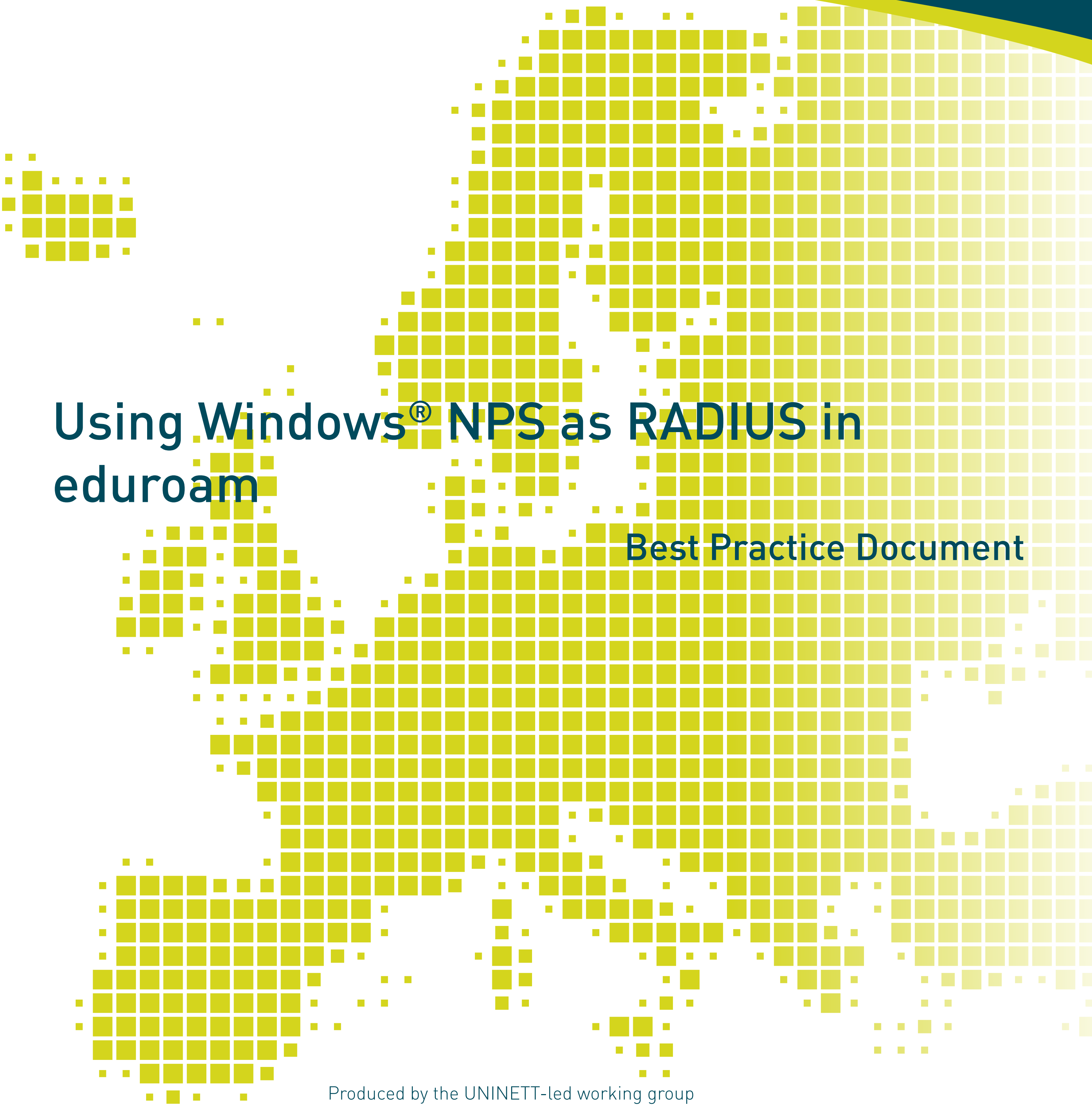


Using Windows® NPS as RADIUS in eduroam

Best Practice Document

Produced by the UNINETT-led working group
on campus networking

Authors: P. Dekkers (SURFnet), T. Myren (UNINETT)

February 2015

Document No:	GN3-NA3-T4-UFS140
Version/ date:	V1.0 / February 2015
Source language:	English
Original title:	“Using Windows NPS as RADIUS in eduroam”
Original version/ date:	Version 1 / 7 October 2014
Contact:	campus@uninett.no

UNINETT bears responsibility for the content of this document. The work has been carried out by a UNINETT-led working group on campus networking as part of a joint-venture project within the HE sector in Norway. Original input for this document was given by Paul Dekkers from SURFnet in the Netherlands. DANTE and TERENA joined forces in October 2014 to become the GÉANT Association.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 605243, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3plus)'.

Table of Contents

Executive Summary

Network Policy Server (NPS) is the Microsoft Windows implementation of a Remote Access Dial-in User Service (RADIUS) server and proxy. An increasing number of institutions in the Norwegian HE sector have chosen to use Windows NPS as their RADIUS server connected to the eduroam infrastructure. This document is provided to explain in some detail how Windows NPS should be configured to best fit in with eduroam.

The examples in this document are collected from a mix of both Windows Server 2008 R2 Enterprise and Windows Server 2012 R2. The dialogue screens differ slightly between the two versions, but the configuration items are very similar.

The instructions in this document assume a basic setup of an Active directory.

For the configuration of related equipment (Access Points, controllers and other RADIUS servers), please see the References section for links to other resources. This includes both other best practice documents and TERENA confluence pages.

1 Introduction

This is a listing of tasks involved in setting up Windows NPS for eduroam as a quick-start for more experienced users. The topics below are covered in more detail through the rest of this document:

- Installing NPS as a server role
- A server certificate suitable for eduroam (and NPS) is required. This could be a self-signed certificate or signed by a public Certificate Agency (CA).
- Configuring RADIUS clients (and shared secrets). Wireless Controllers (or Access points) and the proxy-servers of your National Roaming Operator (NRO) must be defined. Details for national proxy servers must be provided and negotiated (shared secrets) with NRO.
- Configuring RADIUS servers in NPS to allow sending requests to NRO proxy-servers for visiting eduroam users. The proxy-servers will be configured in a server group, with one server preferred and with a secondary configured for failover.
- Connection Request Policies to determine how a request is dealt with. Handle locally or proxy to NRO. For local-accounts create a User Name condition that matches your users with their realms, while preventing usage of unknown / unused sub-realms or no realm in username.
    - Such a Connection Request Policy can use “.institution\.no$” as a match for the User Name attribute, matching your realm and all sub realms. Also configure this policy to override Network Policy authentication settings and configure “Microsoft PEAP” as EAP Type (Add, then Edit to select the server certificate) and deselect all “less secure” mechanisms.
    - A Connection Request Policy to forward requests to the proxy-server group could match a User Name “@.+\..+$”. Or matching only valid TLD realms “@.+\.[a-z]{2,6}$”
- Configure one or more Network Policies. These handle all requests that the Connection Request Polices have set to be authenticated locally. These will handle the actual EAP authentication of your users, unless overwritten in the Connection Request Policy. A policy can be duplicated to add VLAN assignment attributes for local use, while travelling users should not receive these attributes.

In the following sections, mainly Windows Server 2012 R2 is used in the examples; configuration in Windows Server 2008 R2 is very similar.

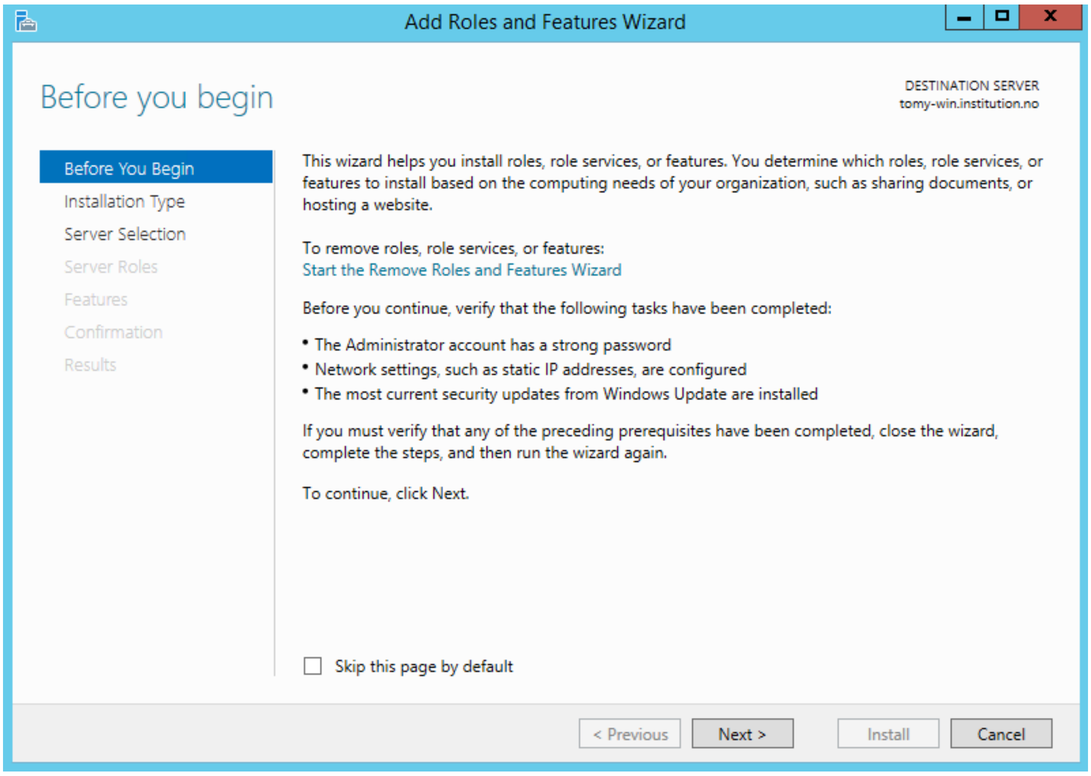
2 Limitations

The Network Policy Server has a few limitations:

- You cannot strip attributes (for instance VLAN attributes assigned by other identity providers (IdPs), but you can explicitly set values applicable to your environment if you work with VLANs or want to prevent invalid attributes.
- You cannot add attributes in outbound requests: adding an “Operator-Name” attribute to indicate where a user gets online is thus not possible and could be set by the National Roaming Operator instead.
- NPS doesn't answer to Status-Server requests. It is best-practise for eduroam proxy servers to check your servers’ availability with those requests, and ideally you would do that the other way round too.
- Because of the previous limitations, inform your National Roaming Operator that you’re working with NPS.
- While the outer username (via the Connection Request Policy) can be rewritten, the inner username (often users configure both to be the same) handled by the Network Policy cannot. This means that your users will have to use the registered UPN (User Principal Name) which by convention maps to the e-mail address / user-ID@domain-name.
- Using anonymous outer identities is not possible. Unless “Override network policy authentication settings” is enabled in the Connection Request Policies. This implies that override network policies should be used, but not all consequences of this are known and some functionality (Constraints and Settings) in Network Policies might be lost.
- Logging in Event manager is rather poor (compared to FreeRADIUS) – there is not much detail shown, making the debugging of any connection problems difficult. Be prepared to install Wireshark for this purpose.

