the installer-actions, and need to click “Install” to continue. Wait for the installation to finish, and click “Close”.

You can now find the “Network Policy Server” under the “Administrative Tools” in the start menu, in the Server Manager, or as a snap-in to mmc.

Server certificate for NPS

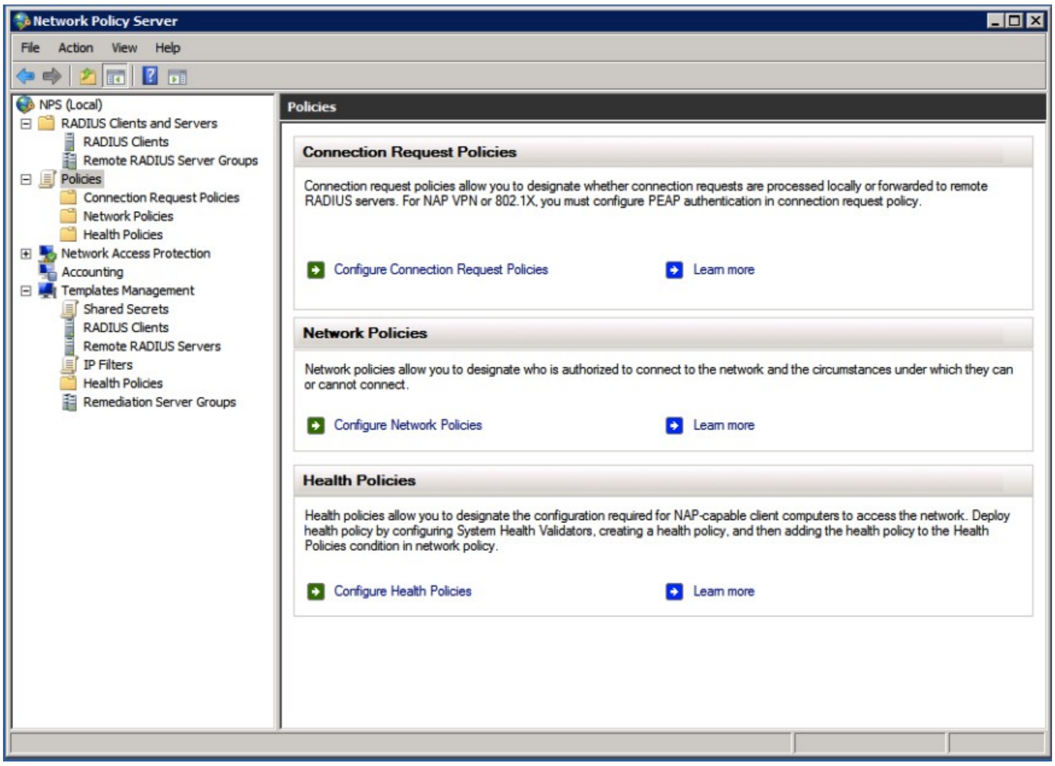
You need to have a server certificate in order to use PEAP-authentication with eduroam. PEAP sets up a secure tunnel (just like HTTPS does for websites) in order to protect the credentials, and is an important part of the mutual authentication: both the user needs to prove who he is, and the authentication server needs to prove to the user that he or she is providing credentials to the right authority.

Without certificate (self signed or not) it's not possible to do local authentication. NPS can still be used as a proxy to receive requests from Access Points, log, filter, and forward to the eduroam infrastructure.

If you have no certificate installed (or in doubt about your certificate), read Appendix A about Certificates.

Configuration of NPS

The NPS console (snap-in) allows you do use a Wizard for 802.1X / secure wireless. While you can use this for eduroam, it doesn't provide all the required settings (like realm/user-name pattern-matching), so you need to make some more changes in the created policies anyway. In these instructions, we'll create the policies directly from the “Connection Request Policies” and the “Network Policies”.



Connection Request Policies

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.

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.

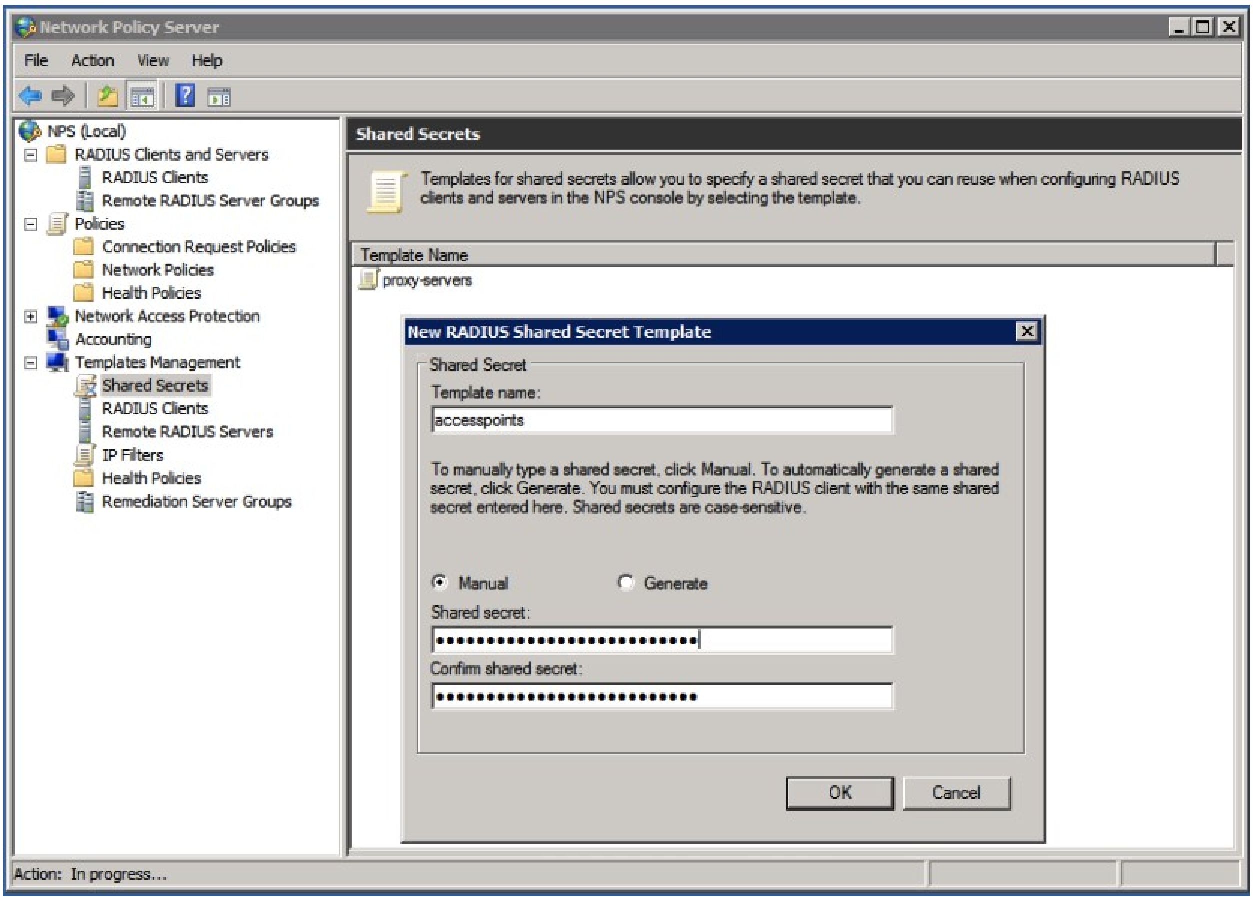
Health Policies

Health policies allow you to designate the configuration required for NAP-capable client computers to access the network. Deploy health policy by configuring System Health Validators, creating a health policy, and then adding the health policy to the Health Policies condition in network policy.

Before any policy can be applied to authentication requests, we need to create “RADIUS clients” in order to allow both your Access Points (and/or Switches) and the eduroam infrastructure to actually send requests to your server (that's also a client).

To prevent typo's between multiple peers and allow easier changes, it's preferable to create a shared secret template for peers using the same shared secret. You can for instance create one for your accesspoints and one for the proxy-servers. The proxy-server secret you need to negotiate with your national eduroam roaming-operator. The access-point secret, you configure on your own access-points so you can make something up there yourself.

You can create these templates in the “Template Management” and “Shared Secrets” section, by right-clicking and selecting “New”...



Templates for shared secrets allow you to specify a shared secret that you can reuse when configuring RADIUS clients and servers in the NPS console by selecting the template.

proxy-servers

New RADIUS Shared Secret Template

Shared Secret

Template name: accesspoints

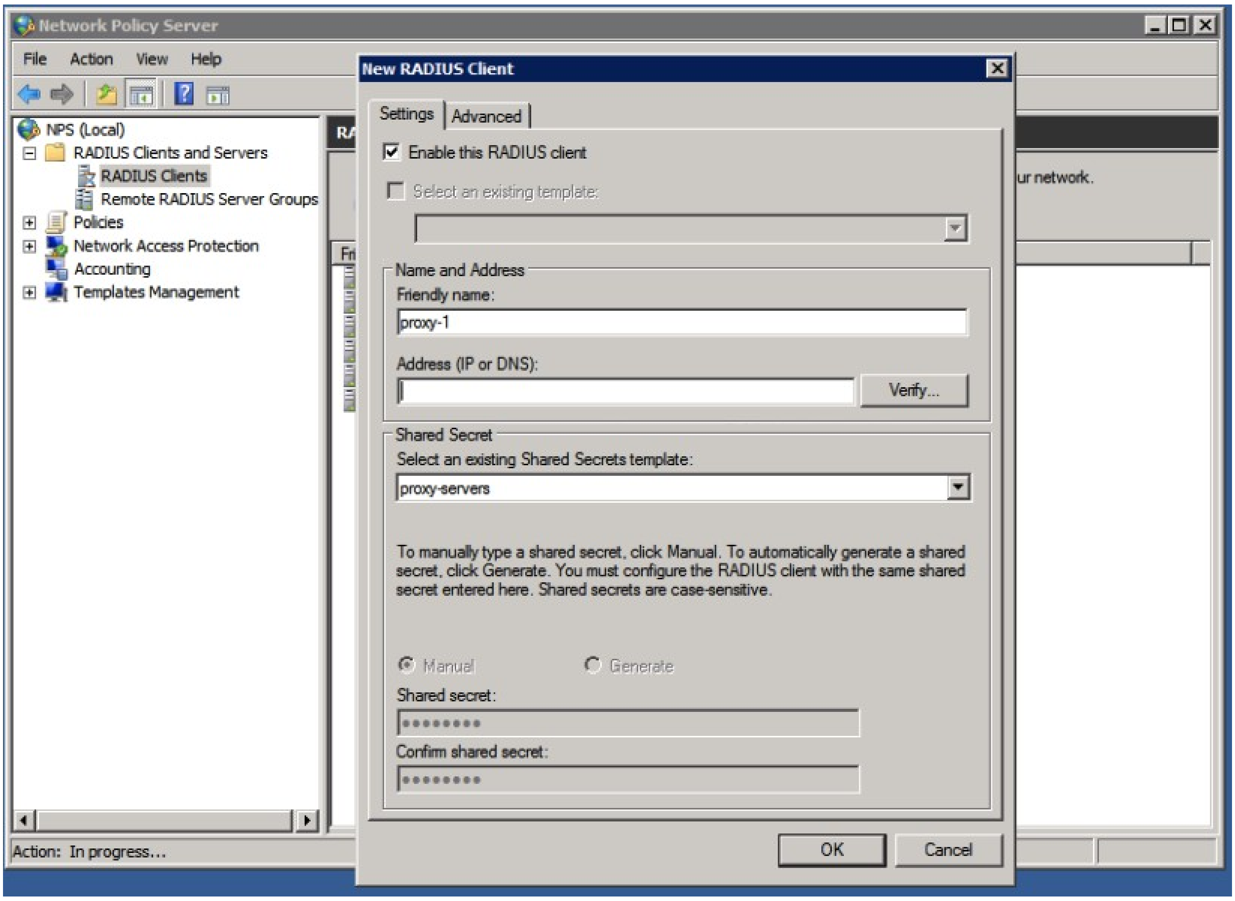
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••••••••

After creating the template, create clients for your access-points and proxy-servers, by right-clicking “RADIUS clients” (under RADIUS Clients and Servers) and “New”:



New RADIUS Client

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: proxy-1

Address (IP or DNS):

Shared Secret

Select an existing Shared Secrets template: proxy-servers

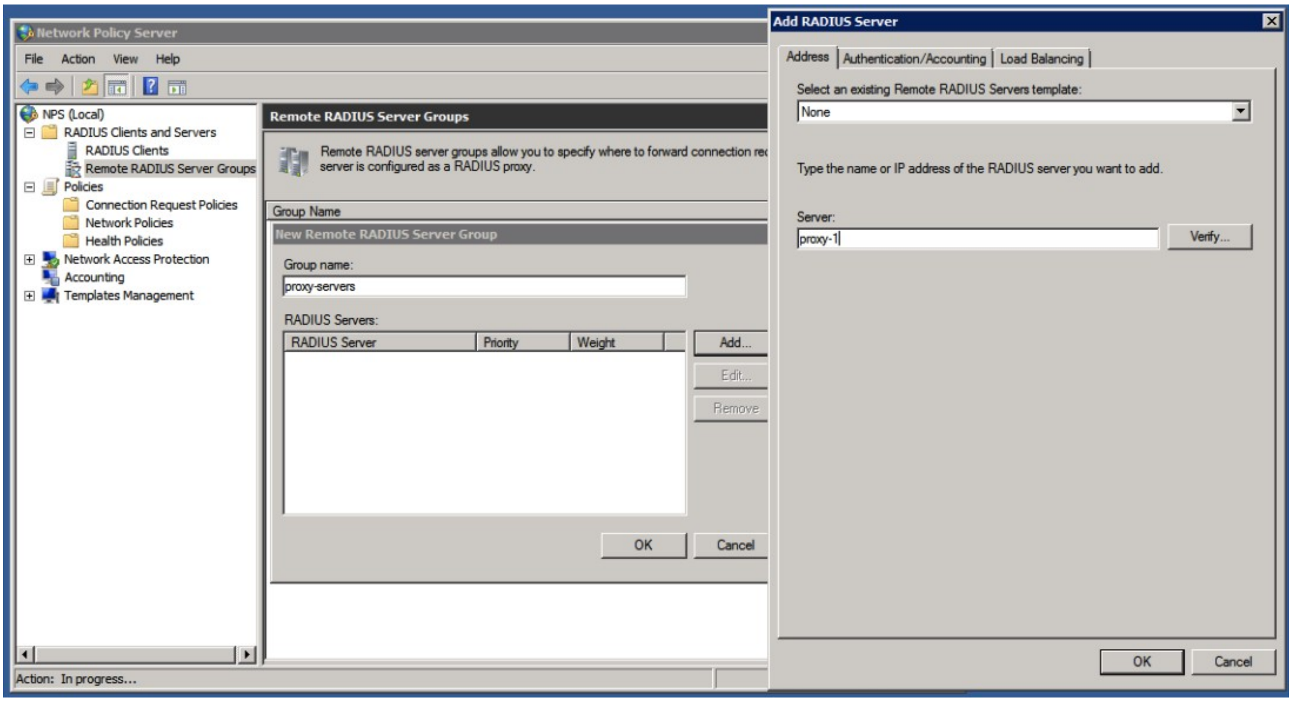
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••

Now, we create a server group for the proxy-servers, that will be used to send authentication requests to for non-local users. In the “RADIUS Clients and Servers” right-click “Remote RADIUS Server Groups” and “New”...


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
Add... Edit... Remove OK Cancel
Address Authentication/Accounting Load Balancing
Verify...

Remote RADIUS Server Groups

Remote RADIUS server groups allow you to specify where to forward connection re server is configured as a RADIUS proxy.