3 Installing NPS

In your Windows server open Server Manager, right click Roles and select Add Roles (2008). Or click Add roles and features. The Add Roles Wizard will open – read the information text and accept the default by just clicking **Next** three times:



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

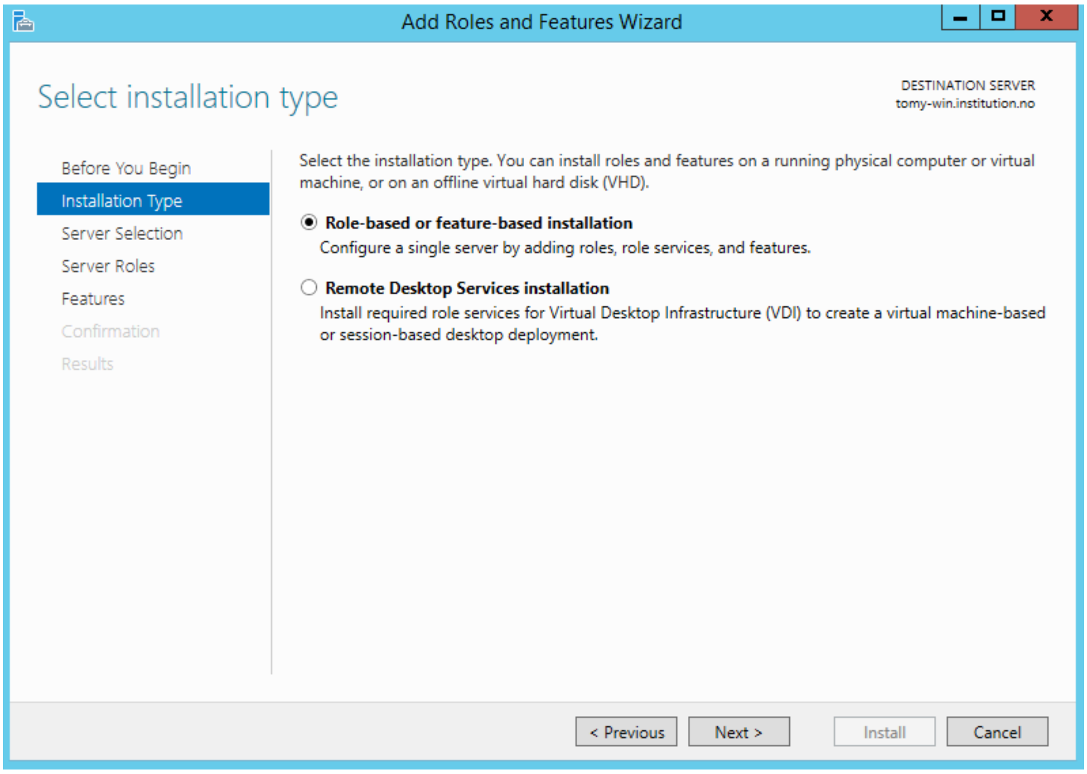
Before you continue, verify that the following tasks have been completed:

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

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default



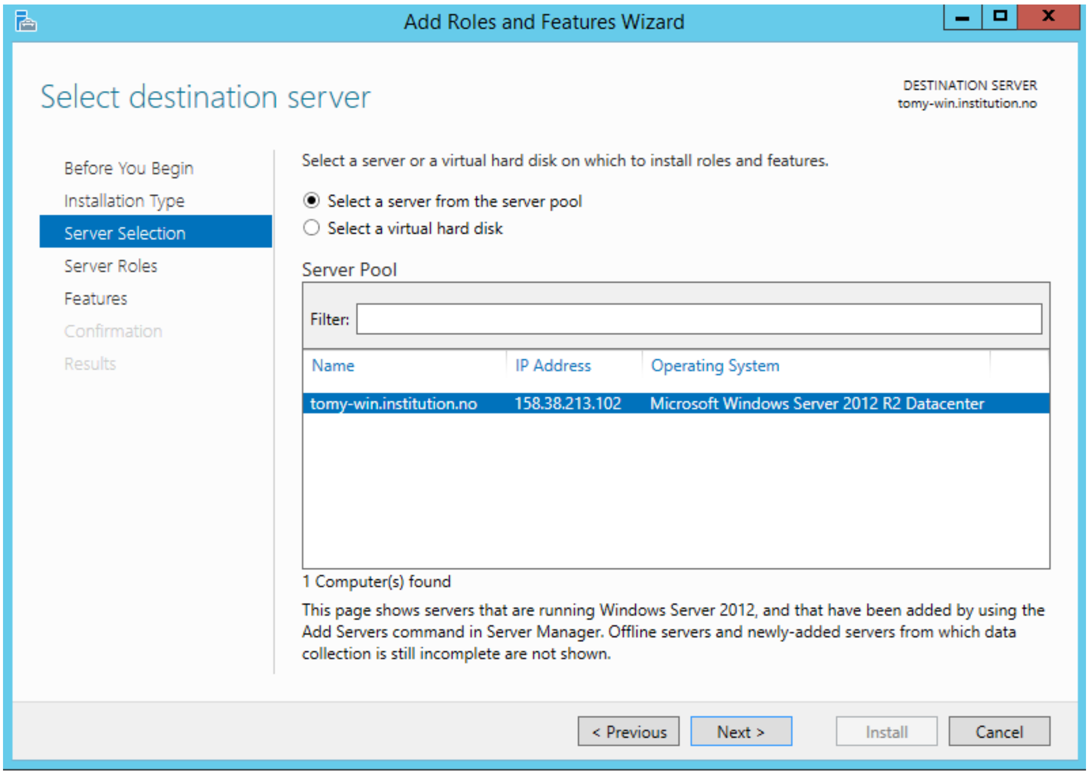
Select installation type

DESTINATION SERVER
tomy-win.institution.no

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Select destination server

DESTINATION SERVER
tomy-win.institution.no

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

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

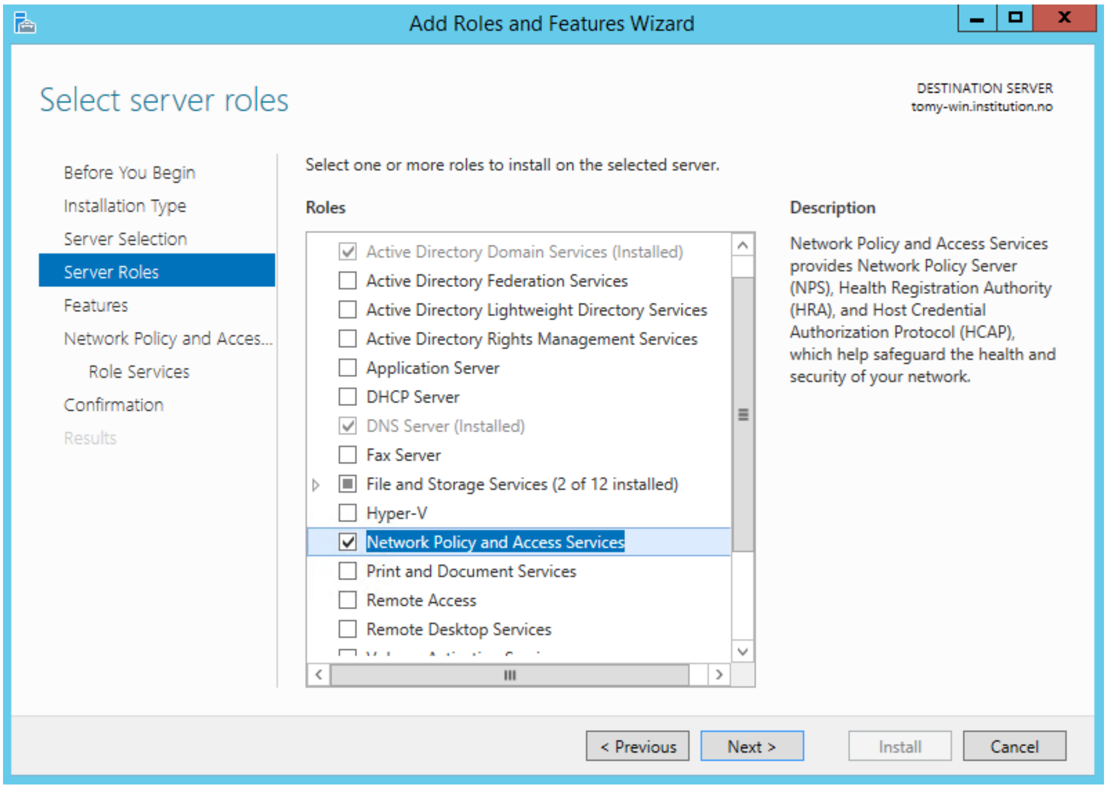
Filter:

Name	IP Address	Operating System
tomy-win.institution.no	158.38.213.102	Microsoft Windows Server 2012 R2 Datacenter

1 Computer(s) found

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

Select **Network Policy and Access Services** – then **Next**:



Select server roles

DESTINATION SERVER
tomy-win.institution.no

Select one or more roles to install on the selected server.

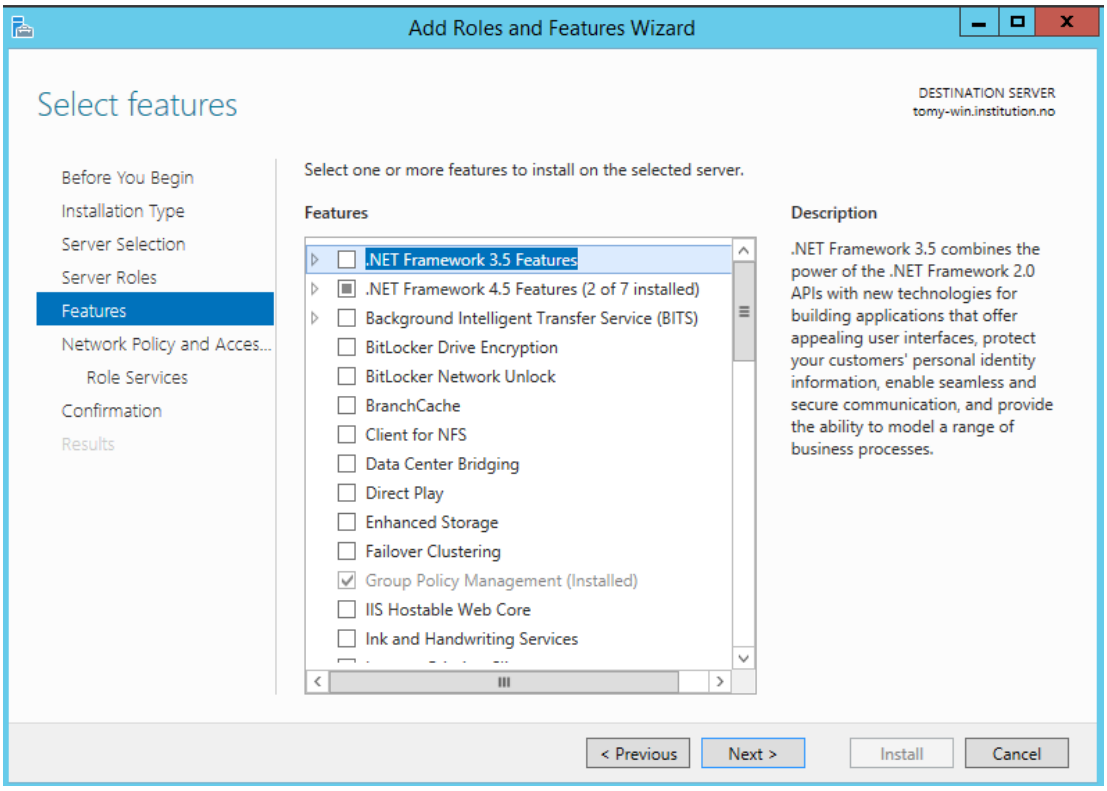
Roles

☑ 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 and Storage Services (2 of 12 installed)
□ Hyper-V
☑ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services

Description

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

Accept the defaults in the next three windows:


Add Roles and Features Wizard

Select features

DESTINATION SERVER
tomy-win.institution.no

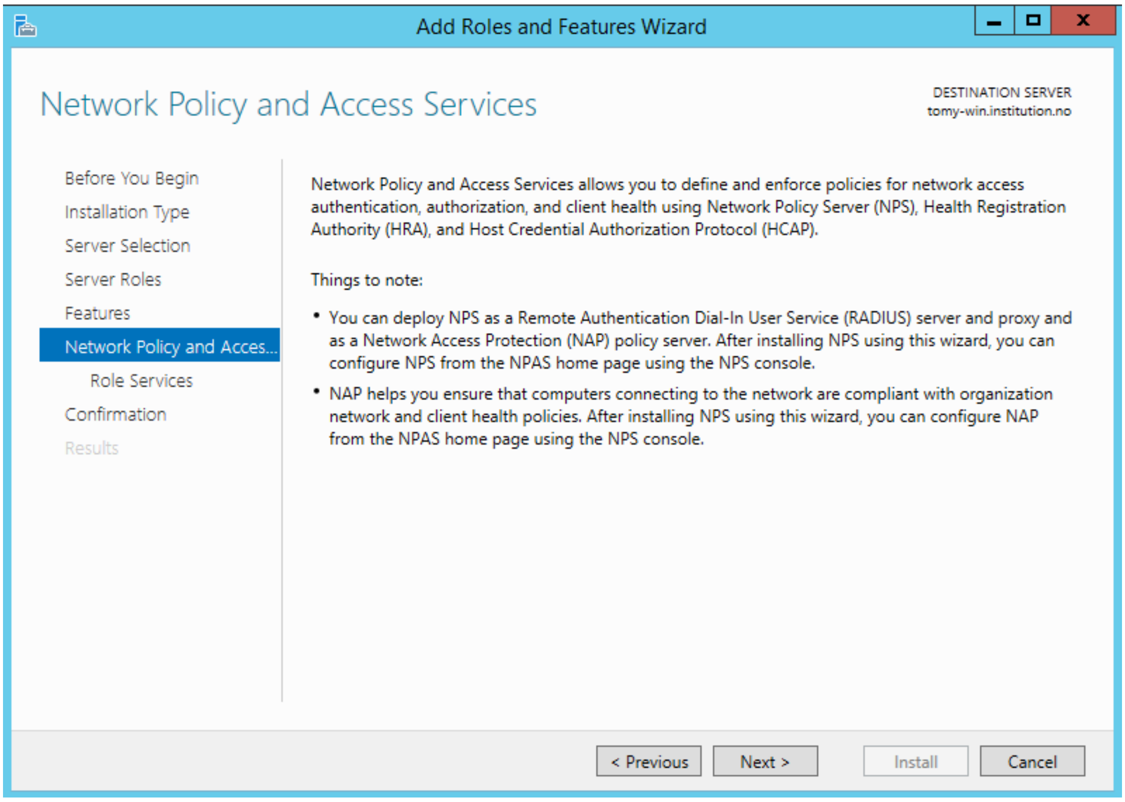
Select one or more features to install on the selected server.

Features

- □ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.


Add Roles and Features Wizard

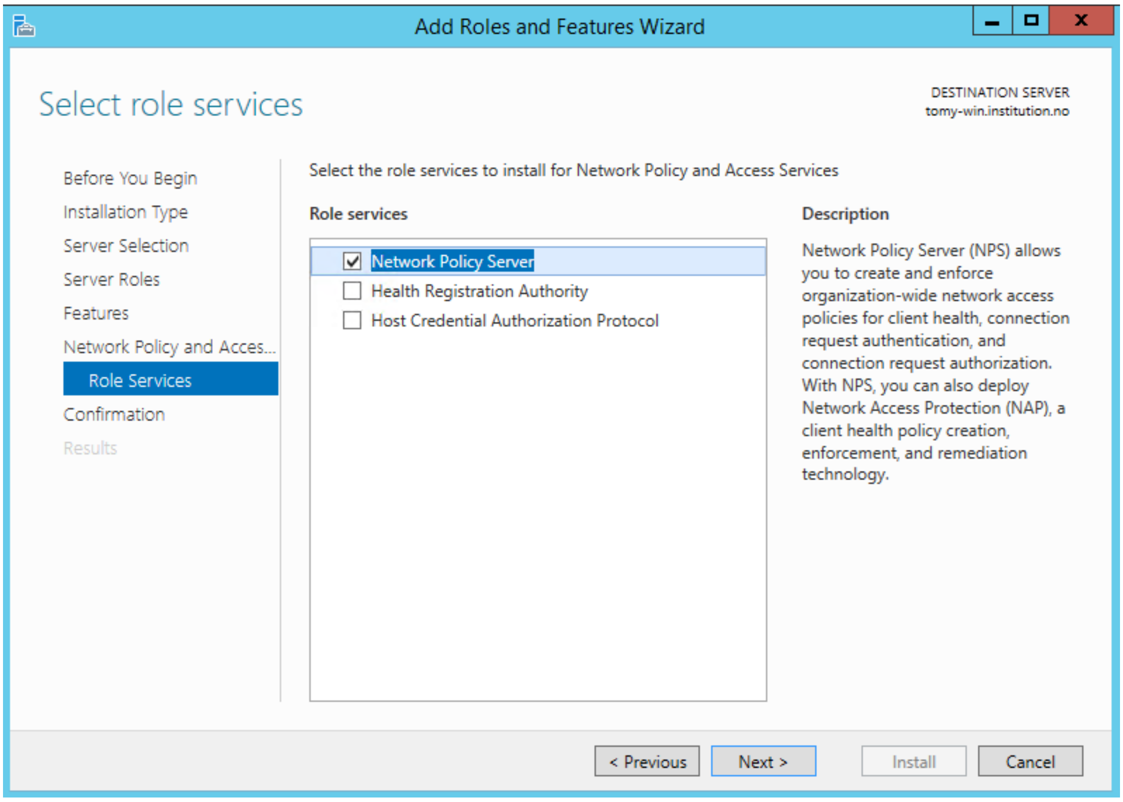
Network Policy and Access Services

DESTINATION SERVER
tomy-win.institution.no

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

Things to note:

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



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
tomy-win.institution.no

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

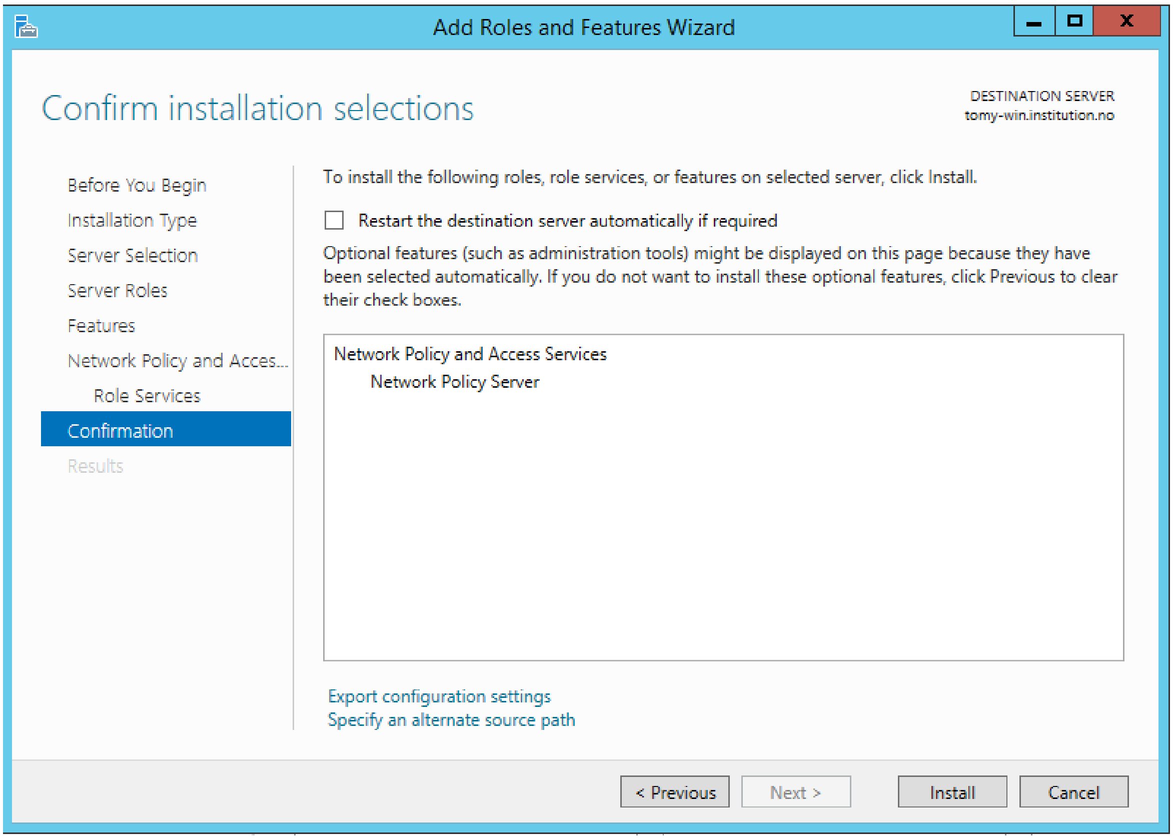
Role services

☑ Network Policy Server
□ 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.

Then **Install**:



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
tomy-win.institution.no

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

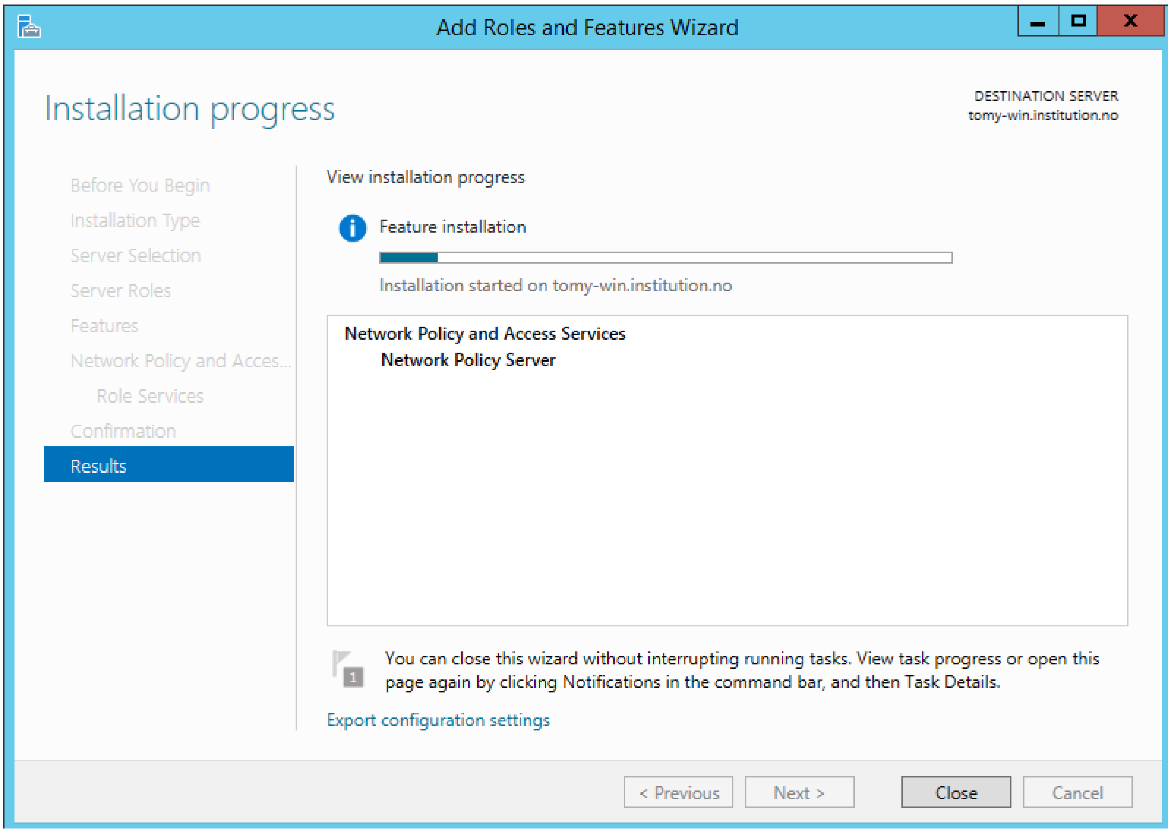
□ Restart the destination server automatically if required

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

Network Policy and Access Services
    Network Policy Server

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

And wait for the installation to finish – **Close**:



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
tomy-win.institution.no

View installation progress

Feature installation

Installation started on tomy-win.institution.no

Network Policy and Access Services
Network Policy Server

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

4 Server certificate for NPS

You need to have a Server Certificate in order to use PEAP-authentication with eduroam.

PEAP (Protected Extensible Authentication Protocol) 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. Firstly the authentication server needs to prove to the user that he or she will be providing credentials to the right authority, then the users need to prove who they are. So the RADIUS server (NPS in this case) will send its certificate to the client before authentication of the user takes place. The client must have previously installed the public certificate of the Certification Authority (CA) that has issued and signed the NPS server’s certificate. This may be distributed using e-mail, a web page such as eduroam CAT (eduroam Configuration Assistant Tool), or a management system such as AD. The client checks the validity of the RADIUS server’s certificate using the CA certificate. The client should also check the name of the certificate. Using a certificate from local CA, rather than certificates from a larger commercial CA, reduces the possibility of phishing.

Please see the TERENA confluence pages on EAP Server Certificate considerations [TERENA] for good information on this topic.

Without a certificate (self-signed or not) it’s not possible to do local authentication, but 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 are in doubt about your certificate), please read Appendix A ‘Certificates’.