New Remote RADIUS Server Group

Group name: proxy-servers

RADIUS Servers:

RADIUS Server	Priority	Weight

Add RADIUS Server

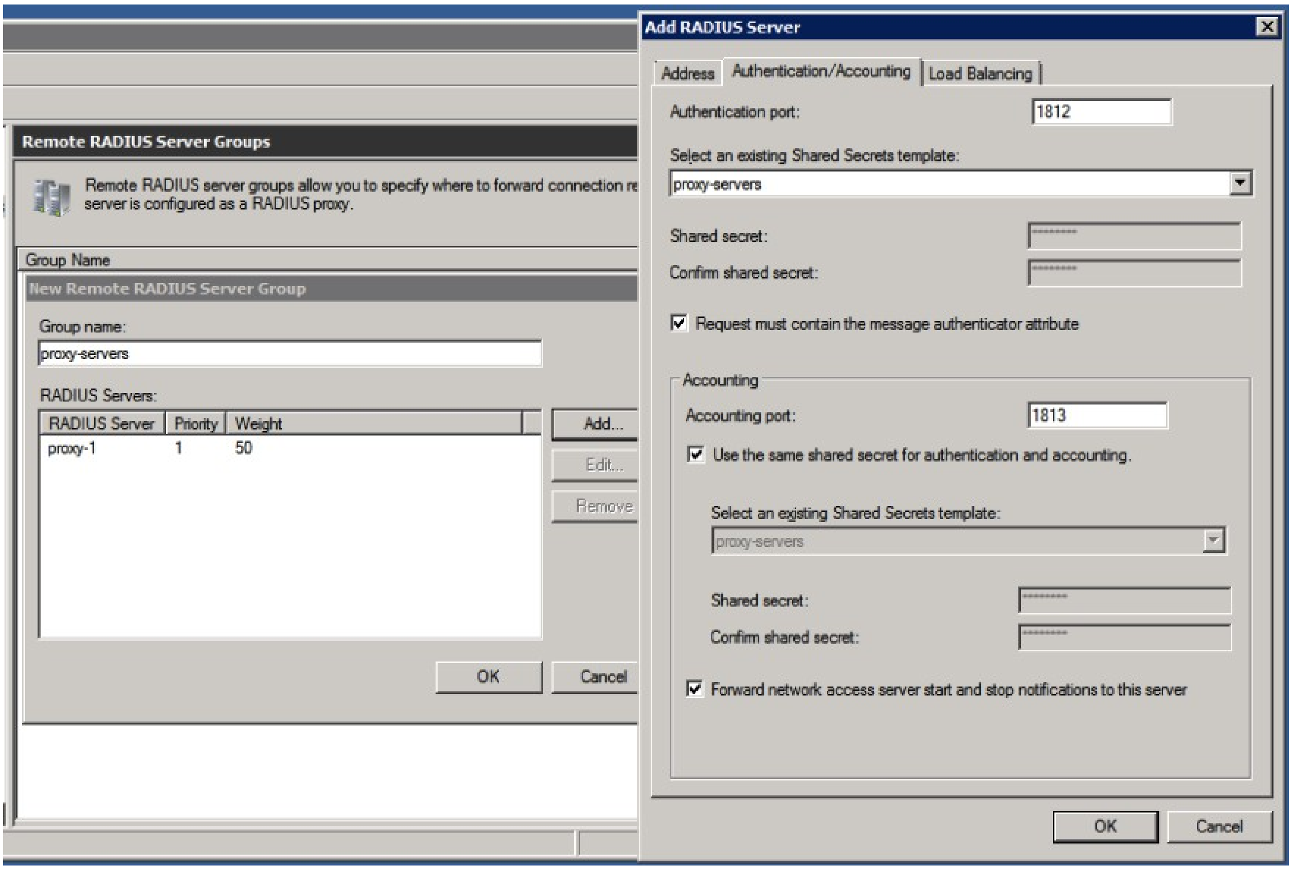
Select an existing Remote RADIUS Servers template: None

Type the name or IP address of the RADIUS server you want to add.

Server: proxy-1

Action: In progress...

Enter a name for your server group, such as “proxy-servers”, and click “Add...” to add one or more of the servers. Enter the proper name (proxy-1 in the example is not a proper name ;-) but you will get these details from your National Roaming Operator (NRO)), and proceed to the Authentication/Accounting tab for the shared secret settings:


Add... Edit... Remove OK Cancel
Address Authentication/Accounting Load Balancing

Remote RADIUS Server Groups

Remote RADIUS server groups allow you to specify where to forward connection re server is configured as a RADIUS proxy.

New Remote RADIUS Server Group

Group name: proxy-servers

RADIUS Servers:

RADIUS Server	Priority	Weight
proxy-1	1	50

Add RADIUS Server

Authentication port: 1812

Select an existing Shared Secrets template: proxy-servers

Shared secret: *********

Confirm shared secret: *********

☑ Request must contain the message authenticator attribute

Accounting

Accounting port: 1813

☑ Use the same shared secret for authentication and accounting.

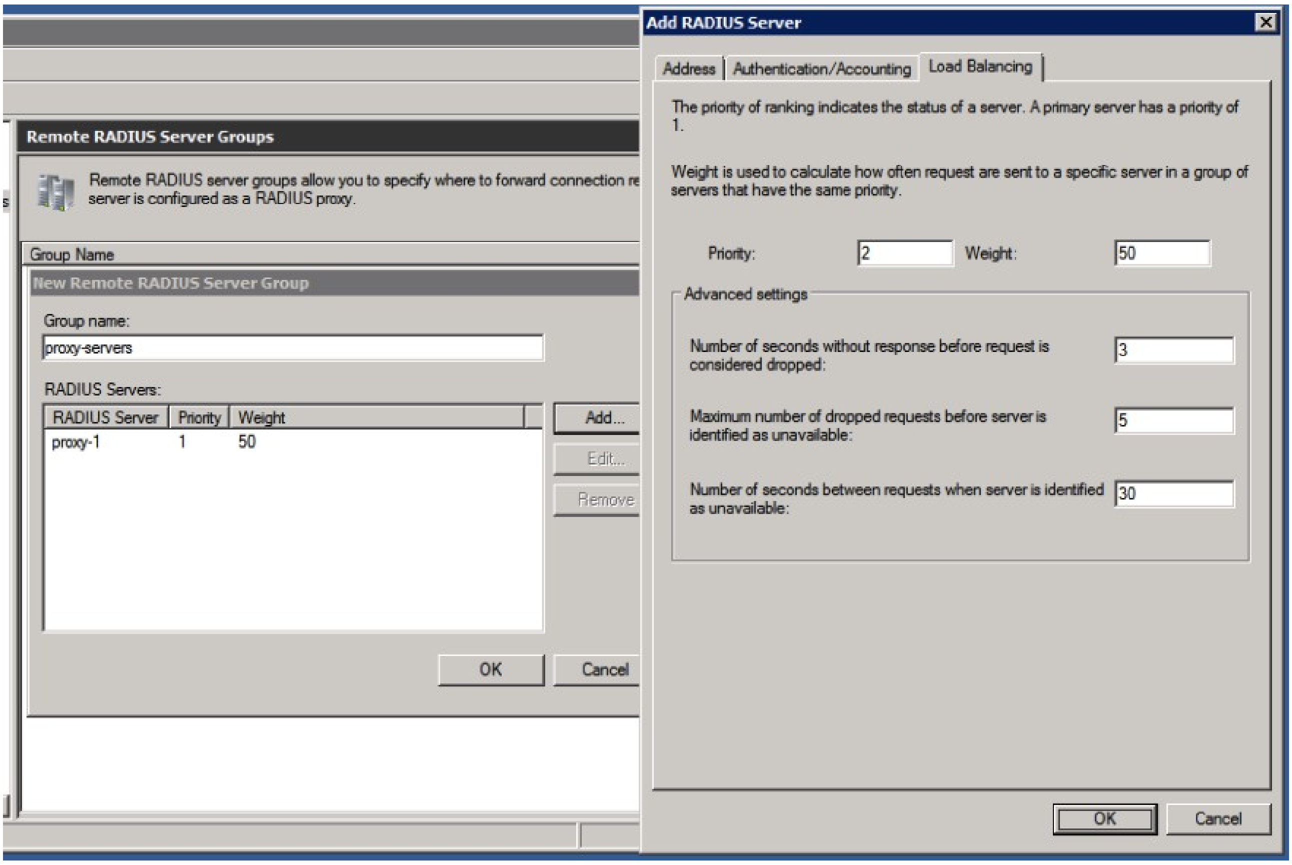
Select an existing Shared Secrets template: proxy-servers

Shared secret: *********

Confirm shared secret: *********

☑ Forward network access server start and stop notifications to this server

For a secondary server, consider the last tab “Load Balancing”. It's recommended not to load-balance single EAP-sessions across multiple servers, which is what NPS will do when the Load-Balancing Priority is all set to the same level. In many situations it just works, but there's no guarantee, so better set it to a lower priority so it's only used for failover. If in doubt, ask your National Roaming Operator for advise.



Remote RADIUS Server Groups

Remote RADIUS server groups allow you to specify where to forward connection re
server is configured as a RADIUS proxy.

Group Name

New Remote RADIUS Server Group

Group name: proxy-servers

RADIUS Servers:

RADIUS Server	Priority	Weight
proxy-1	1	50

Add RADIUS Server

The priority of ranking indicates the status of a server. A primary server has a priority of 1.

Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority.

Priority: 2 Weight: 50

Advanced settings

Number of seconds without response before request is considered dropped: 3

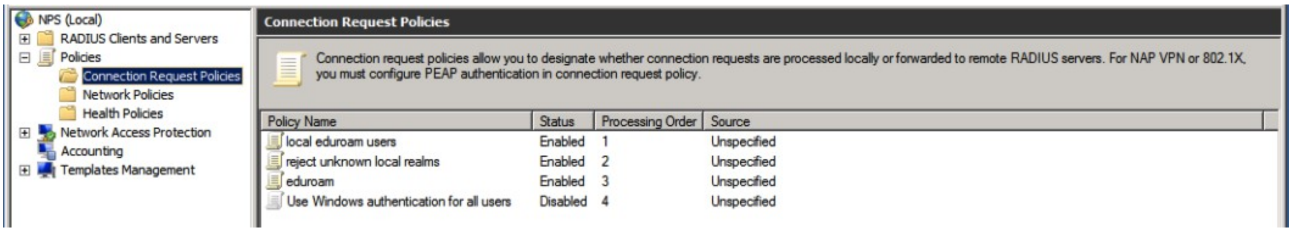
Maximum number of dropped requests before server is identified as unavailable: 5

Number of seconds between requests when server is identified as unavailable: 30

The “Connection Request Policy” is there to decide what to do with an authentication request: forward it to a proxy-server, or authenticate locally. The decision is based on RADIUS attributes, such as the User-Name, but this can also be a RADIUS client IP-address or friendly-name for instance.

The order or Connection Request Policies is important. You can move policy-rules up and down, and also temporarily disable a rule.

A typical order is as follows:



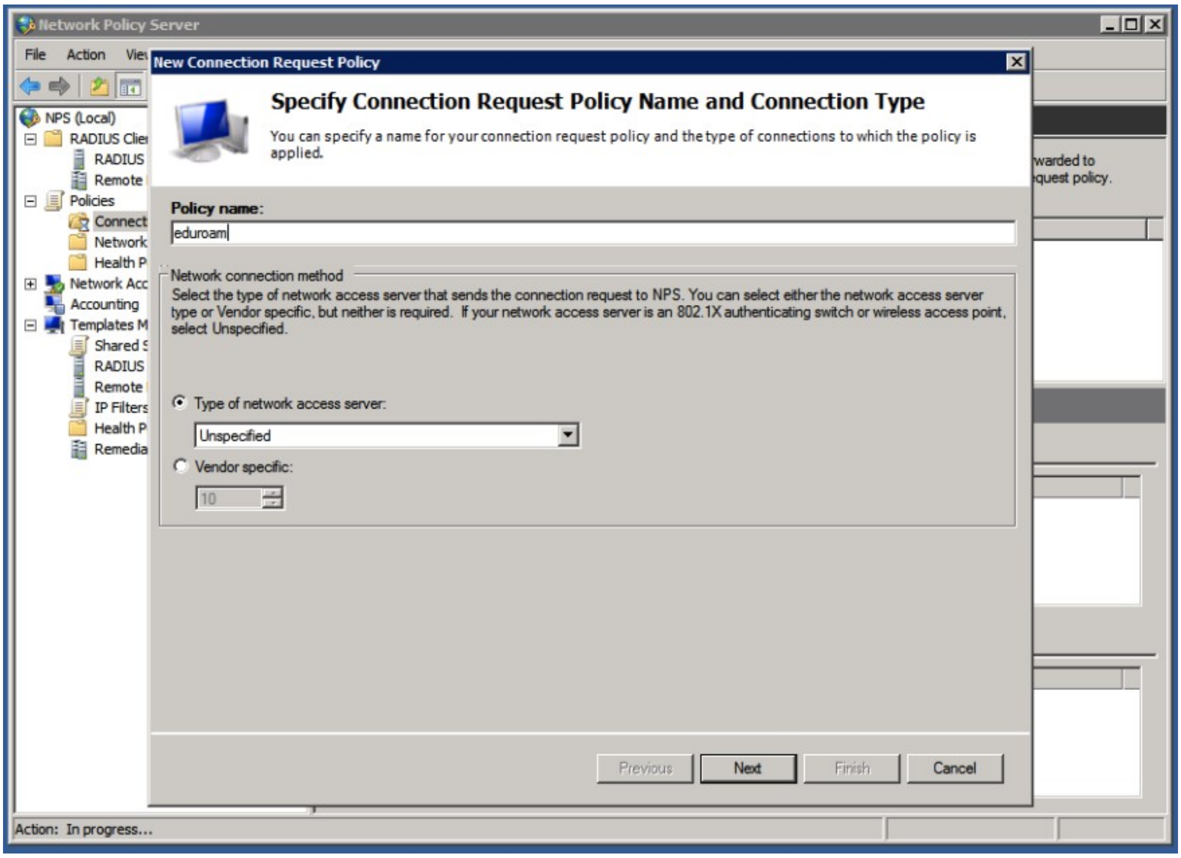
Connection Request Policies

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

Policy Name	Status	Processing Order	Source
local eduroam users	Enabled	1	Unspecified
reject unknown local realms	Enabled	2	Unspecified
eduroam	Enabled	3	Unspecified
Use Windows authentication for all users	Disabled	4	Unspecified

1. authenticate local users @your-realm.tld
   (you can add more for eg. @student.your-realm.tld)
2. authenticate mis-matches in your-realm, such as non-existant.your-realm.tld
3. forward to remote proxy-servers

First, create a connection to the proxy-servers by right-clicking the “Connection Request Policies” and “New”.