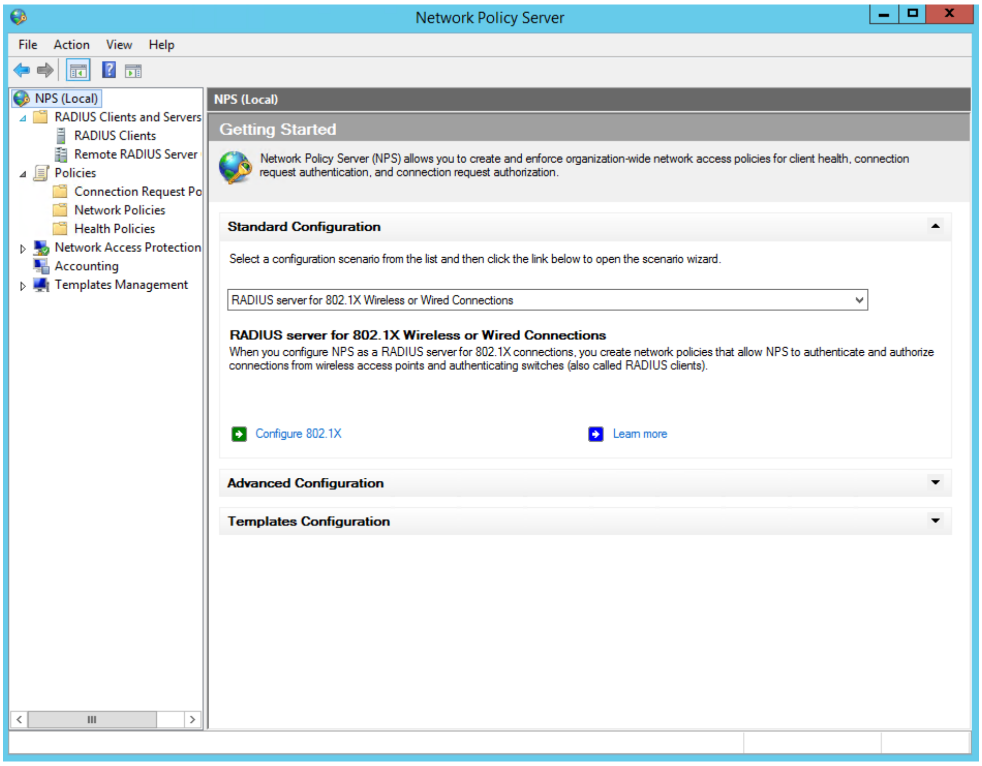
5 Configuring NPS

Open the NPS console (snap-in):

2012: In **Server Manager** > **Tools** > **Network Policy Server**

2008: **Start** > **Administrative Tools** > **Network Policy server**

A Wizard is available for configuring 802.1X Wireless or wired connections, see the next picture. You may use this for eduroam, but it does not provide all required settings (like realm/username pattern-matching) so you will need to make some changes in the created policies.



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.

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

RADIUS server for 802.1X Wireless or Wired Connections

RADIUS server for 802.1X Wireless or Wired Connections

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

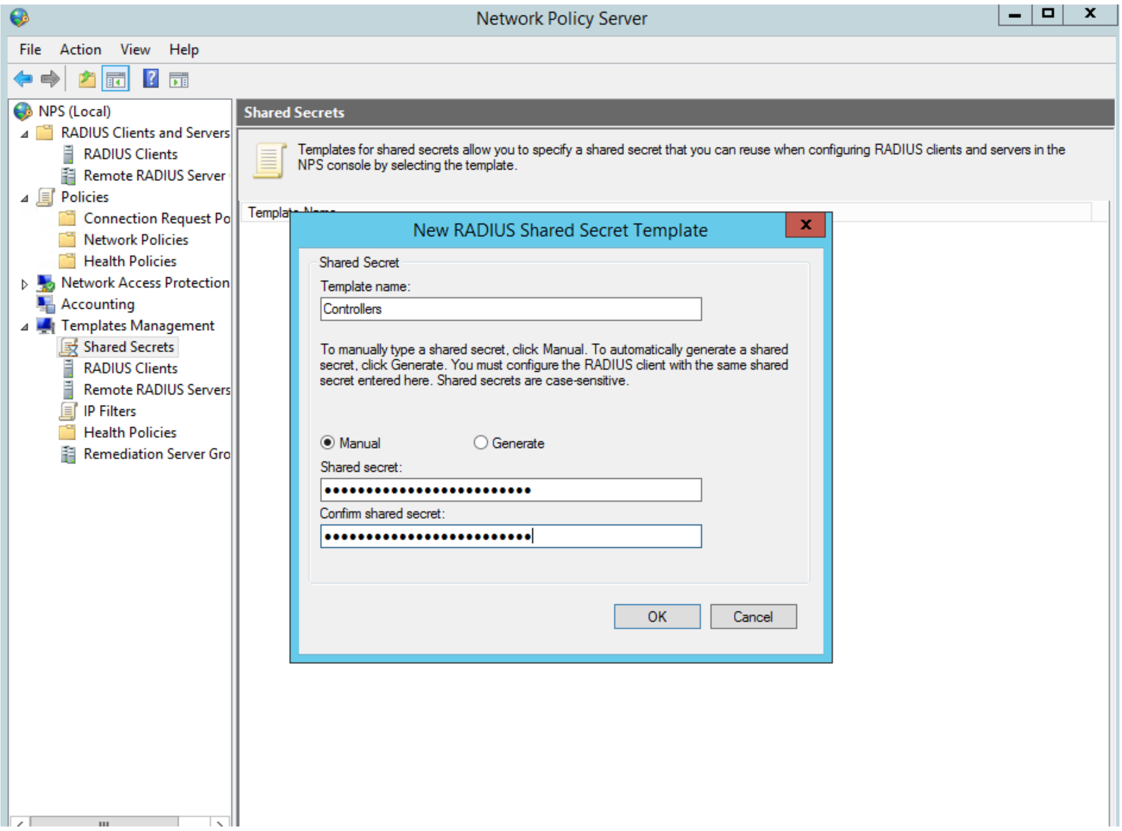
In these instructions RADIUS clients and servers, Connection Request and Network policies will be created separately i.e. not using the above Wizard.

5.1 Defining Clients and Servers

Before any policy can be applied to authentication requests we need to create RADIUS clients and servers. This is to allow wireless controllers (or Access Points) and the national proxy servers (they are all clients) to send requests to NPS and the national proxy servers to receive requests (now servers) from NPS.

If you have several controllers or Access Points that need to be defined as clients, it is recommended that you define a shared secret template first (it means you will re-use the same secret for all) and later apply this to each client, in this way avoiding mistyping problems.

Defining shared secret template:



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.

Template name: Controllers

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

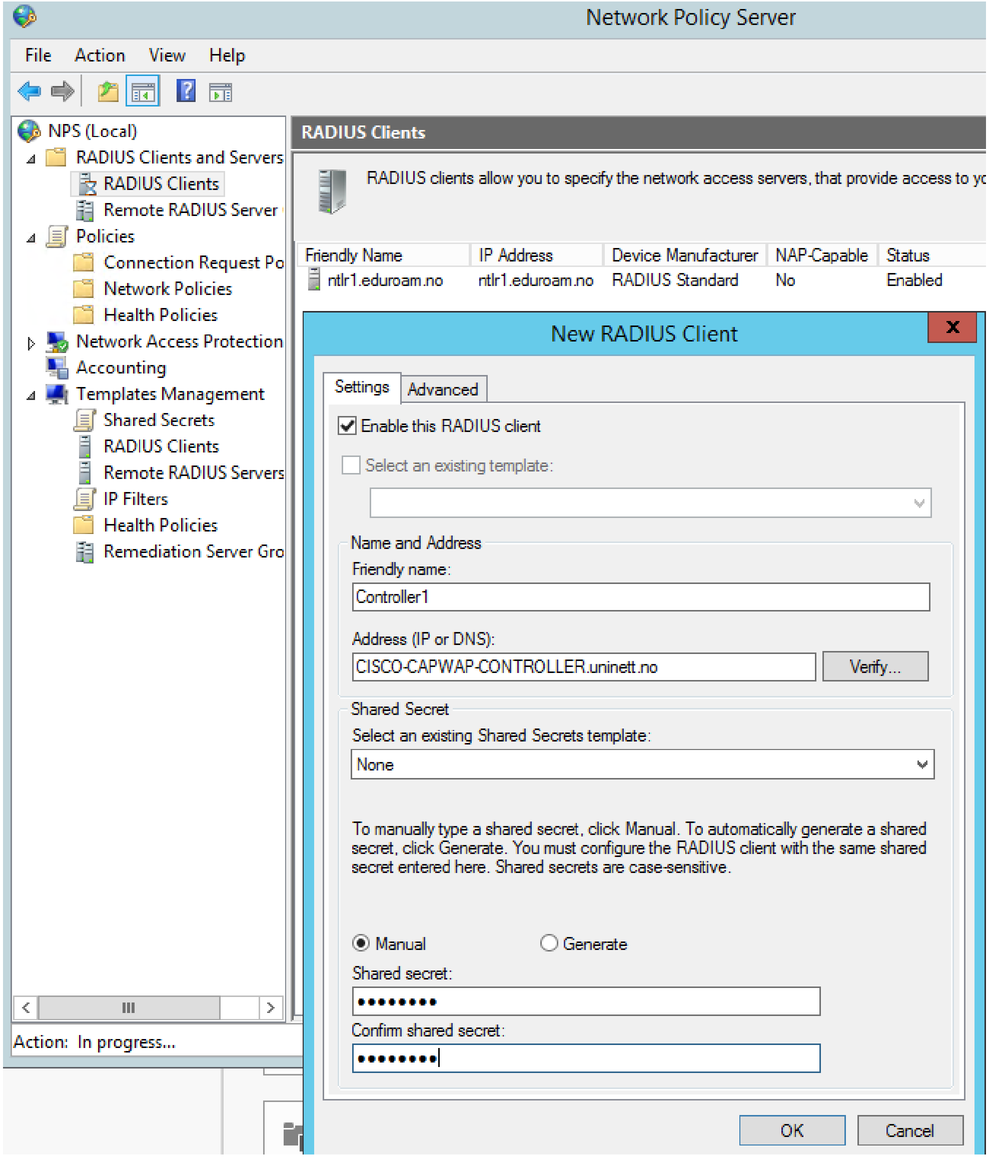
Shared secret: ••••••••••••••••••••••••

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

The above screen shows a template for Controllers; in addition you may create one for national proxy servers.

After creating the templates, create the Clients by right-clicking **RADIUS clients** and select **New**.

Enter a friendly name (it can later be referred to and used in pattern matching), IP address or DNS name and a shared secret (use the template if has been created). Details for national proxies must be agreed with your NRO.



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

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
ntlr1.eduroam.no	ntlr1.eduroam.no	RADIUS Standard	No	Enabled

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: Controller1

Address (IP or DNS): CISCO-CAPWAP-CONTROLLER.uninett.no

Shared Secret

Select an existing Shared Secrets template: None

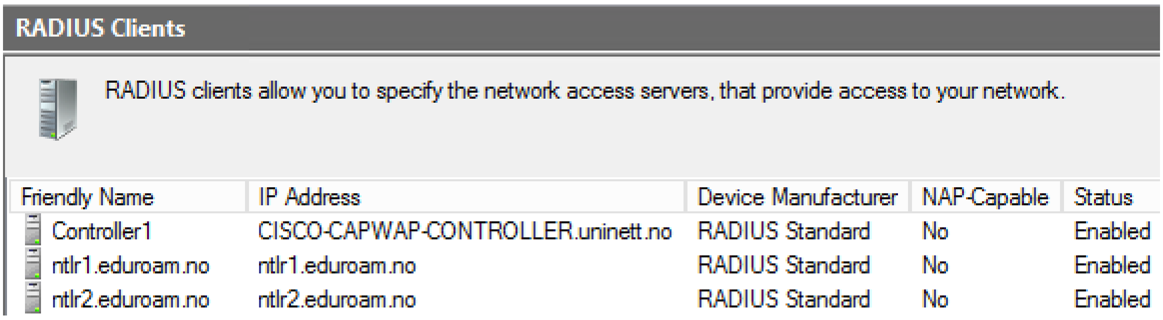
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••

Repeat the above until all needed clients are defined, together with at least two national proxies and one wireless controller.