New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

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

Policy name: eduroam

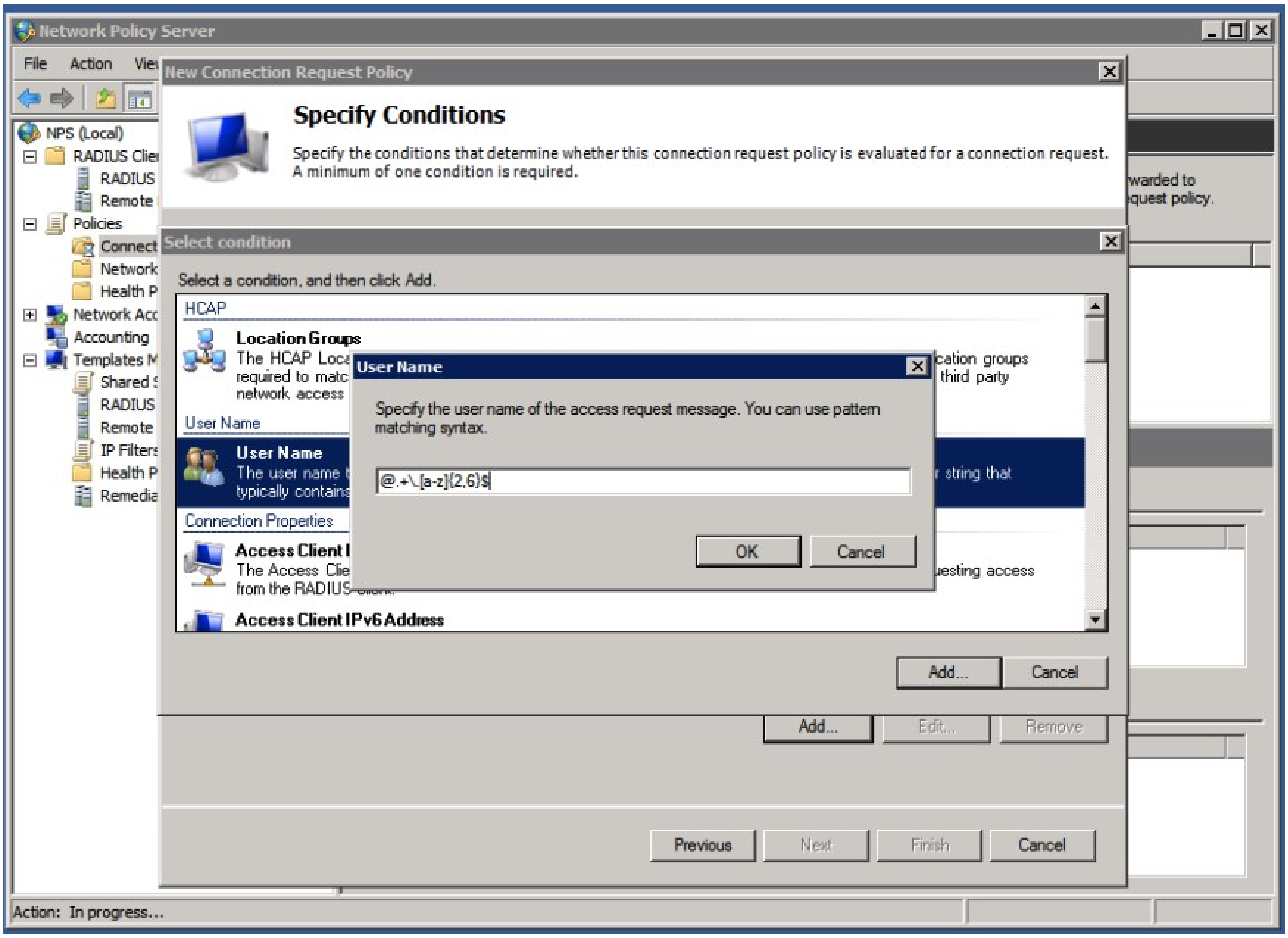
Network connection method

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

Give the policy a name (such as “eduroam”), and click “Next”. Now conditions for matching this policy have to be specified. This rule will be based on User-Name matching.



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.

Select condition

Select a condition, and then click Add.

HCAP

Location Groups
The HCAP Loca... location groups required to matc... third party network access...

User Name

User Name
The user name t... string that typically contains...

Connection Properties

Access Client I...
The Access Clie... requesting access from the RADIUS client.

Access Client IPv6 Address

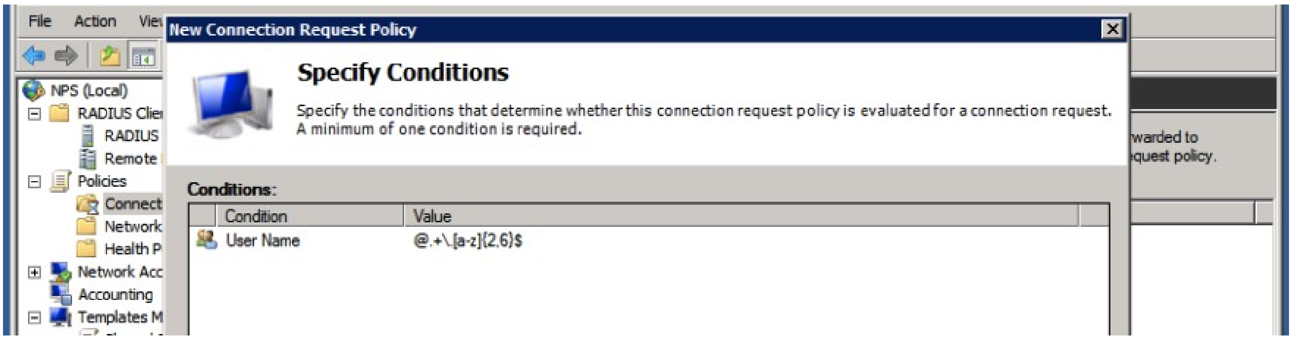
User Name

Specify the user name of the access request message. You can use pattern matching syntax.

@.+\.[a-z]{2,6}$

We use a regular expression here to match user-names that look valid. User-names in eduroam are like the e-mail addresses, and end on something.tld – that means we shouldn't forward realms that have no dot “.” in them, or when there's no realm (after the @-sign, the domain is realm in RADIUS-slang) at all.

The regular expression @.+\.[a-z]{2,6}$ is a case-insensitive match for realms ending on something dot tld between 2 and 6 letters. Keep in mind that this might change in the future when internationalized top-level domains are allowed, then this regular expression might need to be updated. A more lenient regexp would be @.+\..+$ to allow a realm with something dot something as a minimum. Both regexps handle any number of sub-realms.



New Connection Request Policy

Specify Conditions

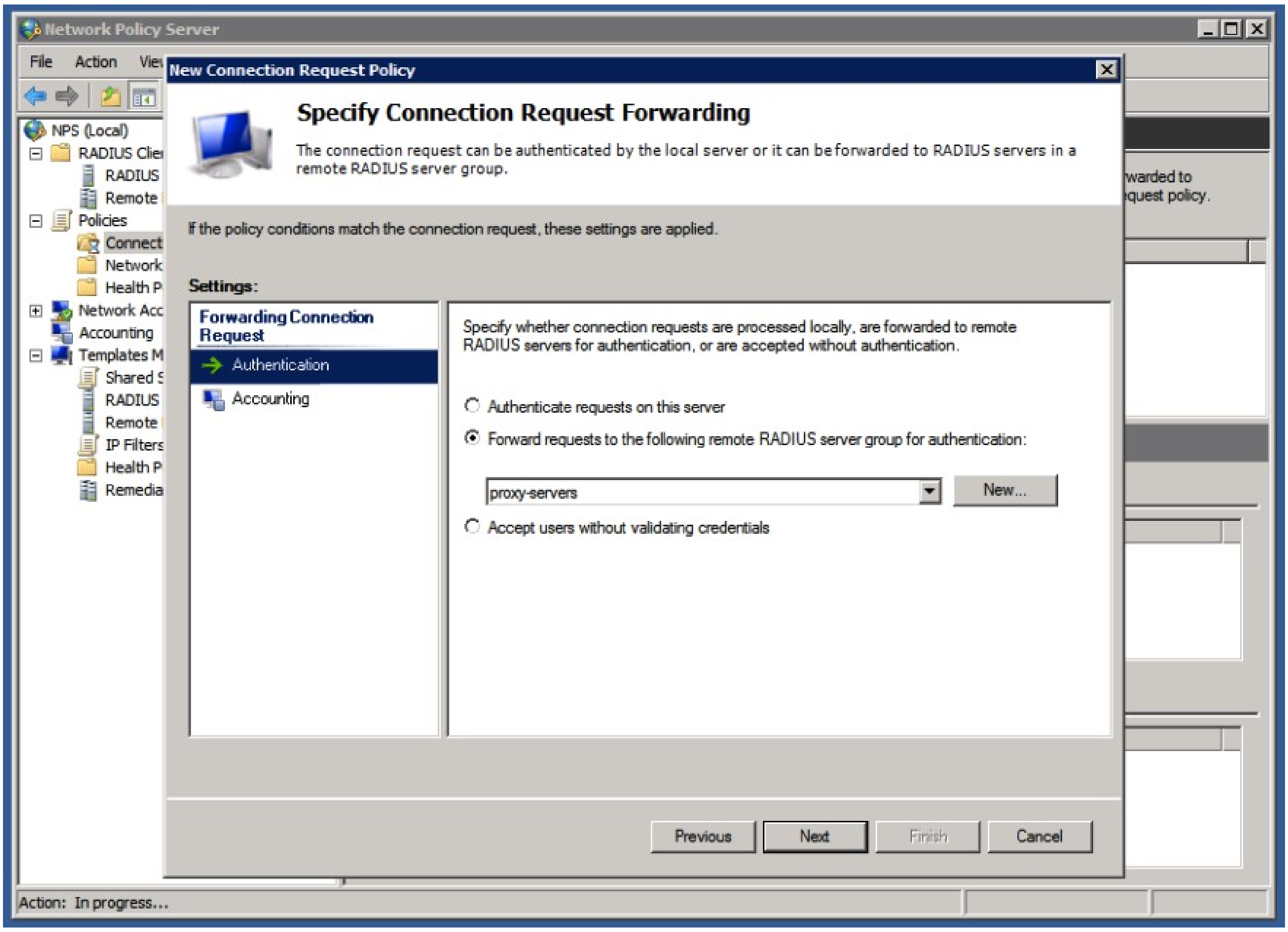
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
User Name	@.+\.[a-z]{2,6}$

After the condition is set, click “Next”. (Note that the default Wizard also adds a condition for NAS Port Type, and sets this to “Wireless – IEEE 802.11”. This is fine if your Access Points add this and if you need to do that kind of filtering of RADIUS requests. You could add “Wired”, as some AP's seem to be non-compliant and add this.)

Next, specify what to do with the requests that match the condition. In this case, we want to forward the request to the proxy-servers, so the RADIUS server group needs to be selected:



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.

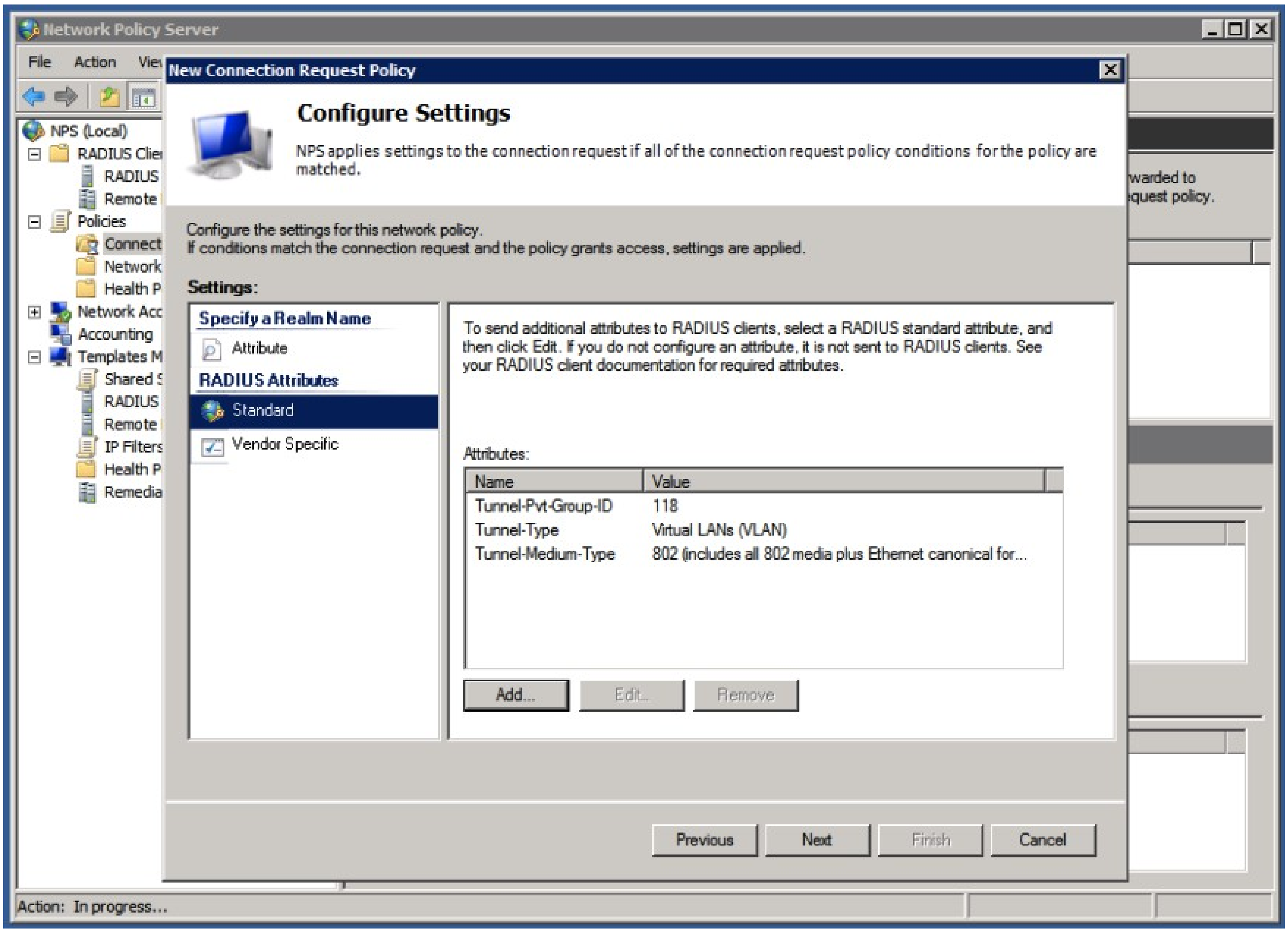
○ Authenticate requests on this server

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

proxy-servers

○ Accept users without validating credentials

The final configuration options for a Connection Request Policy allows you to add RADIUS attributes to the RADIUS reply. You don't need to do anything with this, but you can define or override VLAN attributes if your Access Point is configured to use VLANs. This way you can define a different VLAN for guests compared to local users. (More about VLANs for local-users later.)



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

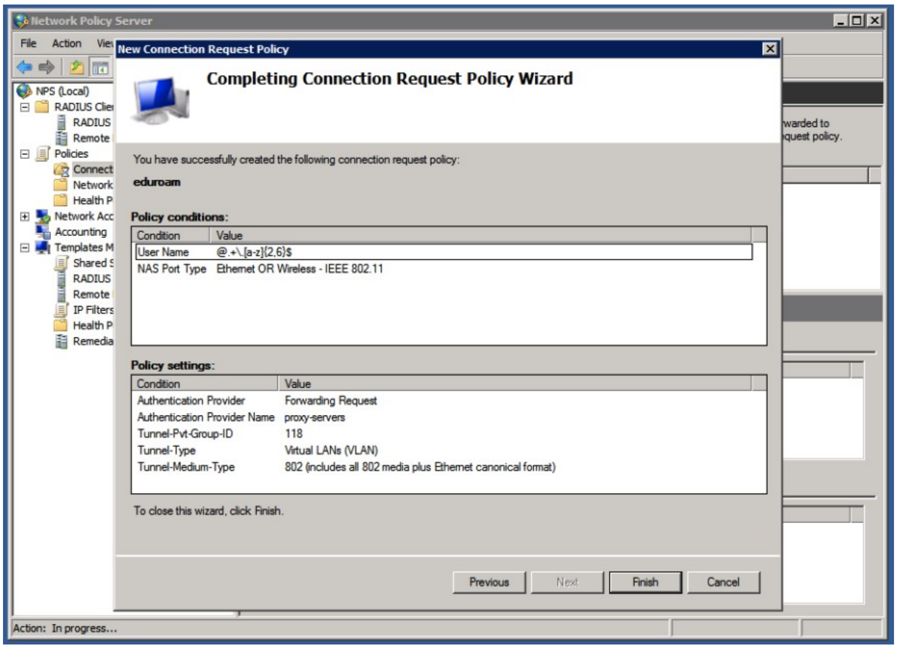
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Tunnel-Pvt-Group-ID	118
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...

The above example adds VLAN 118 for guests authenticated via your Access-Points. Look at your Access-Point documentation to find the actual attributes you need to use, some use non-standardized attributes for this. When in doubt, start without any of these attributes.

As final step, review the settings made by the wizard, and click Finish.



New Connection Request Policy

Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

eduroam

Policy conditions:

Condition	Value
User Name	@.+\.[a-z]{2,6}$
NAS Port Type	Ethernet OR Wireless - IEEE 802.11

Policy settings:

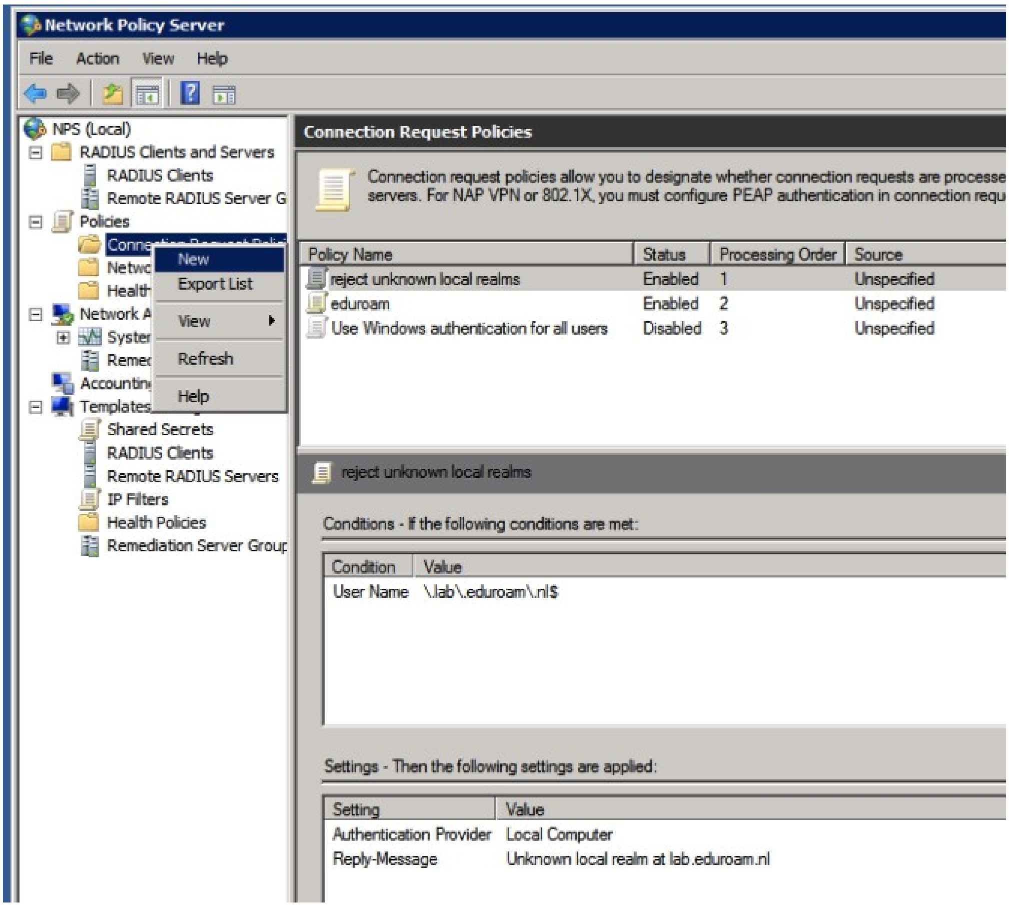
Condition	Value
Authentication Provider	Forwarding Request
Authentication Provider Name	proxy-servers
Tunnel-Pvt-Group-ID	118
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)

To close this wizard, click Finish.

After creating a new policy-rule, always reconsider the order of policies. A policy might catch all the requests and make NPS not consider any of the newer requests.

While testing, take into account that it might take a second or two before NPS actually uses the newly configured settings.

You could test eduroam authentication with a remote (test)-account provided you have one. The next step is to create a policy for local users.



Connection Request Policies

Connection request policies allow you to designate whether connection requests are processe servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection requ

Policy Name	Status	Processing Order	Source
reject unknown local realms	Enabled	1	Unspecified
eduroam	Enabled	2	Unspecified
Use Windows authentication for all users	Disabled	3	Unspecified

reject unknown local realms

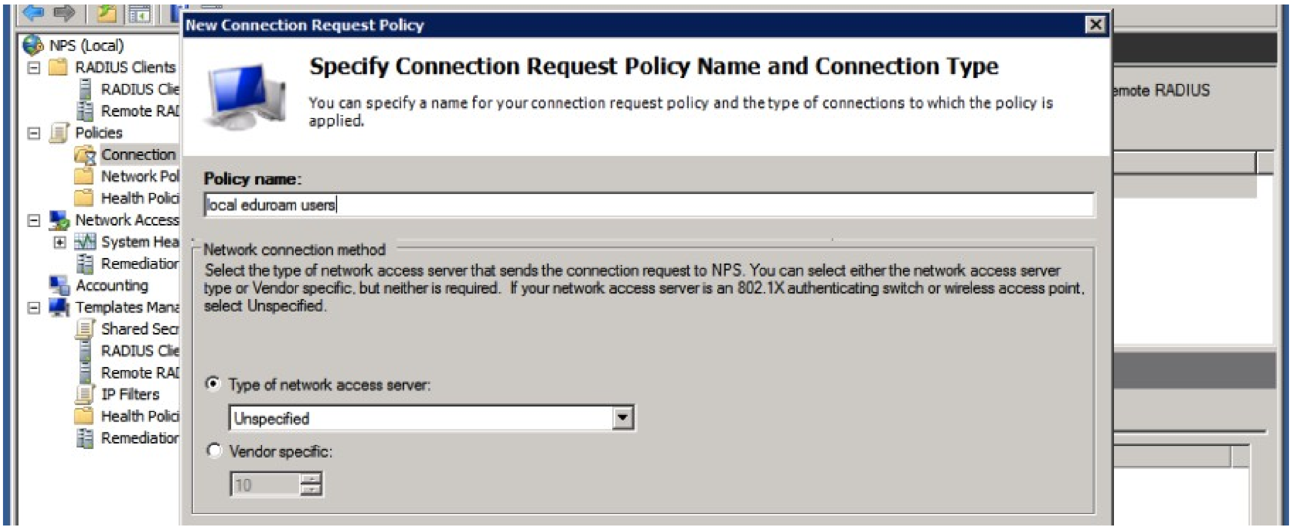
Conditions - If the following conditions are met:

Condition	Value
User Name	\.lab\.eduroam\.nl$

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer
Reply-Message	Unknown local realm at lab.eduroam.nl

Again, click the “Connection Request Policies” tree-item and select “New”.



New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

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

Policy name: local eduroam users

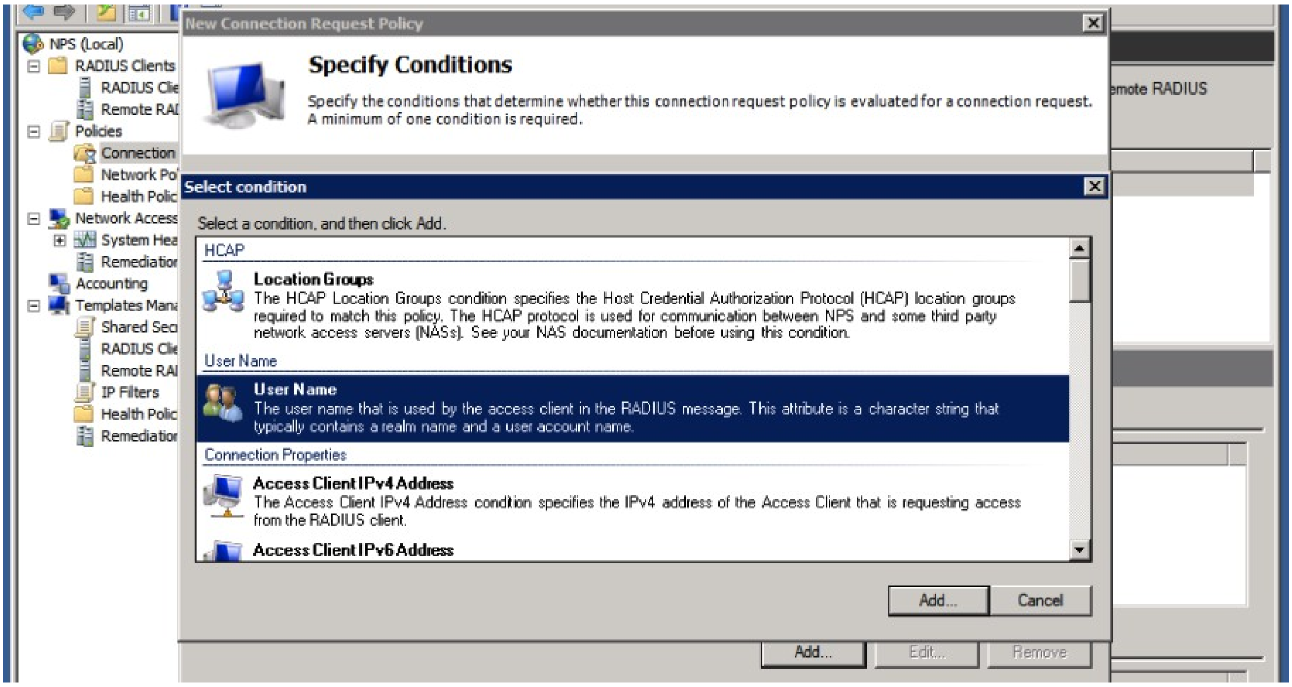
Network connection method

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

Give the policy a name such as “local eduroam users”, and click “Next”.



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.

Select condition

Select a condition, and then click Add.

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.

User Name

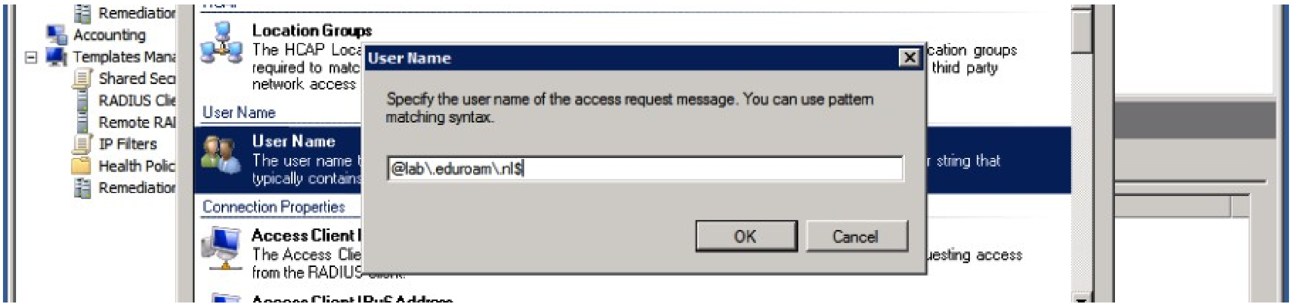
User Name
The user name that is used by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name.

Connection Properties

Access Client IPv4 Address
The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.

Access Client IPv6 Address

Again, we need to specify conditions for the policy to match. In this case we'll want to match local users, by their user-names. This can be done by a regular expression:



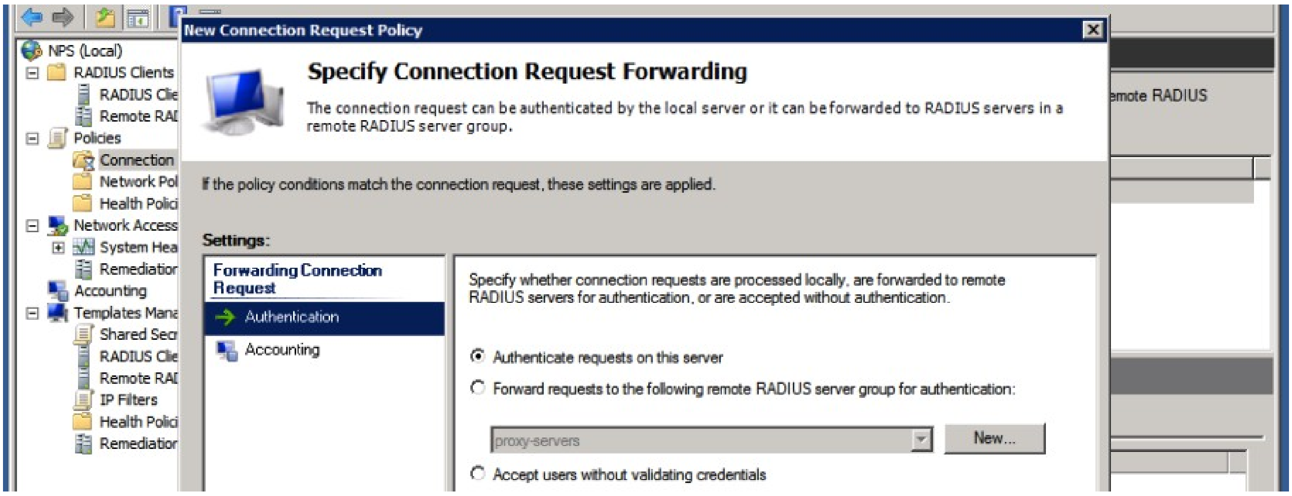
User Name

Specify the user name of the access request message. You can use pattern matching syntax.

@lab\.eduroam\.nl$

Please don't allow users to authenticate without realm! It will be very confusing for users if it works locally without @realm, and you need to have a @realm in a remote location. That breaks the whole working of eduroam for this user and it will lead to misconfigured clients and support-calls.

Click “OK” and “Next” when done.



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:

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

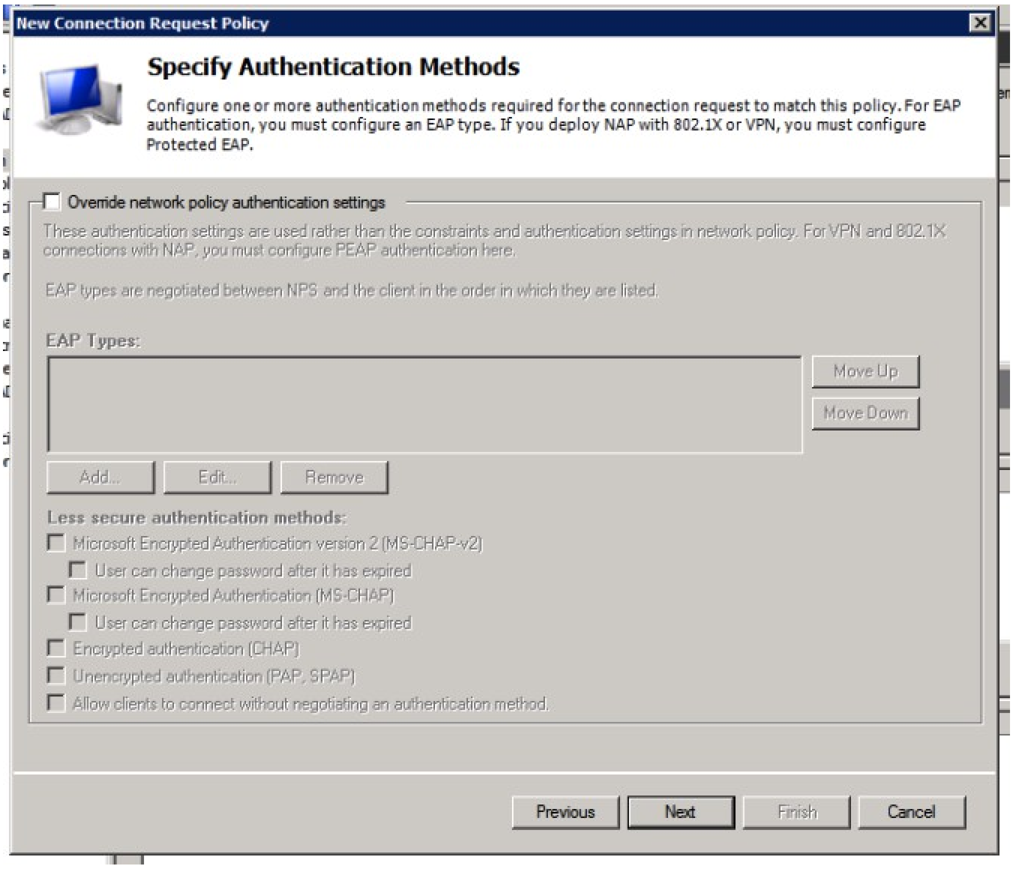
○ Forward requests to the following remote RADIUS server group for authentication:

proxy-servers

○ Accept users without validating credentials

Now, select to “Authenticate requests on this server”.

The next screen asks to override authentication methods configured for this user in the Network Policies.



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.