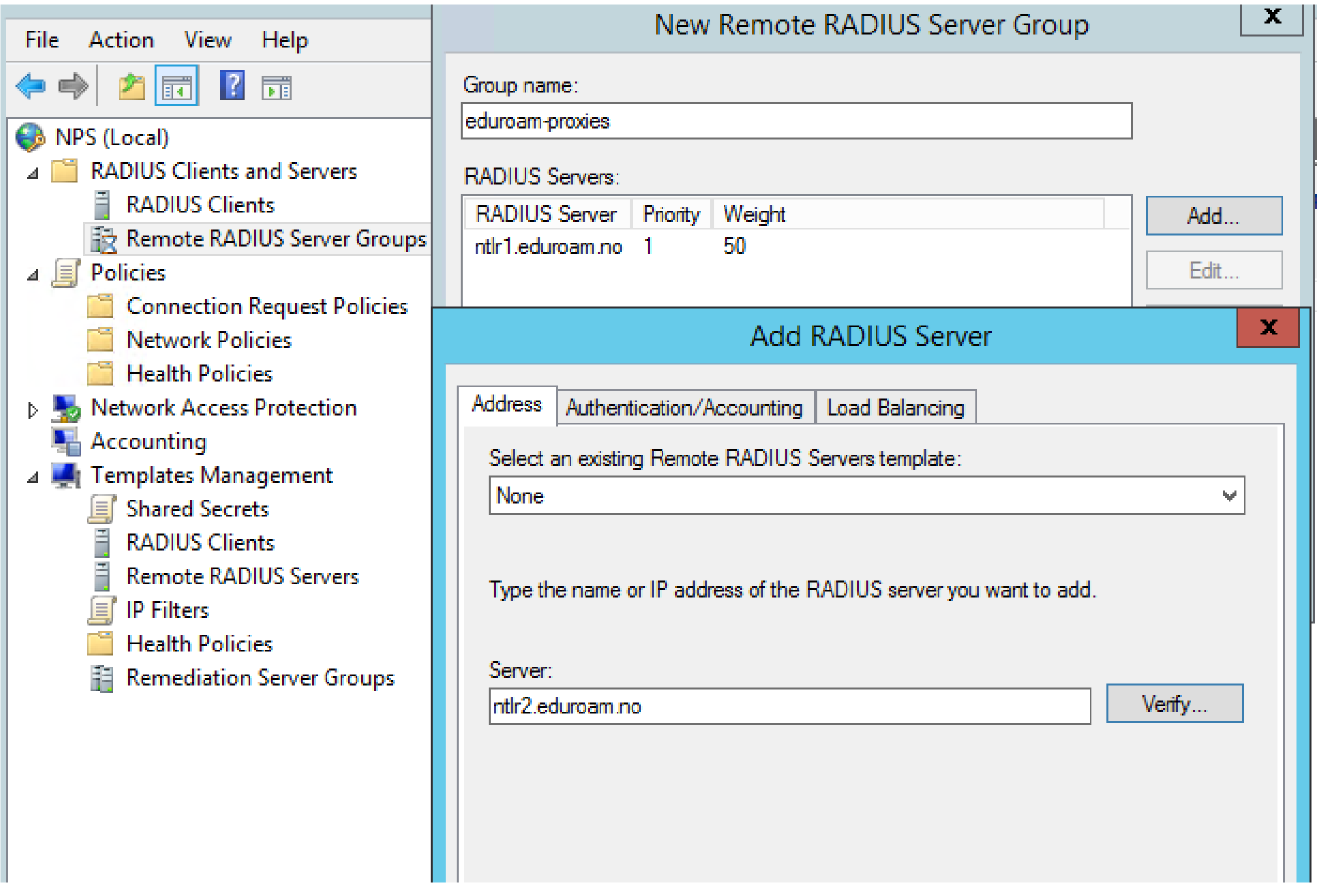
RADIUS Clients

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

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
Controller1	CISCO-CAPWAP-CONTROLLER.uninett.no	RADIUS Standard	No	Enabled
ntlr1.eduroam.no	ntlr1.eduroam.no	RADIUS Standard	No	Enabled
ntlr2.eduroam.no	ntlr2.eduroam.no	RADIUS Standard	No	Enabled

Next, create a server group for the proxy-servers, this will be used to send authentication requests from non-local users via proxies to their home institutions.

Right-click **Remote RADIUS Server Groups** and select **New**; enter a name for the server group e.g. “eduroam-proxies” then click **Add**:



Group name: eduroam-proxies

RADIUS Servers:

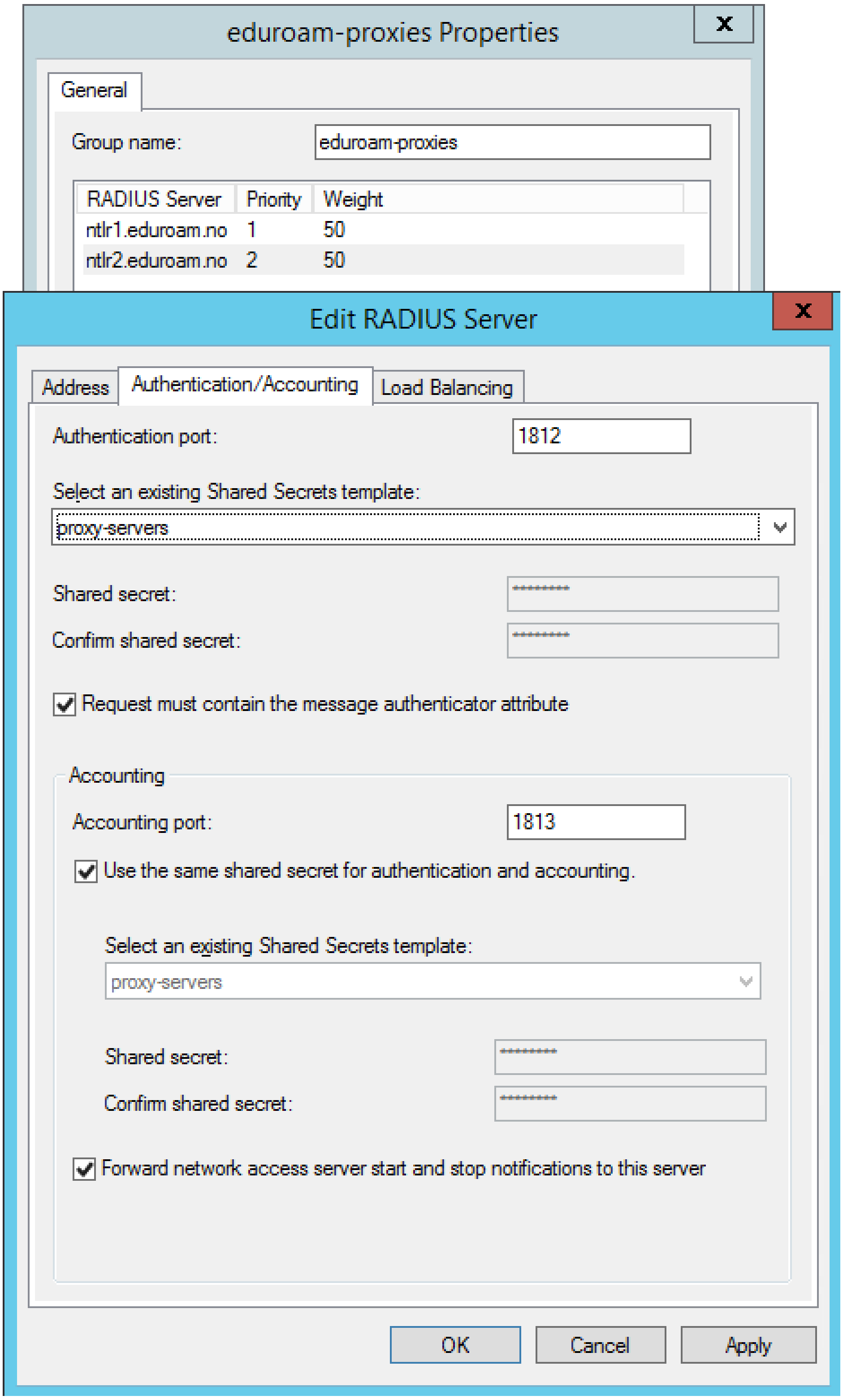
RADIUS Server	Priority	Weight
ntlr1.eduroam.no	1	50

Select an existing Remote RADIUS Servers template: None

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

Server: ntlr2.eduroam.no

Enter the name of the server (details from your NRO) and proceed to the Authentication/Accounting tab for the shared secret settings:



eduroam-proxies Properties

General

Group name: eduroam-proxies

RADIUS Server	Priority	Weight
ntlr1.eduroam.no	1	50
ntlr2.eduroam.no	2	50

Edit RADIUS Server

Address | Authentication/Accounting | Load Balancing

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

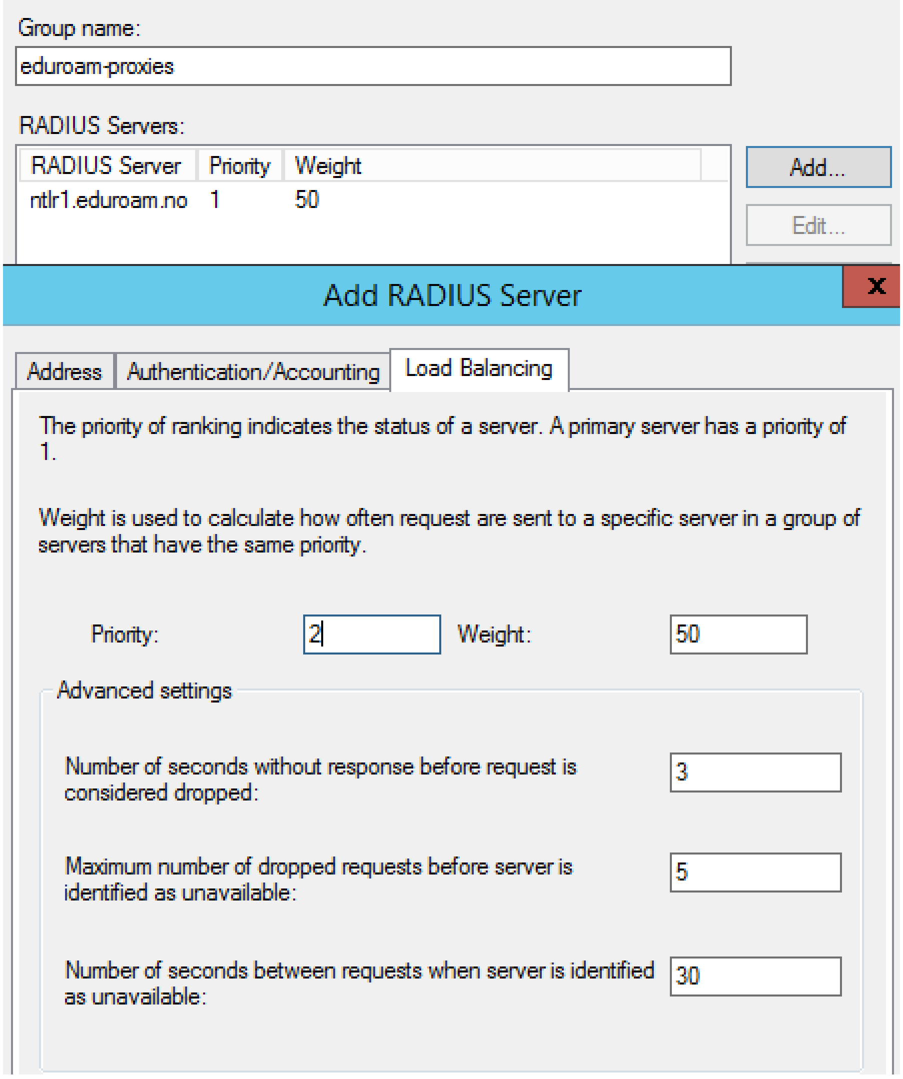
Shared secret: *********

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

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

Enter the shared secret as agreed with the NRO (manually or by choosing the defined template).

For the secondary server, consider also the last tab "Load Balancing". It is 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 will work, but good practice is setting it to a lower priority meaning it will only be used for failover.



Group name: eduroam-proxies

RADIUS Servers:

RADIUS Server	Priority	Weight
ntlr1.eduroam.no	1	50

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

Finish by clicking OK twice.

5.2 Creating policies

Two types of policies are used with NPS: "Connection Request Policies" and "Network Policies". When a request is received, it is first matched against Connection Request Policies, if the resulting match says "local authentication" the request is also matched against "Network Policies". The order of Policies is important, once conditions are met processing of Policies are stopped. You can move policy rules up and down, and disable rules. The two policy types can do much of the same condition matching and settings. The following details a set of policies that will work with eduroam, but is not the only possible way to achieve the same result.