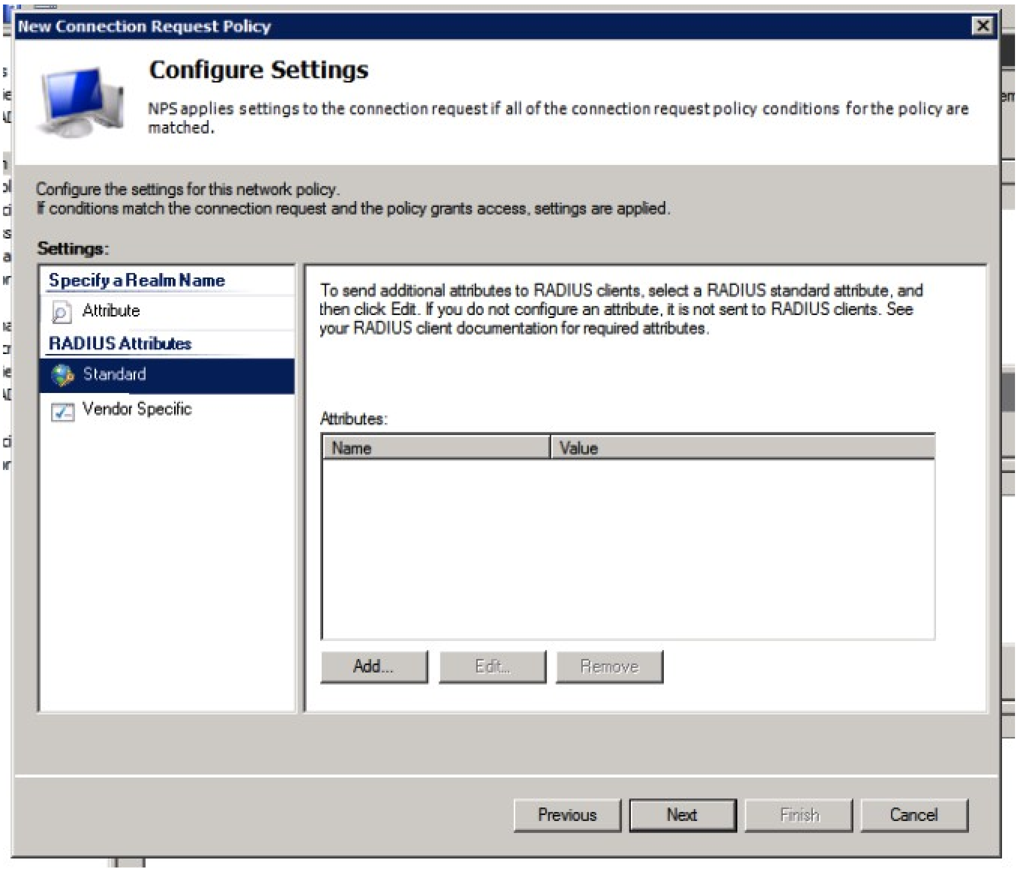
EAP Types:

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.

Make sure no override is done.

The next screen allows you to configure RADIUS attributes, but don't enter anything here.



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:

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.

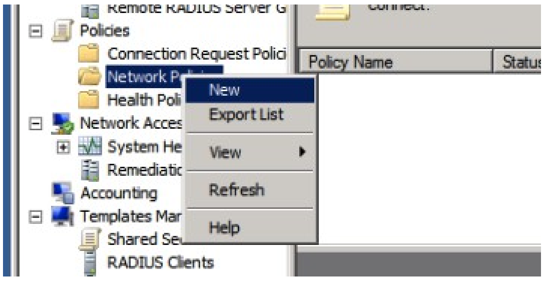
Attributes:

Name	Value

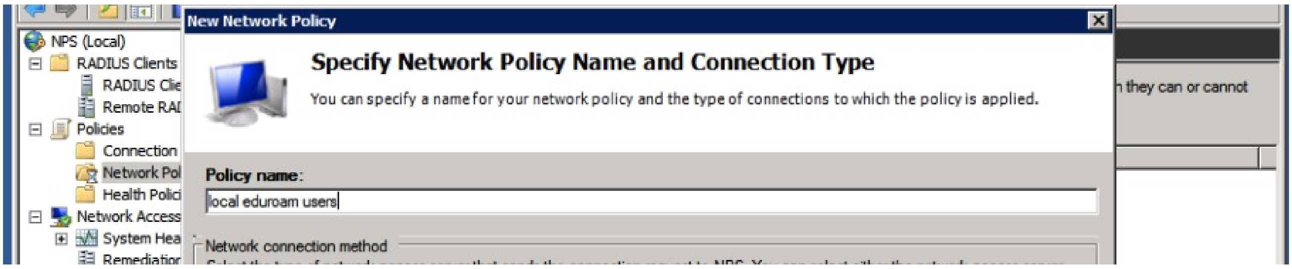
If you want to assign VLAN attributes for your users, you'll need to do that in the Network Policy.

Review your settings, and click “Finish”.

Next, create a Network Policy for your local users.



These policies are only used for Connection Request Policies that have “Authenticate requests on this server” set.



New Network Policy

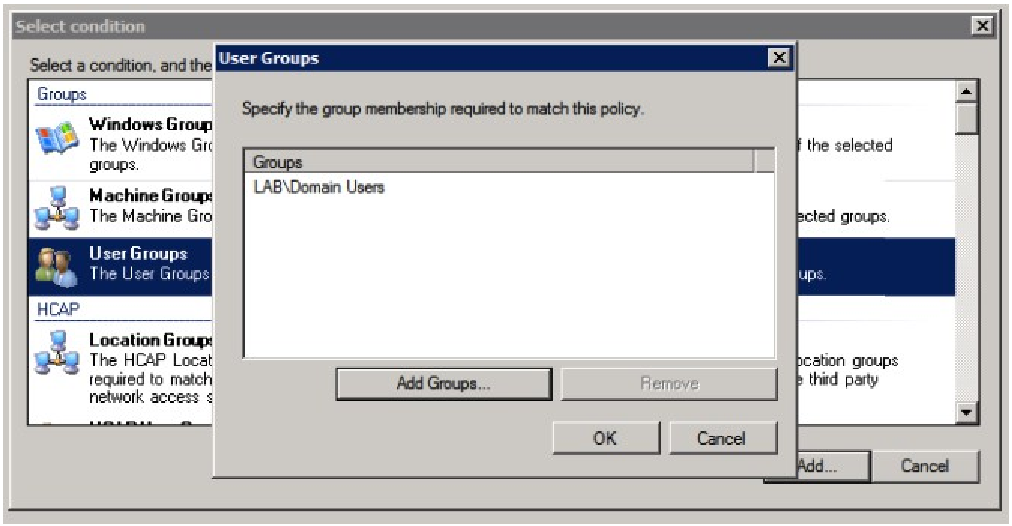
Specify Network Policy Name and Connection Type

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

Policy name: local eduroam users

Network connection method

Give your policy a name such as “local eduroam users” and leave the other settings default.

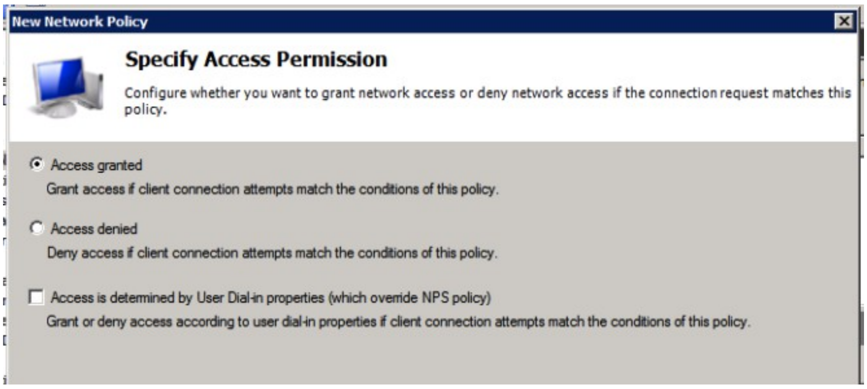


User Groups

Specify the group membership required to match this policy.

Groups: LAB\Domain Users

We need to specify the conditions for matching this request. Here you can define the users in your AD that are allowed to authenticate.



New Network Policy

Specify Access Permission

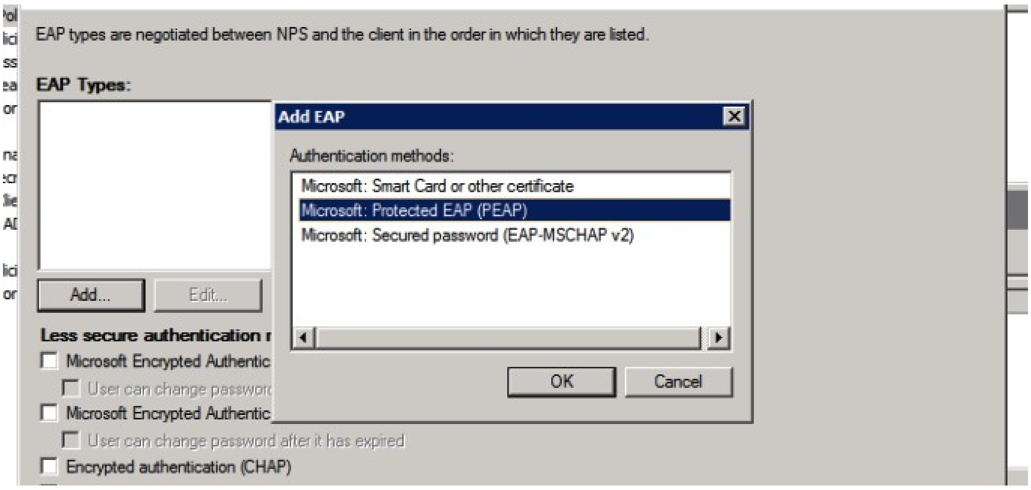
Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● 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.

In the next screen, select to grant access to these users. Now for the authentication methods that are allowed:



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

EAP Types:

Less secure authentication r

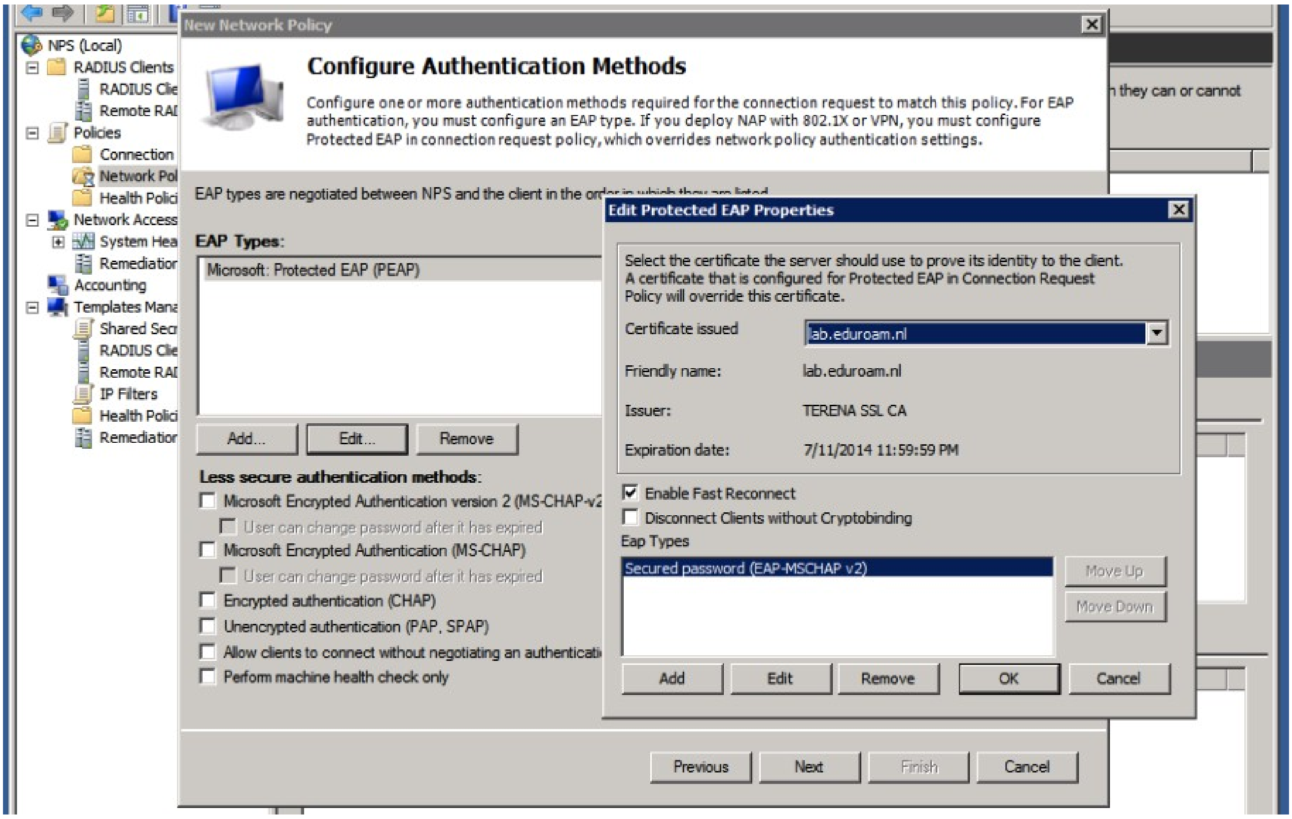
□ Microsoft Encrypted Authentic
□ User can change passworc
□ Microsoft Encrypted Authentic
□ User can change password after it has expired
□ Encrypted authentication (CHAP)

Add EAP

Authentication methods:

Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)

Deslect the “Less secure authentication methods”, and click “Add...” to add an EAP type named “Microsoft: Protected EAP (PEAP)”.



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)

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 authenticati
□ Perform machine health check only

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: lab.eduroam.nl

Friendly name: lab.eduroam.nl

Issuer: TERENA SSL CA

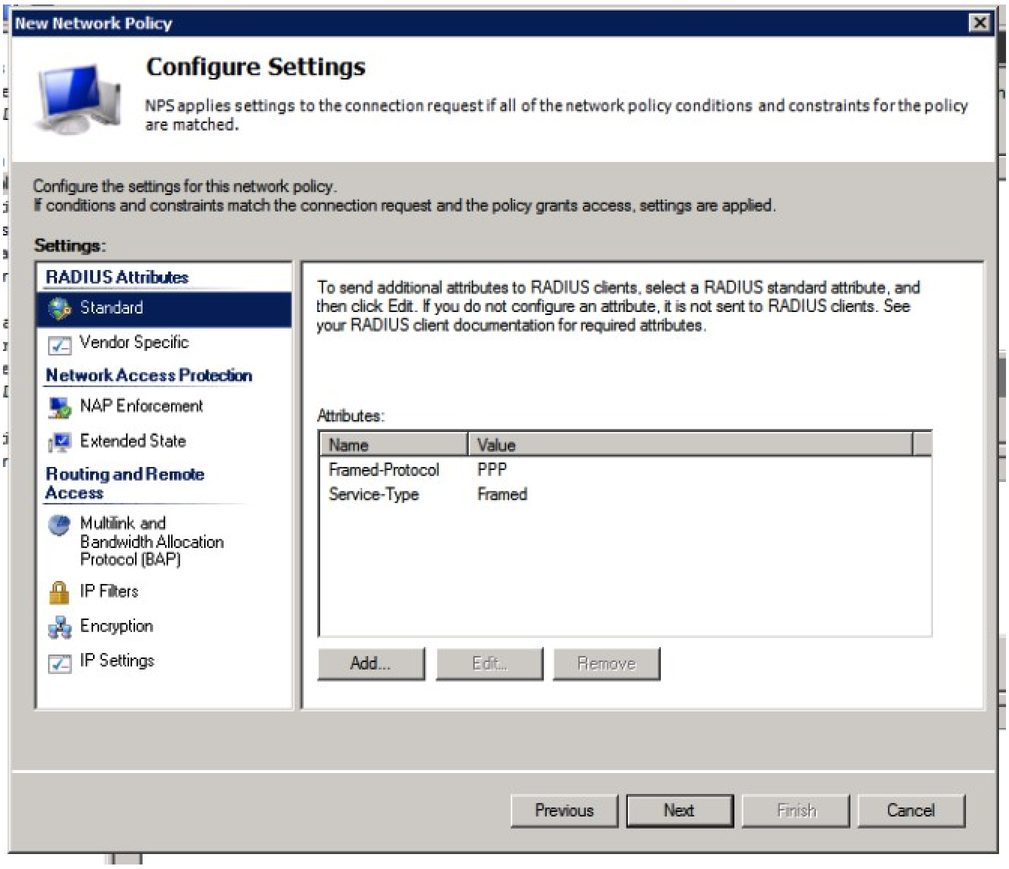
Expiration date: 7/11/2014 11:59:59 PM

☑ Enable Fast Reconnect
□ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

Edit the PEAP settings, and make sure the proper certificate for the server authentication and TLS tunnel setup is selected. (See the Appendix about certificates if any of these steps give a warning or if you don't have a certificate installed just yet.)



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:

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:

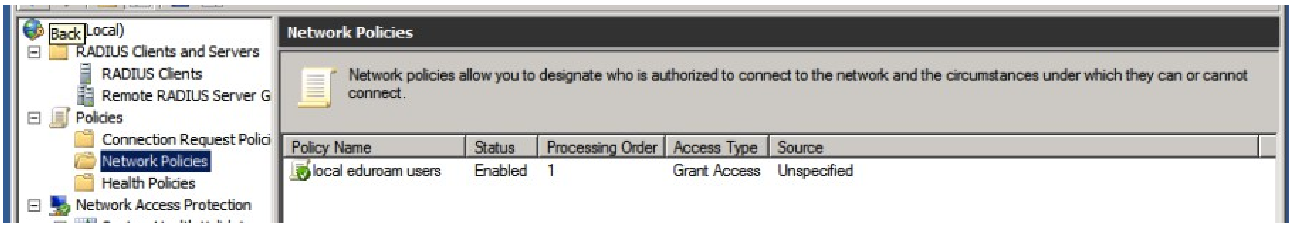
Name	Value
Framed-Protocol	PPP
Service-Type	Framed

In the next step of the wizard you will have the chance to configure any RADIUS attributes.

But: don't add attributes just like that! If you want to override for instance the VLAN by setting attributes for your own users, you need to do this in a seperate policy that only works for your local clients (Access-Points) only. If you set VLAN attributes for your users in authentication requests that originate from the eduroam infrastructure your users might be denied access, which might be a difficult thing to debug.

Don't use NAP enforcement or any of the other settings: they don't have value for eduroam deployments.

Finally, review your settings, and click “Finish”.



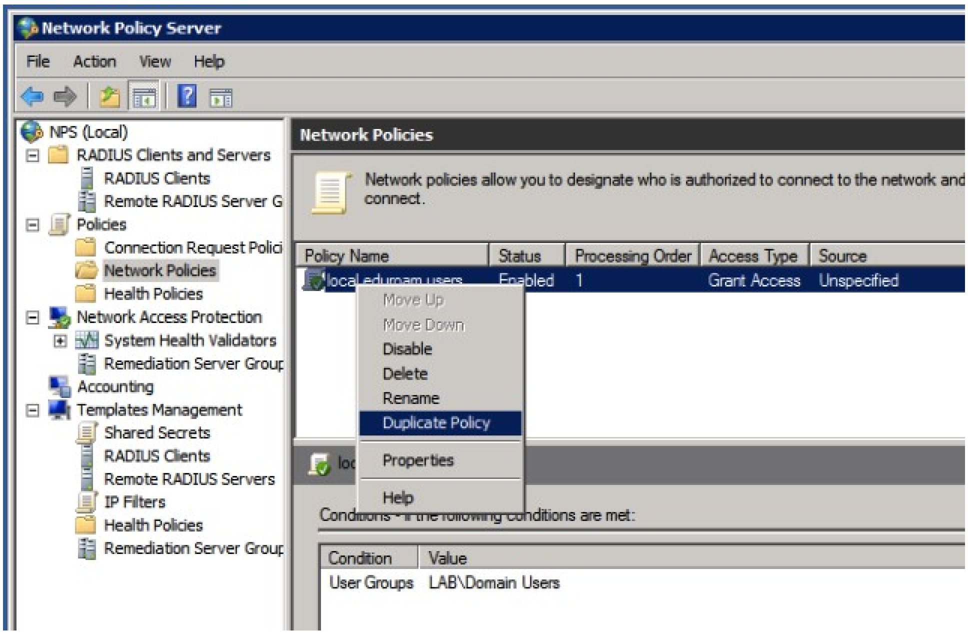
Network Policies

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	Source
local eduroam users	Enabled	1	Grant Access	Unspecified

Your local accounts should now be able to authenticate wirelessly! Go ahead and try it, before making any more changes.

In order to assign VLAN attributes to your local users, we need to duplicate the Network Policy.

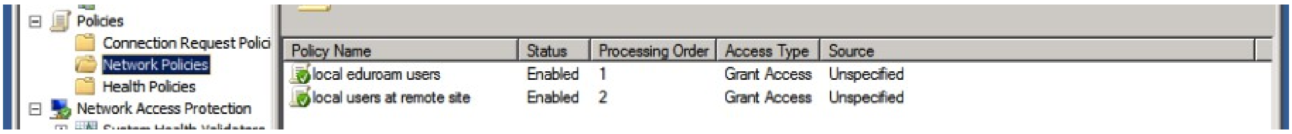


Network policies allow you to designate who is authorized to connect to the network and connect.

Policy Name	Status	Processing Order	Access Type	Source
local eduroam users	Enabled	1	Grant Access	Unspecified

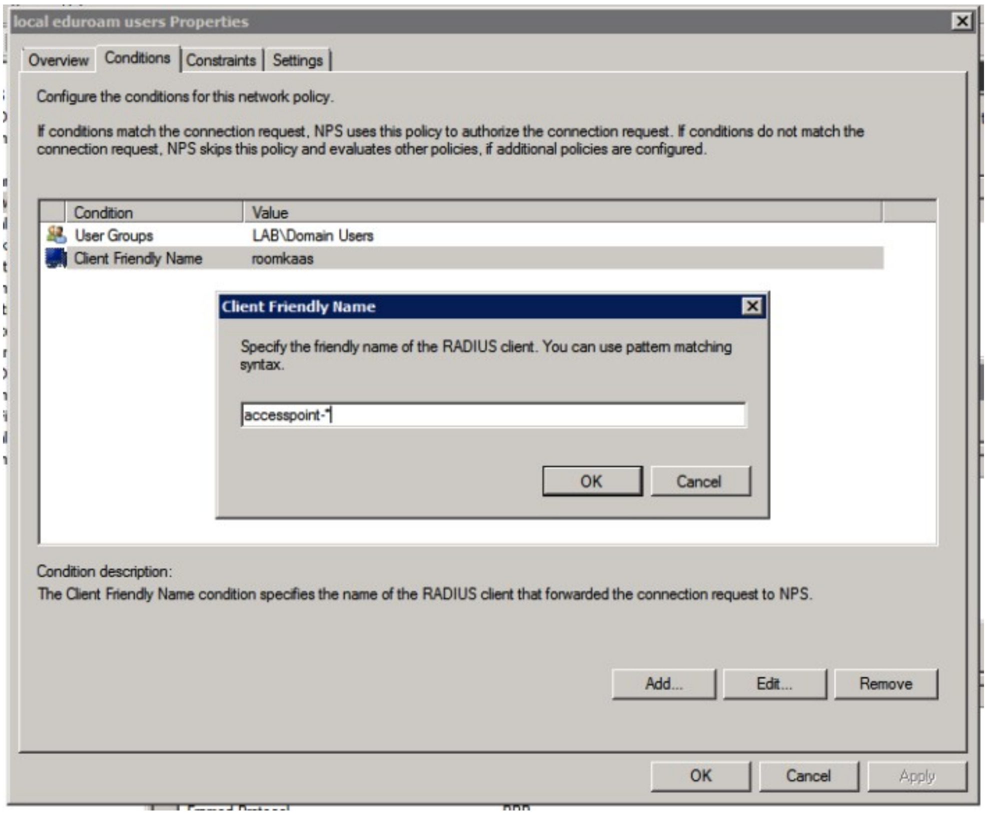
Conditions - If the following conditions are met:

Condition	Value
User Groups	LAB\Domain Users



Policy Name	Status	Processing Order	Access Type	Source
local eduroam users	Enabled	1	Grant Access	Unspecified
local users at remote site	Enabled	2	Grant Access	Unspecified

The order of rules is important: make sure the rule for matching local users is first. You can add extra conditions to this rule to make sure it only matches local requests, and add VLAN attributes in the properties (“Settings” tab) for this policy.



Configure the conditions for this network policy.

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

Condition	Value
User Groups	LAB\Domain Users
Client Friendly Name	roomkaas

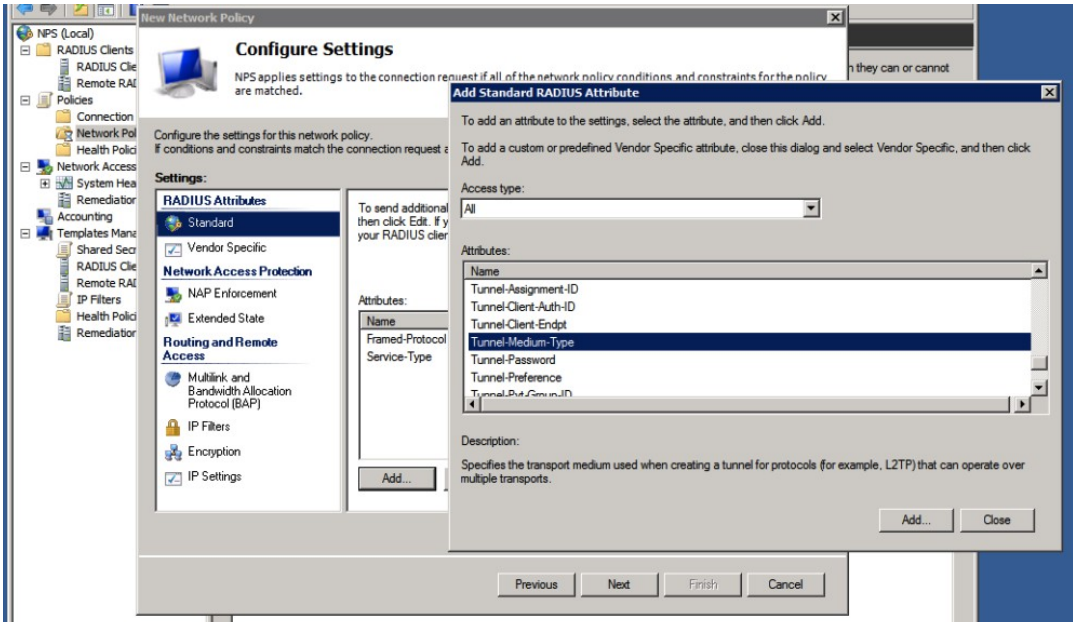
Specify the friendly name of the RADIUS client. You can use pattern matching syntax.

accesspoint-*

Condition description:
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.

First, add a Condition to only match local requests. A simple example is to use the friendly name for your clients: if you named your clients accesspoint-1 and accesspoint-2, you can use an expression here like accesspoint-*

In the settings tab, add additional attributes for your users.



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.

Settings:

Attributes:

Name
Framed-Protocol
Service-Type

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

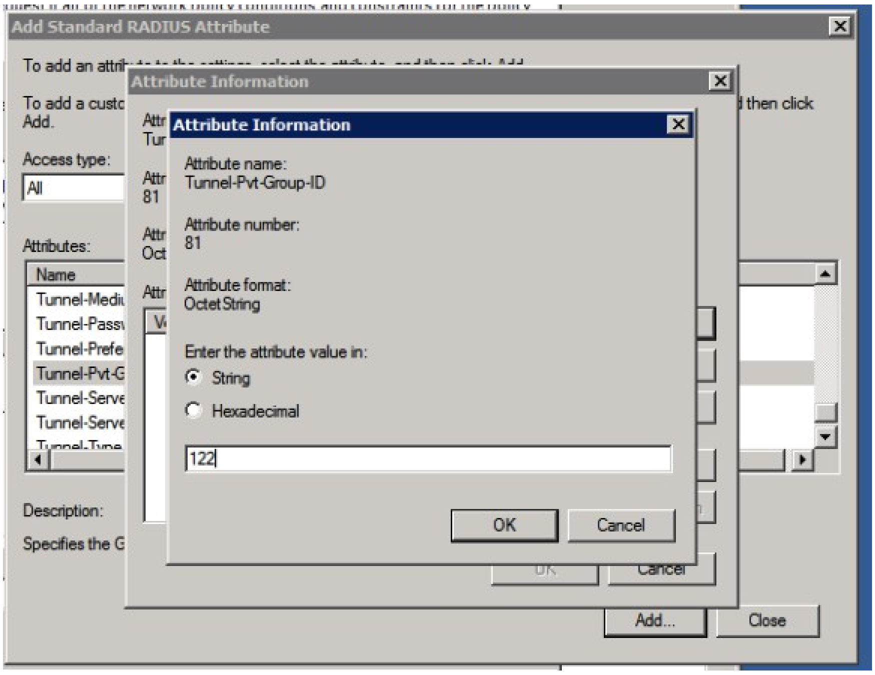
Attributes:

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

Description:

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

The standardized attributes for VLANs are Tunnel-Medium-Type, Tunnel-Type and Tunnel-Pvt-Group-ID where the Tunnel-Pvt-Group-ID contains the number of the VLAN you want to assign.



Attribute Information

Attribute name:
Tunnel-Pvt-Group-ID

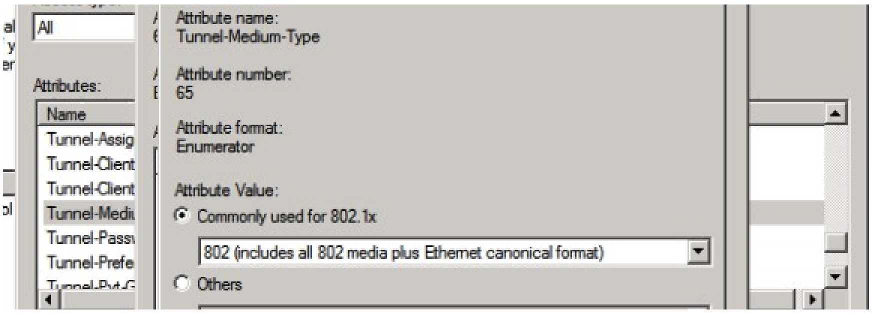
Attribute number:
81

Attribute format:
OctetString

Enter the attribute value in:
● String
○ Hexadecimal

122

The other attributes need to contain default values,



Attribute name:
Tunnel-Medium-Type

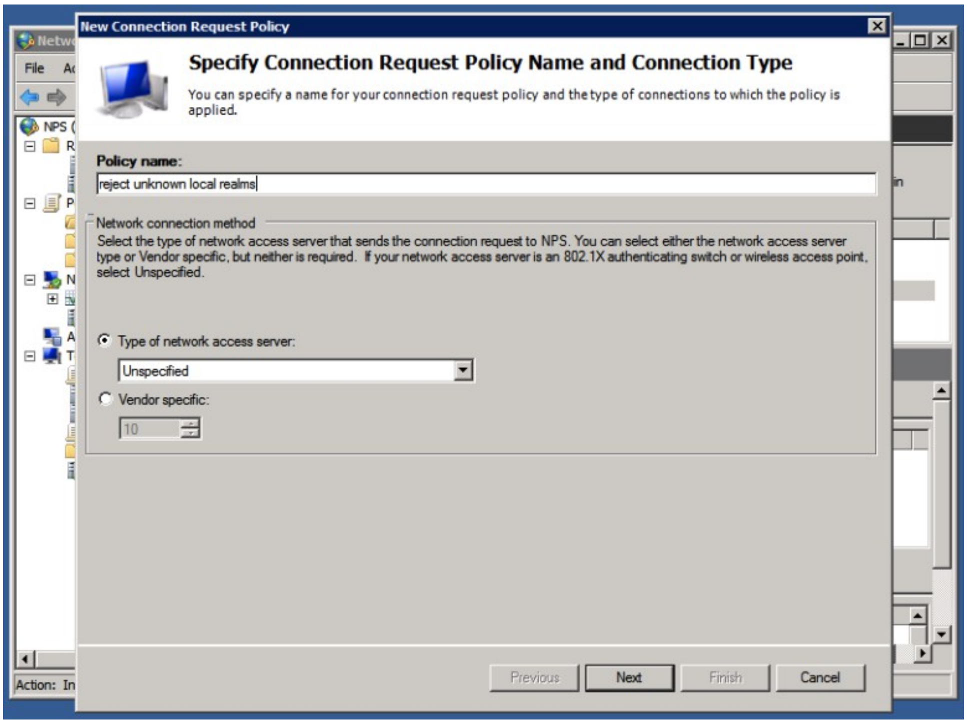
Attribute number:
65

Attribute format:
Enumerator

Attribute Value:
● Commonly used for 802.1x
802 (includes all 802 media plus Ethernet canonical format)
○ Others

Tunnel-Medium-Type = 802, and Tunnel-Type = Virtual LANs (VLAN).