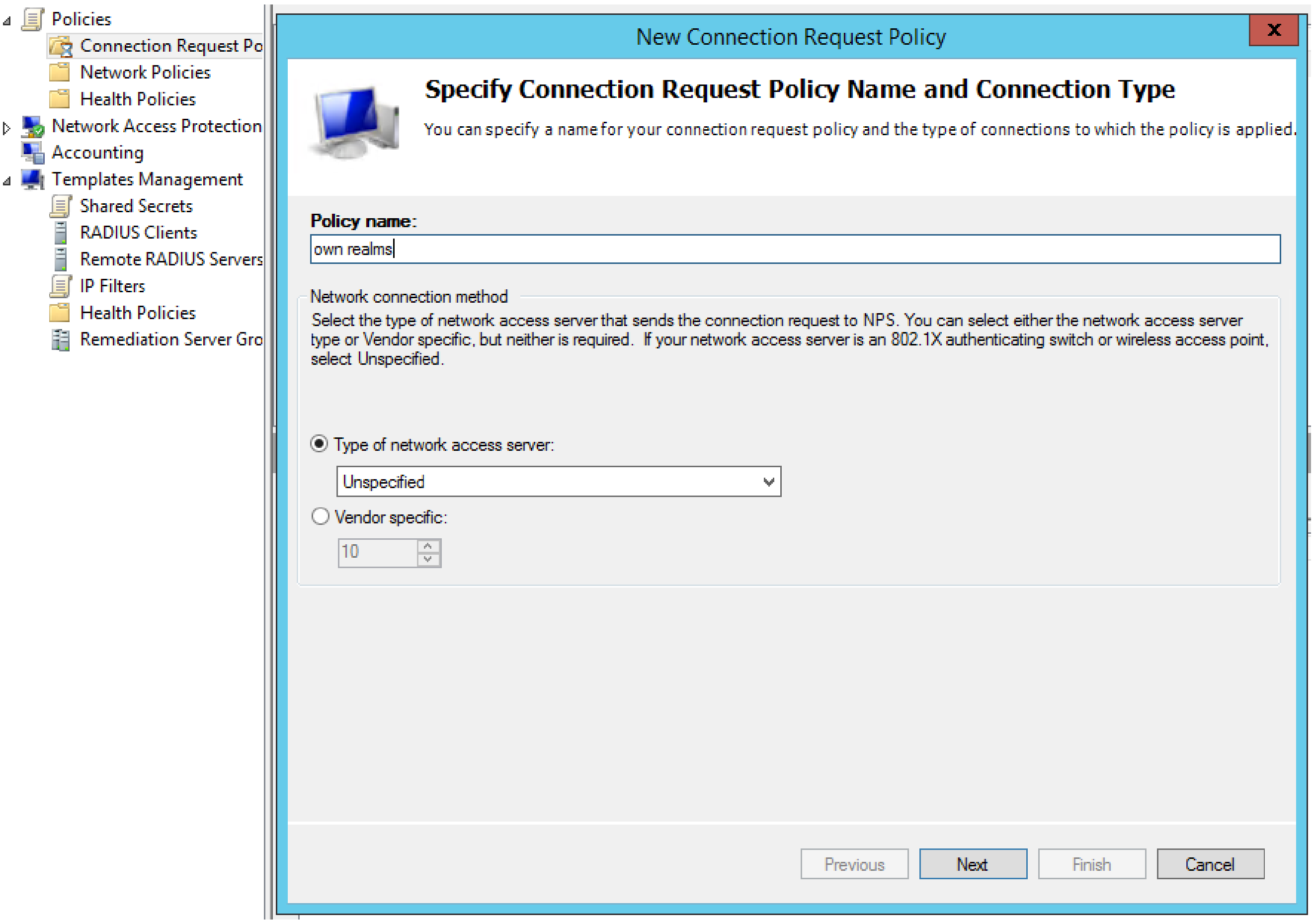
5.2.1 Connection Request Policies

The “Connection Request Policies” decide what to do with an authentication request, either by forwarding it to a proxy-server or by authenticating locally. The decision is based on conditions set in a policy such as RADIUS attributes (e.g. User Name), RADIUS client IP-address (or friendly name) and several other options, when conditions are matched to the settings of that particular policy. For eduroam we only need two Connection Request Policies, in this order:

1. Authenticate own realms “your-realm.tld” locally (use Network Policies)
2. Forward eduroam visitors to eduroam proxy-servers.

The following screens show how to create the two Connection Request Policies:

Right click **Connection Request Policies** – Select **New**.



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:
own 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:

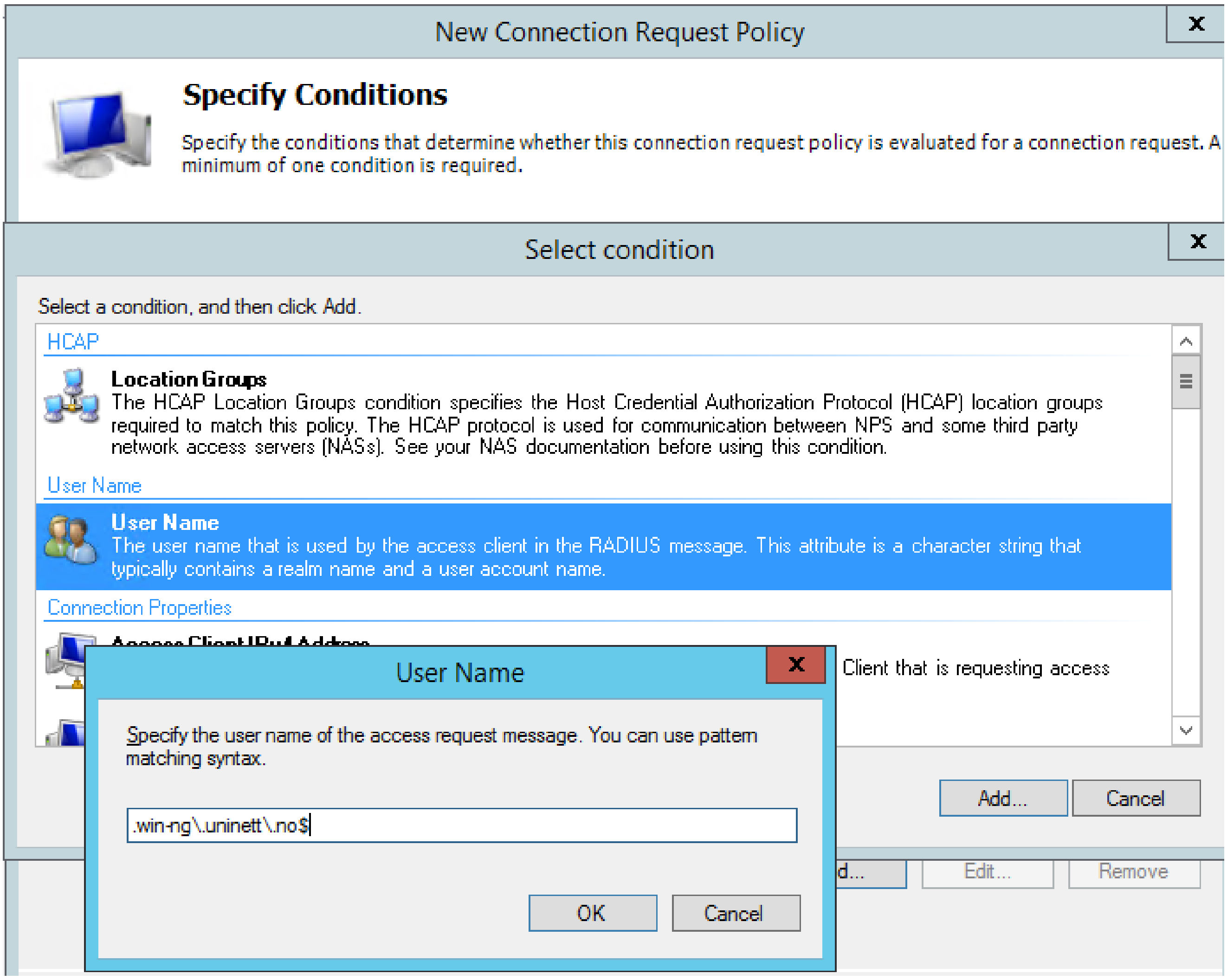
Unspecified

○ Vendor specific:

10

Enter a Policy name (e.g. **own realms**) – click **Next**

Click **Add** – to enter a condition, Select **User Name** and click **Add**: (in the example below, our realm is **win-ng.uninett.no**)



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

User Name

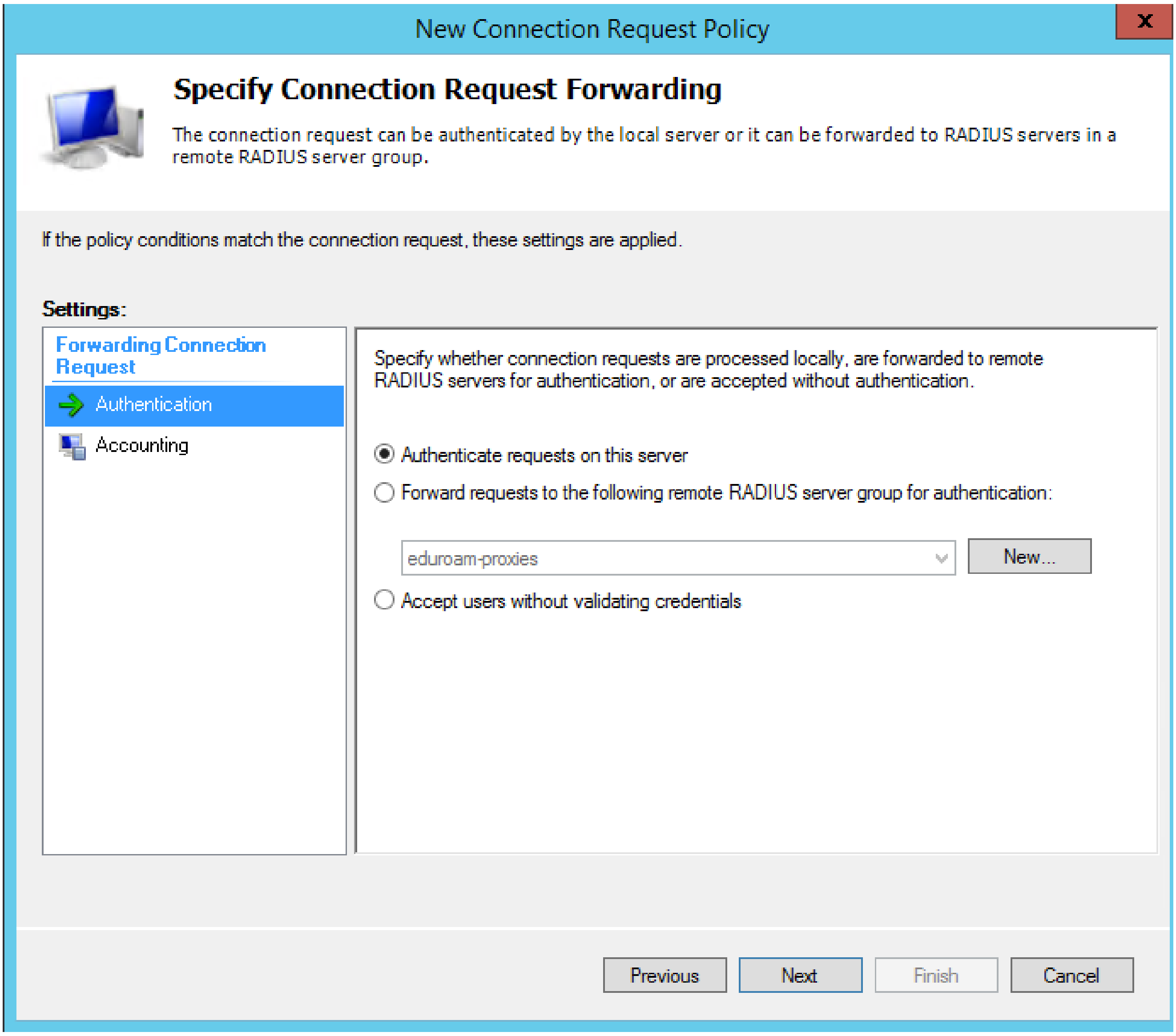
Specify the user name of the access request message. You can use pattern matching syntax.

.win-ng\.uninett\.no$

Enter the username pattern to match for then press **OK**.

Note: See [PATTERN] for pattern matching syntax. Here we match for any username ending with "win-ng.uninett.no", this includes possible sub-realms as student.win-ng.uninett.no.

Then click **Next**.



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:

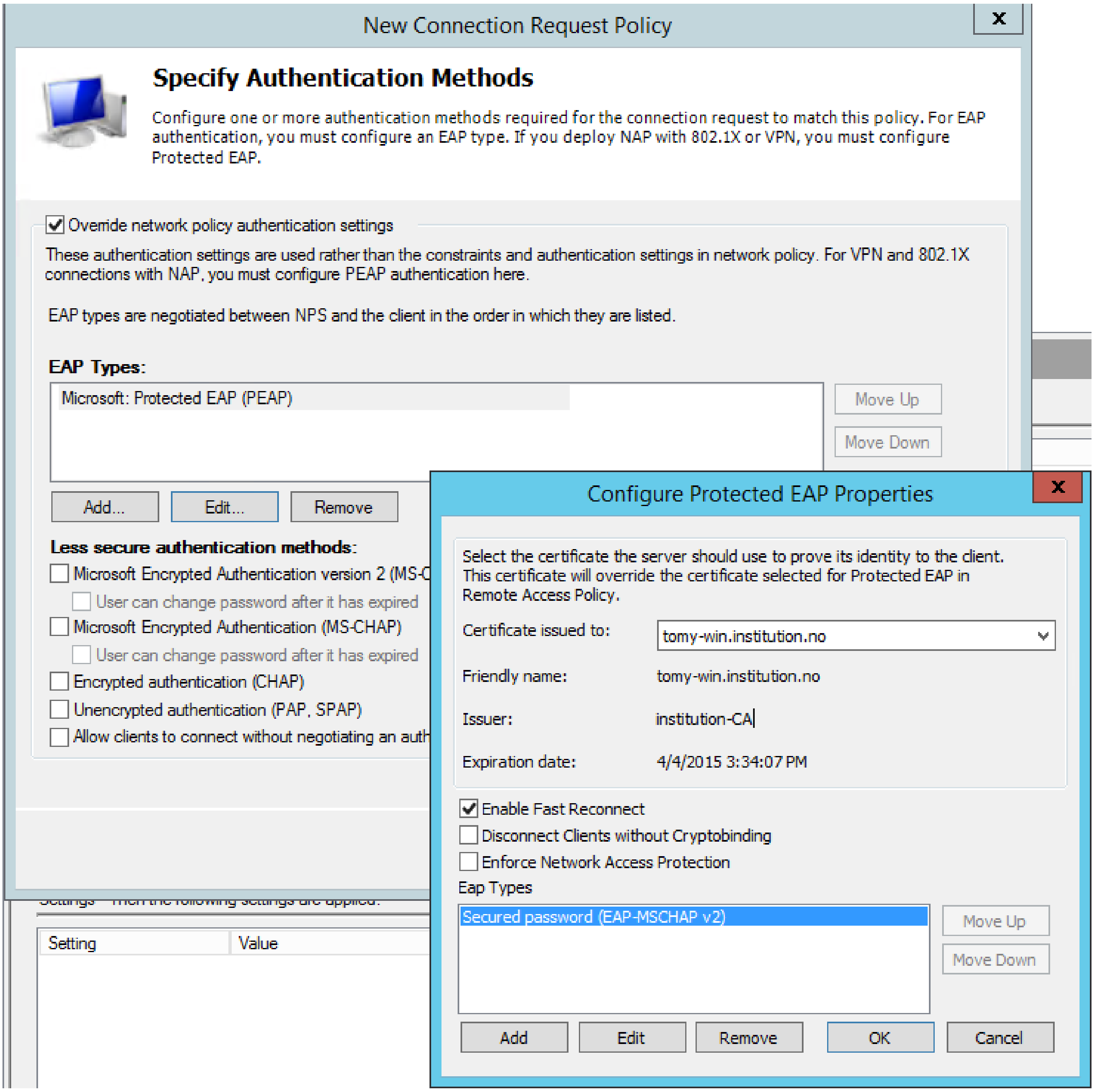
eduroam-proxies

○ Accept users without validating credentials

Authenticate on this server – click **Next**.

Select “Override network policy authentication settings” and click **Add** to add PEAP as EAP, select **OK**.

Mark “Microsoft: Protected EAP (PEAP)” and click **Edit …**:



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:

Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-C

□ 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 auth

Configure Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. This certificate will override the certificate selected for Protected EAP in Remote Access Policy.

Certificate issued to: tomy-win.institution.no

Friendly name: tomy-win.institution.no

Issuer: institution-CA

Expiration date: 4/4/2015 3:34:07 PM

☑ Enable Fast Reconnect

□ Disconnect Clients without Cryptobinding

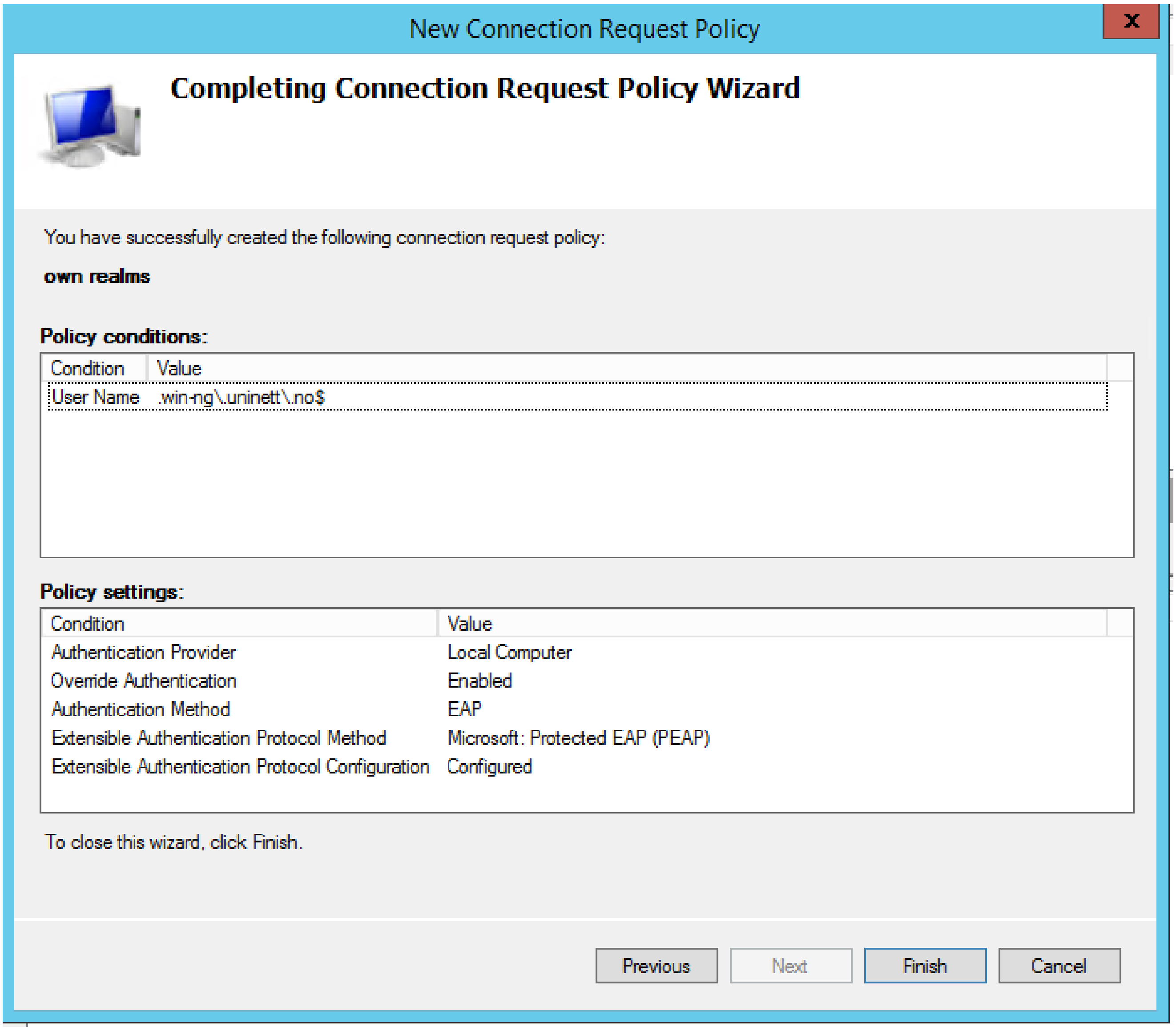
□ Enforce Network Access Protection

Eap Types

Secured password (EAP-MSCHAP v2)

Select the previously installed server certificate (above is just an example) and deselect “Enforce Network Access Protection”. Then click **OK**, followed by **Next** twice.

Check configuration:



Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

own realms

Policy conditions:

Condition	Value
User Name	.win-ng\.uninett\.no$

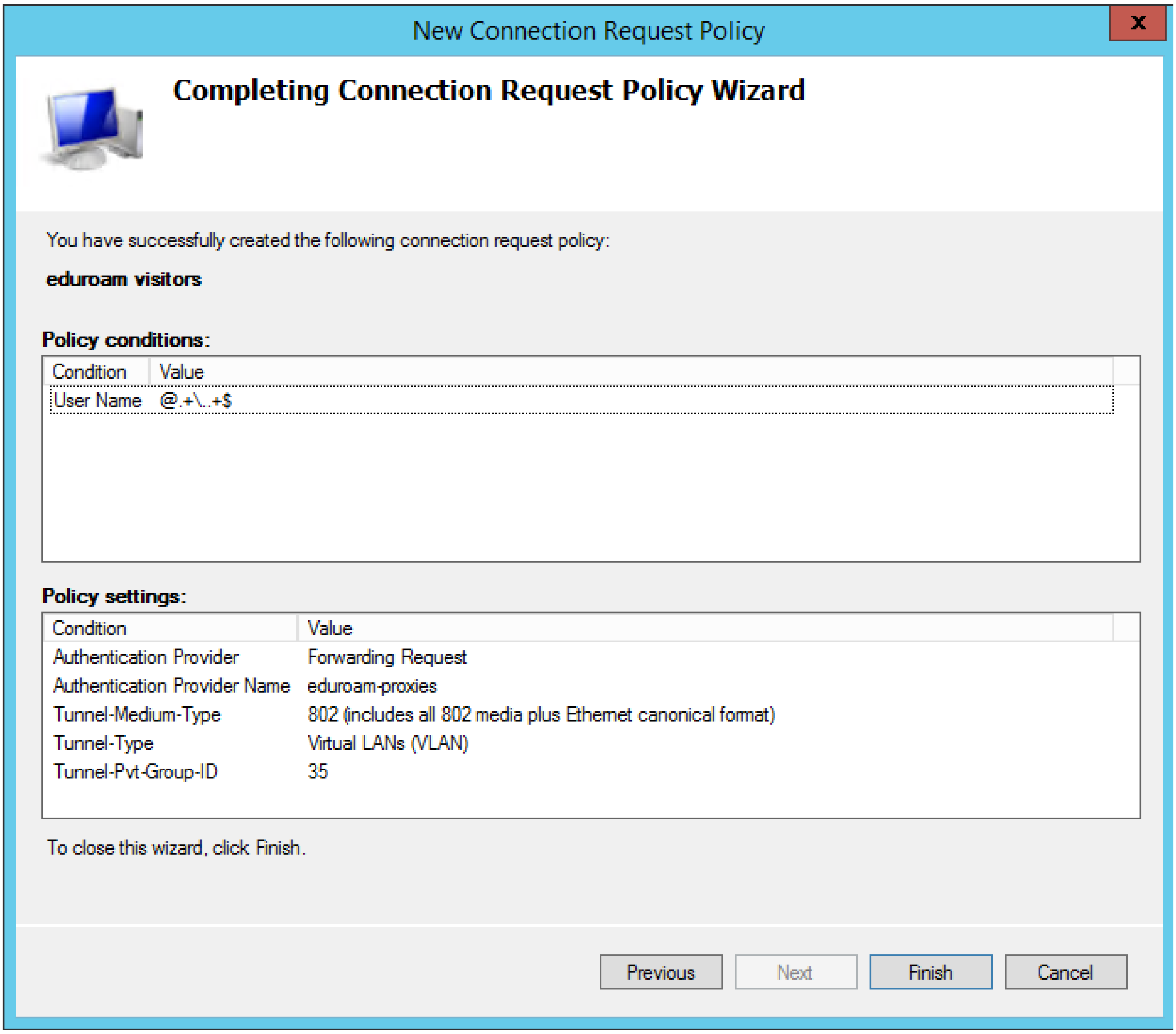
Policy settings:

Condition	Value
Authentication Provider	Local Computer
Override Authentication	Enabled
Authentication Method	EAP
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
Extensible Authentication Protocol Configuration	Configured

To close this wizard, click Finish.

Click **Finish**.

Next, you need the Connection Request Policy to forward requests to the national proxy servers – Add new policy as above with the following settings:



Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

eduroam visitors

Policy conditions:

Condition	Value
User Name	@.+\..+$

Policy settings:

Condition	Value
Authentication Provider	Forwarding Request
Authentication Provider Name	eduroam-proxies
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Pvt-Group-ID	35

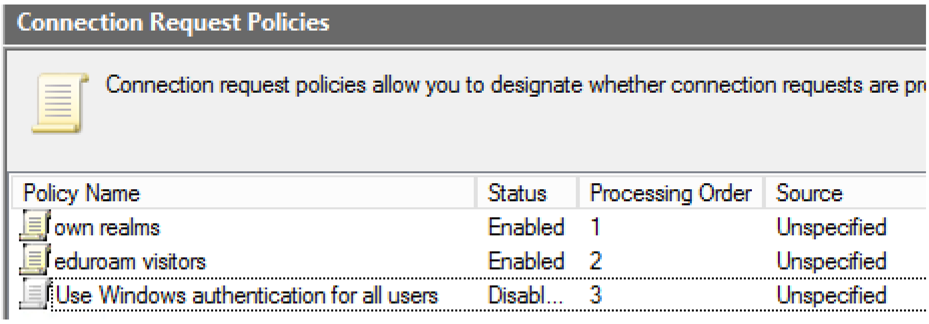
To close this wizard, click Finish.