One last Connection Request Policy needs to be created (unless your National Roaming Operator only forwards the realms you're using to your servers).



New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

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

Policy name:

reject unknown local realms

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.

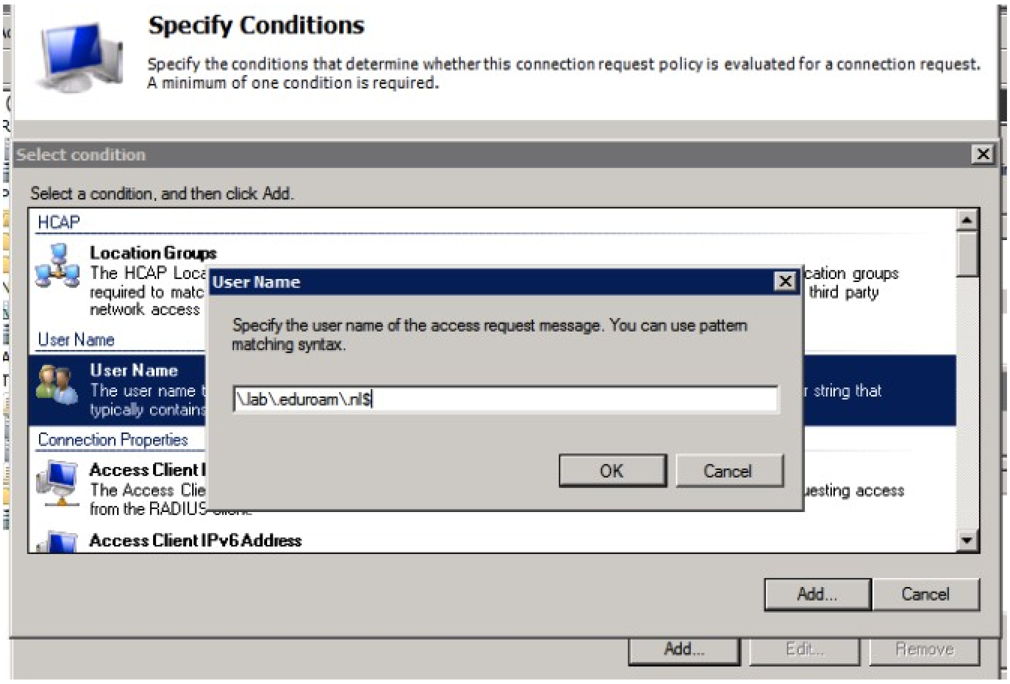
● Type of network access server:

Unspecified

○ Vendor specific:

10

We need to create a policy to reject “unknown local realms”: realms that are sub-realms of your realm, but are not actually used. When they are forwarded to you by the proxies, you shouldn't forward them back to the proxy servers, because that will create loops.



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.

Select condition

Select a condition, and then click Add.

HCAP

Location Groups
The HCAP Loca ... required to matc ... network access ... cation groups ... third party

User Name

User Name
The user name ... typically contains ... string that

Connection Properties

Access Client I
The Access Clie ... from the RADIUS ... uesting access

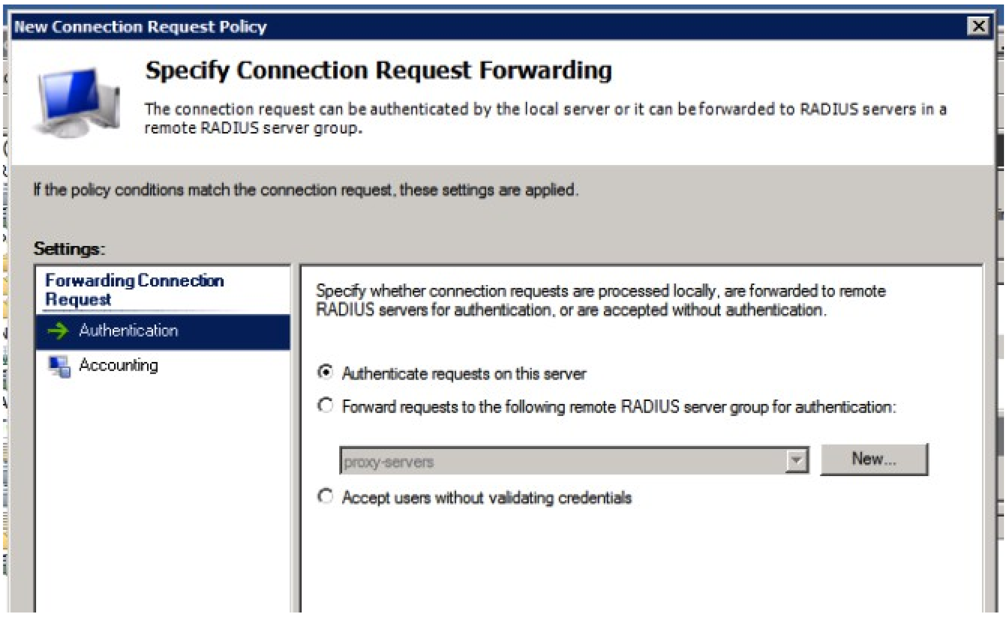
Access Client IPv6 Address

User Name

Specify the user name of the access request message. You can use pattern matching syntax.

\.lab\.eduroam\.nl$

The condition to match for this rule (that should come after all other rules for local users but before the proxy userse) should match a user-name ending on your top-level realm. This is done by a regular expression such as \.lab\.eduroam\.nl$



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:

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

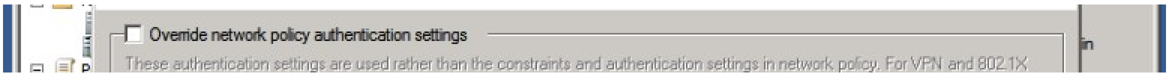
● Authenticate requests on this server

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

proxy-servers

○ Accept users without validating credentials

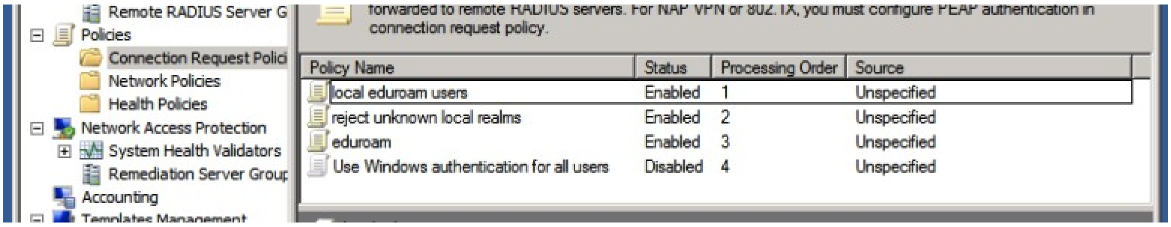
Though we're going to reject the request, set it to authenticate on this server. It needs to be processed locally, and not forwarded.



☐ 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

Don't override any of the settings and finalize the policy; you can create a Network Policy to match the requests as well and assign a Reply-Message to log why the request was rejected, but it's no problem to leave that out.



forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
local eduroam users	Enabled	1	Unspecified
reject unknown local realms	Enabled	2	Unspecified
eduroam	Enabled	3	Unspecified
Use Windows authentication for all users	Disabled	4	Unspecified

Make sure the order of Connection Request Policies and the Network Policies is correct, and test your configuration.

Topics not yet covered (and/or left as exercise to the reader):

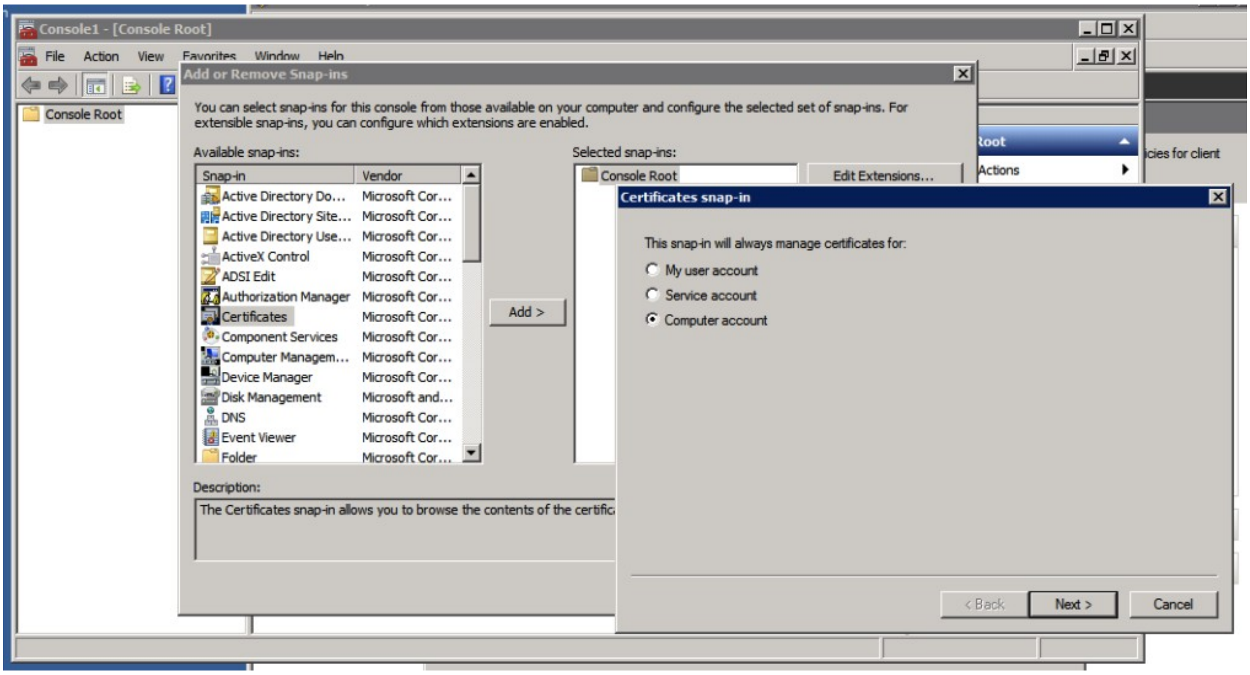
- Logging (Take a look at the Accounting section)
- Adding the Operator-Name attribute (That needs a dictionary change, annoying)
- Loop prevention (By using conditions to filter on proxyserver-* for instance, or only trigger with conditionon accesspoint-*)

Appendix A: Certificates

You need to have a server certificate in order to use PEAP-authentication with eduroam. PEAP sets up a secure SSL tunnel (just like HTTPS does for websites) in order to protect the credentials, and is an important part of the mutual authentication: both the user needs to prove who he or she is, and the authentication server needs to prove to the user that he or she is providing credentials to the right authority.

Without certificate (self signed or not) it's not possible to do local authentication. NPS can still be used as a proxy to receive requests from Access Points, log, filter, and forward to the eduroam infrastructure.

Open the Microsoft Management Console, mmc (via “Start” – “Run” – “mmc”). Go to “File”, “Add/Remove Snap-in...”, select “Certificates”, click “Add >” and answer the prompt by choosing “Computer account”:



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...

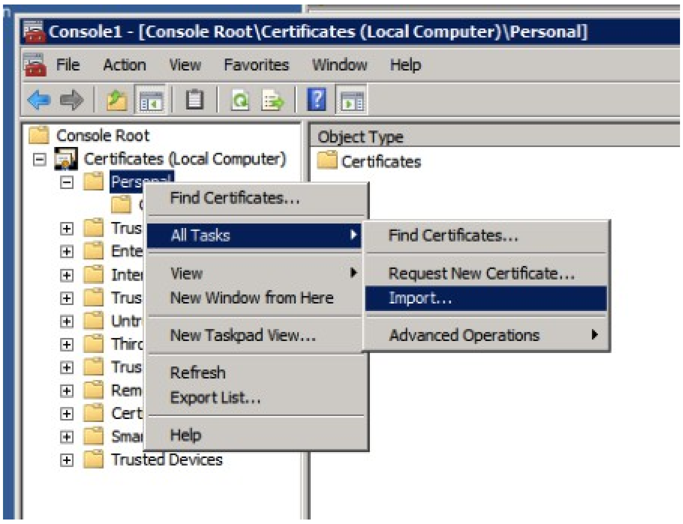
The Certificates snap-in allows you to browse the contents of the certific

This snap-in will always manage certificates for:

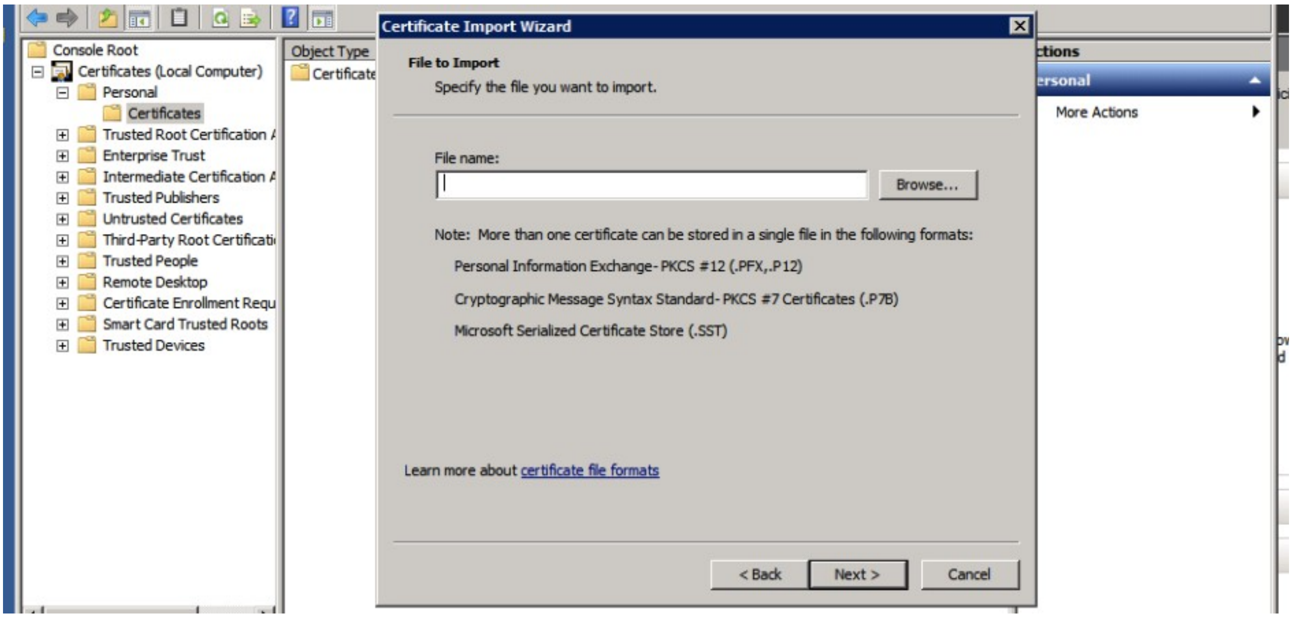
○ My user account
○ Service account
● Computer account

After this, select you want to access the resources on the Local Computer (assuming that's where you install your NPS on), and click “Ok” in the “Add or Remove Snap-ins” window to work with the MMC console.

If you have a signed certificate already in pkcs12 format, you can import it (and/or intermediate certificates) to the “Personal” store by right-clicking the “Personal” folder and choosing “Import...” under “All Tasks”.



Clicking “Next” after the Certificate Import Wizard introduction asks you for the certificate files to import.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

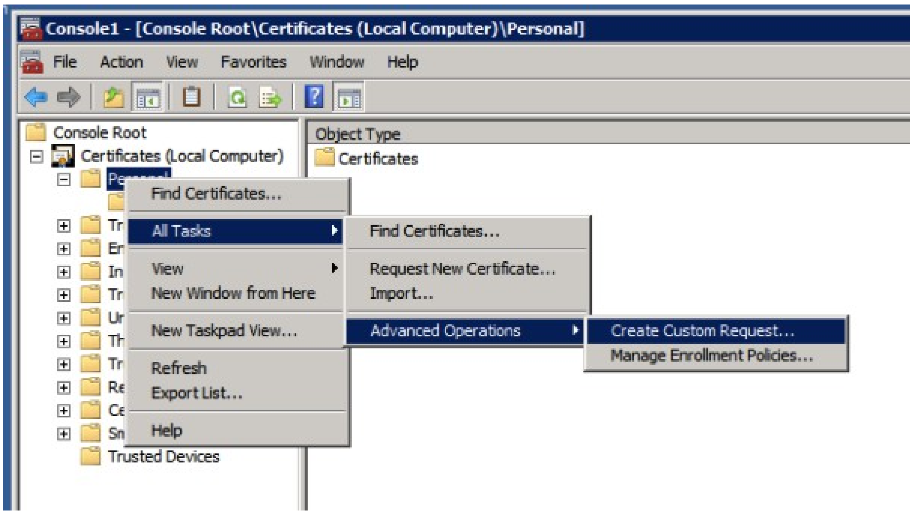
Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

In the next screens you're asked for the password that protected the file, and folder to store the certificate in (this is the “Personal” folder that you just selected). Then the import is complete you will find your certificate in the Personal folder, and you can select it from NPS later.

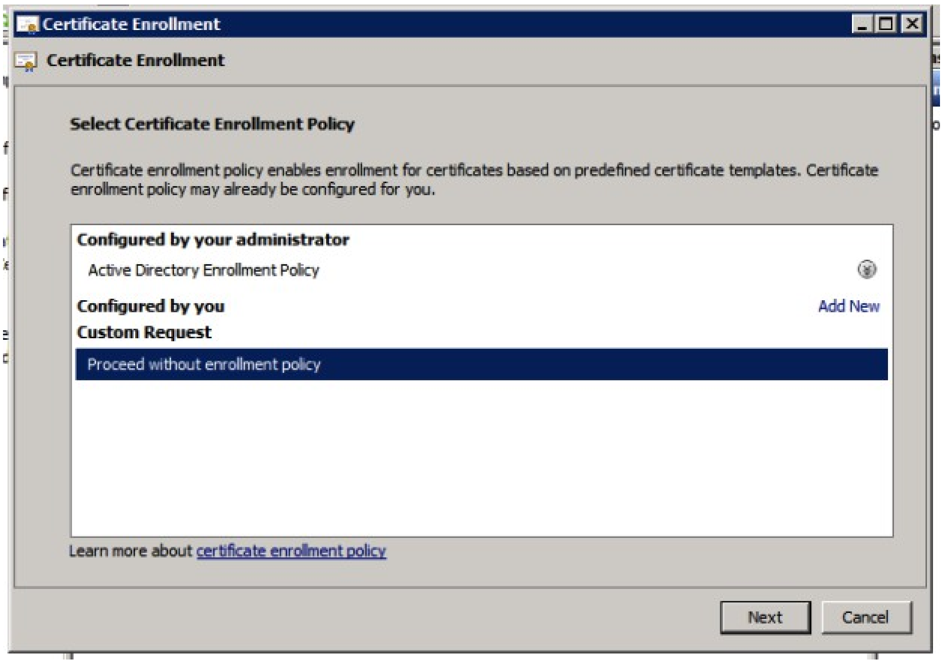
Generate a certificate request

If you have no existing certificate to import, you need to generate a CSR to be signed.



Create the request by right-clicking the “Personal” tree in the Certificates snap-in, selecting “All Tasks – Advanced Operations” and “Create Custom Request”. Click “Next” after the introduction and (assuming you have no internal CA running) choose “Custom Request, proceed without enrollment policy” as shown below.

If you have an internal CA, the procedure is different. If your (Windows) clients also get this CA enrolled by the Active Directory, an internal CA might be an option for your server certificate. If your clients (especially true with “bring your own” devices) don't have the internal certificate, having a certificate from a public certificate authority (CA) makes the configuration of eduroam on the devices easier. Windows for one, refuses to authenticate if it can't verify the certificate used by any of its stored CA's, whether public or not. A self-signed certificate, means more work for the end-users (and maybe more support calls).



Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

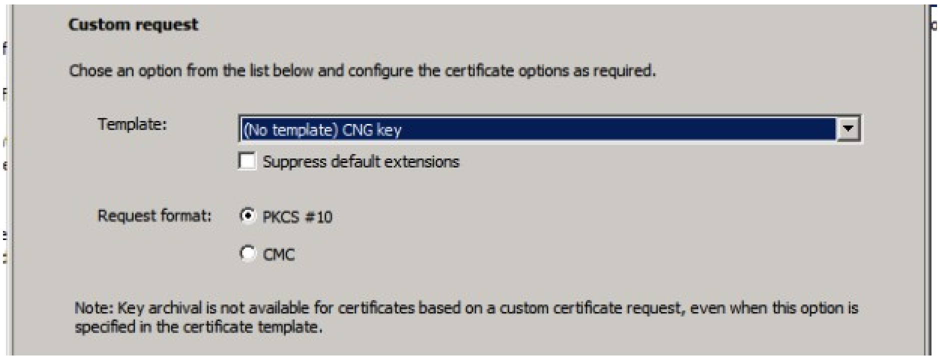
Configured by you

Custom Request

Proceed without enrollment policy

Learn more about certificate enrollment policy

After clicking “Next”, leave the options for the Custom request default to PKCS10;



Custom request

Chose an option from the list below and configure the certificate options as required.

Template: (No template) CNG key

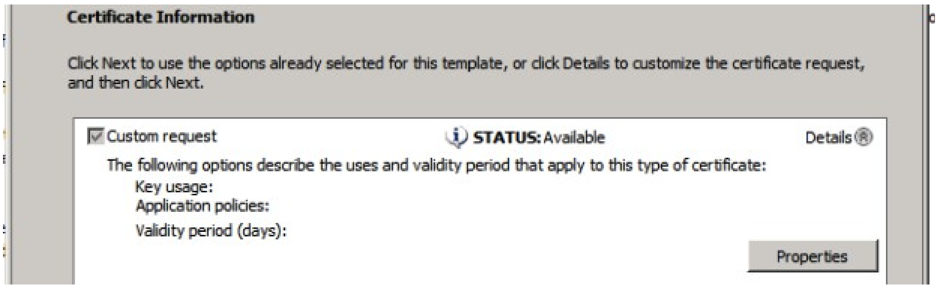
□ Suppress default extensions

Request format: ● PKCS #10

○ CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

In the next screen though, you need to change some properties for the requested certificate:



Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ Custom request   STATUS: Available

The following options describe the uses and validity period that apply to this type of certificate:

Key usage:

Application policies:

Validity period (days):

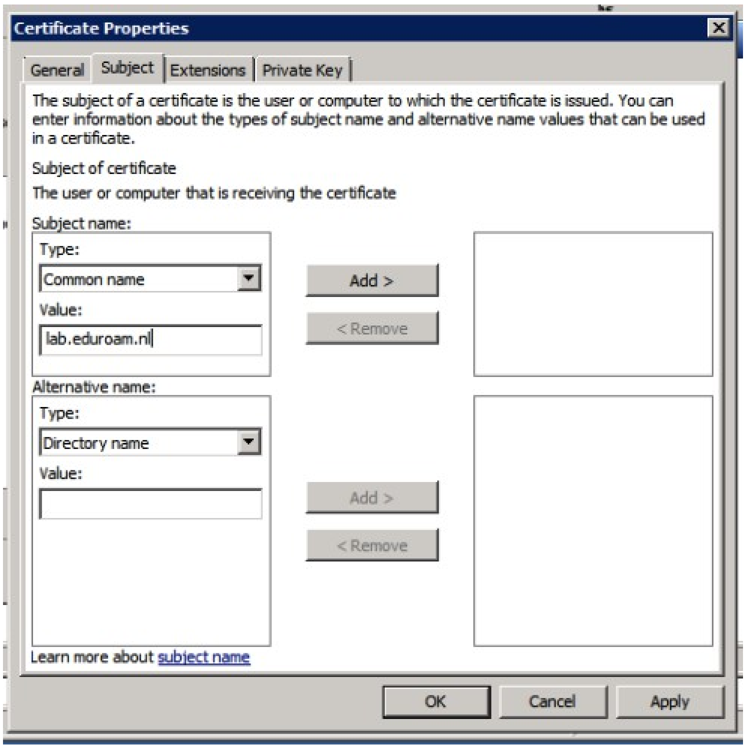
In the “General” tab you can configure a friendly name for the certificate; in this example the “common name” (CN) of the certificate is used: lab.eduroam.nl – this is also the domain under which the Active Directory operates, and it will be the RADIUS realm too.

In the “Subject” tab, enter the “Common Name” for your certificate. You probably need to prove ownership of the hostname/domain used to the certificate authority (CA), plus your users will see this name in the certificate: so this name is important.

It doesn't need to be the name of the host itself: actually, if you have multiple NPS servers, it's important that all servers have the same certificate because devices will (at least) prompt when there is a certificate change (which is what then happens during failover).

If your users recognize the name of the certificate when they're prompted, that's probably safer and easier for instructions. (Besides, they might need to check other properties of the certificate, eg. the fingerprint, which is what the Windows 8 client will show for verification.)

If you make the certificate “eduroam.your-org.tld” for instance, that's fine. In this case, we're using “lab.eduroam.nl” for the CN.



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value: lab.eduroam.nl

Alternative name:

Type: Directory name

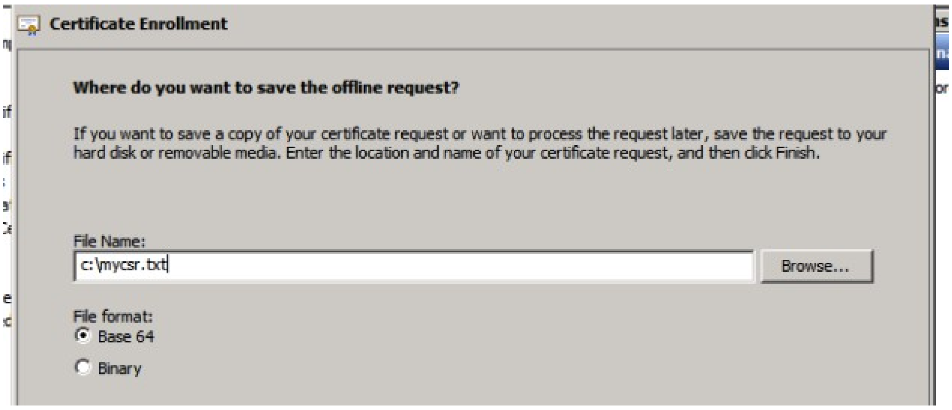
Value:

Learn more about subject name

Click “Add” for the subject, and go to the Private Key menu. It's recommended (and by some CA's required) to make the key size 2048 bits. Click “OK” after these changes, and proceed to the “Next” step in the Wizard.

(Make sure the profile used at the public CA includes the TLS server extensions. If you use an internal CA in your Active Directory, you might want to include these extensions in the “Extensions” tab. For a public CA, you probably don't have to worry about this.)

Store your certificate signing request (CSR) in a file: to request the certificate you need to copy-paste the BASE64 contents to the request page.



Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

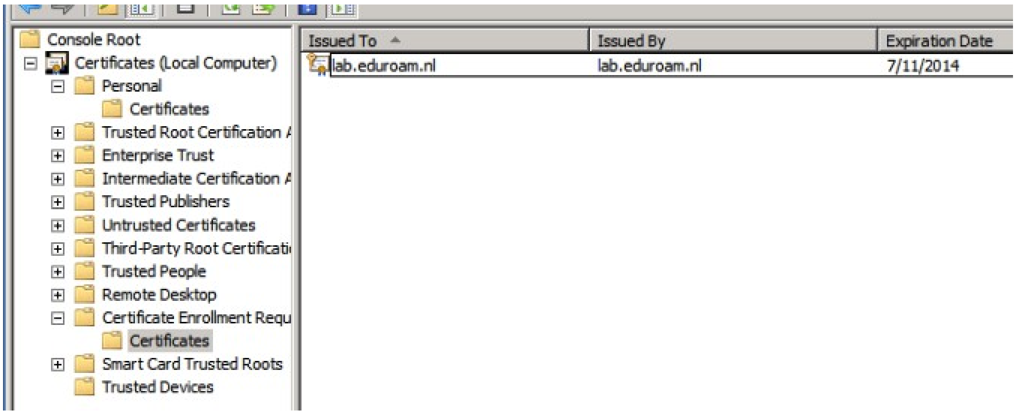
File Name: c:\mycsr.txt

File format:

● Base 64

○ Binary

The certificate request (and private key for now), you will find under the Certificate Enrollment Requests. You can also delete it from there if you made a mistake.

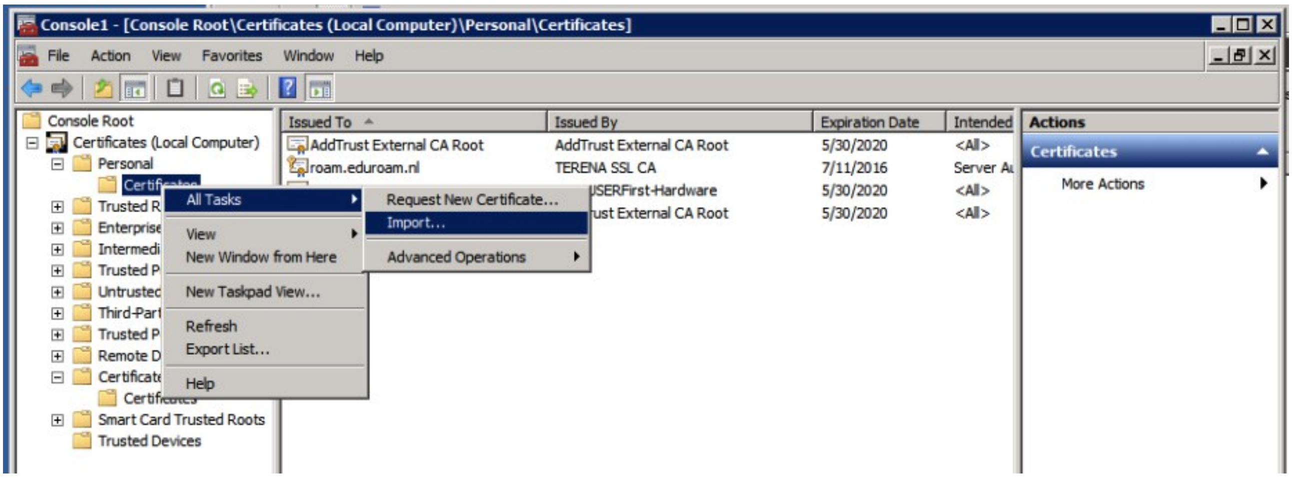


Issued To	Issued By	Expiration Date
lab.eduroam.nl	lab.eduroam.nl	7/11/2014

Now, request your certificate using the file/BASE64 copy-pasted content at your CA page. If you're a Terena Certificate Service you probably know the URL for this; you can also request a certificate at any of the well known commercial CA vendors, such as Comodo, GlobalSign, Verisign... or even test it with a trial-certificate that's valid for limited time.

It's preferable to make your certificate expire after a longer period, such as 3 years: your users might receive a prompt about the new certificate that you need to tell them about before changing it. (Normally if they get such a prompt, this could be a man-in-the-middle attack, so inform them about that too! Mutual authentication is an important part of your security!)

After your certificate is issued by the CA, import it via the MMC snap-in:



Issued To	Issued By	Expiration Date	Intended
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	<All>
roam.eduroam.nl	TERENA SSL CA	7/11/2016	Server Au
	JSERFirst-Hardware	5/30/2020	<All>
	ust External CA Root	5/30/2020	<All>

You can download the .pem files provided by the provisioning interface of the public CA.

Also install the intermediate certificates that you receive from your CA, in particular if they're not already installed in your store. The NPS server needs to send them (along with the certificate) to the clients in order to do proper verification. (This isn't different from protecting a website with SSL certificates.)