Note:

Pattern matching used is for any realm of the form “@something.something”, another option is to use “@.+\.[a-z]{2,6}$” which is a case-insensitive match for realms ending in “@something.tld” where tld is between 2 to 6 letters.

In the above example, eduroam visitors are placed into VLAN 35 by setting the attributes Tunnel-Medium-Type, Tunnel-Type and Tunnel-Pvt-Group-ID. This can be omitted if you would like your eduroam visitors placed in the default VLAN for your eduroam SSID as configured on the wireless controller (or Access Points). It is however good practise to also include the VLAN setting here; it will overwrite attributes returned from the IdP. (Some do even if they should not!). For placing local users into specific VLANs we will use Network Policies (see later).

Make sure your Connection Request Policies are processed in this order:



Connection Request Policies

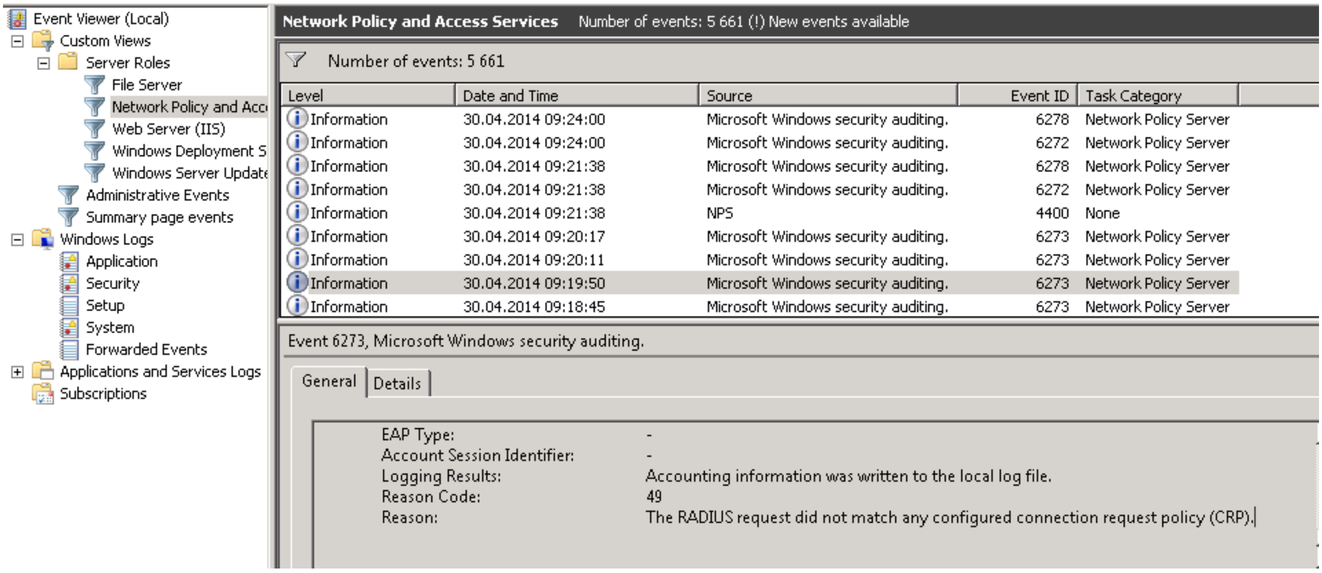
Connection request policies allow you to designate whether connection requests are pr

Policy Name	Status	Processing Order	Source
own realms	Enabled	1	Unspecified
eduroam visitors	Enabled	2	Unspecified
Use Windows authentication for all users	Disabl...	3	Unspecified

Note:

The original policy “Use Windows authentication for all users” should be deleted or disabled. Please do not have it enabled! (This policy would catch users without a realm included in their username and could actually work for authenticating your own users, but eduroam will not work for such users at other eduroam locations).

With just the above two policies enabled, a username without a realm will give an entry in your Event Viewer similar to the following example (also revealing the username):



Network Policy and Access Services Number of events: 5 661 (!) New events available

Number of events: 5 661

Level	Date and Time	Source	Event ID	Task Category
Information	30.04.2014 09:24:00	Microsoft Windows security auditing.	6278	Network Policy Server
Information	30.04.2014 09:24:00	Microsoft Windows security auditing.	6272	Network Policy Server
Information	30.04.2014 09:21:38	Microsoft Windows security auditing.	6278	Network Policy Server
Information	30.04.2014 09:21:38	Microsoft Windows security auditing.	6272	Network Policy Server
Information	30.04.2014 09:21:38	NPS	4400	None
Information	30.04.2014 09:20:17	Microsoft Windows security auditing.	6273	Network Policy Server
Information	30.04.2014 09:20:11	Microsoft Windows security auditing.	6273	Network Policy Server
Information	30.04.2014 09:19:50	Microsoft Windows security auditing.	6273	Network Policy Server
Information	30.04.2014 09:18:45	Microsoft Windows security auditing.	6273	Network Policy Server

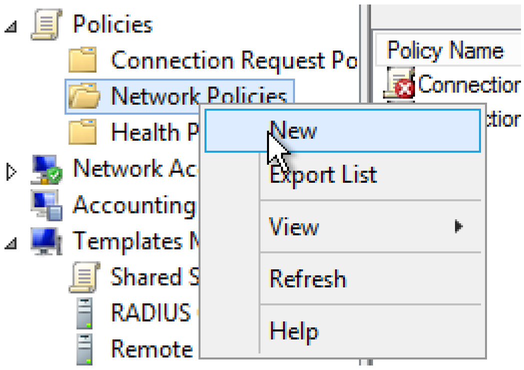
Event 6273, Microsoft Windows security auditing.

```
EAP Type:                    -
Account Session Identifier:  -
Logging Results:             Accounting information was written to the local log file.
Reason Code:                 49
Reason:                      The RADIUS request did not match any configured connection request policy (CRP).
```

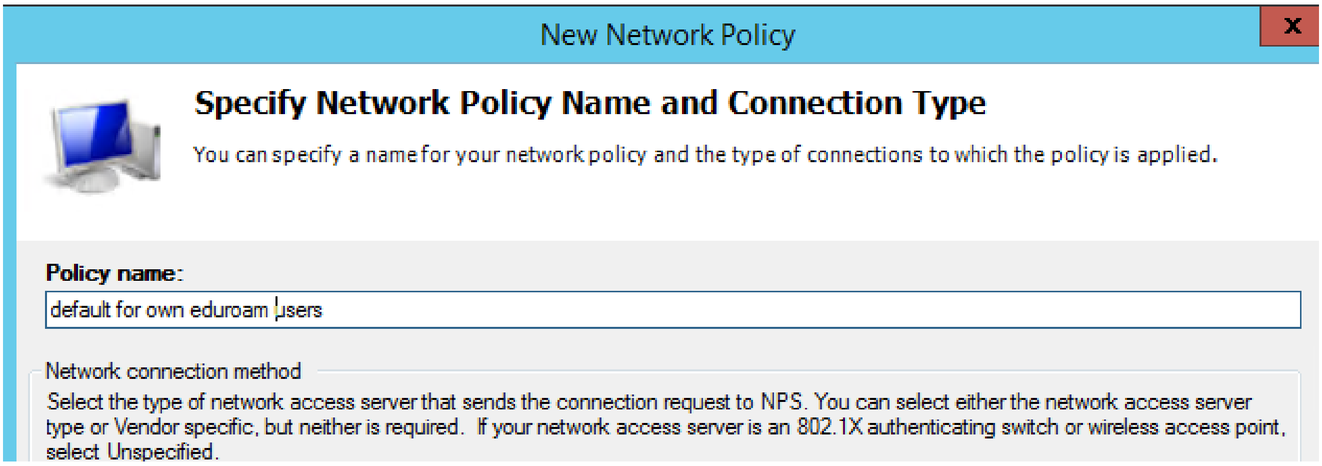
eduroam visitors should now be able to connect from your site. Check if possible as a guest at your institution.

5.2.2 Network Policies.

“Network Policies” are applied to requests that are to be authenticated locally. (As decided in the Connection Request Policy). In a very basic setup, only one Network Policy is needed, so first we create this policy:



Give your policy a name such as “default for own eduroam users”:



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:

default for own eduroam users

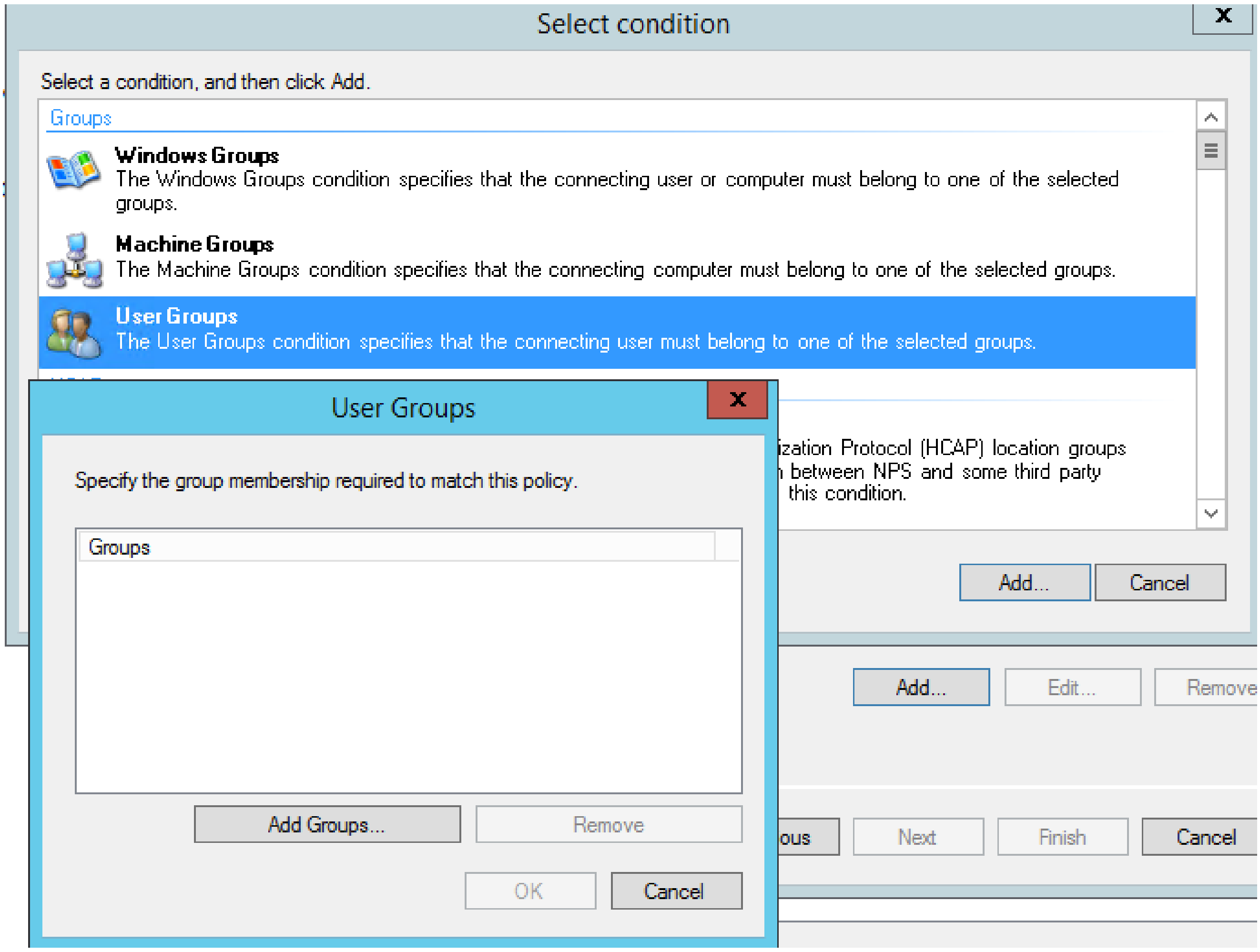
Network connection method

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.

Click **Next**

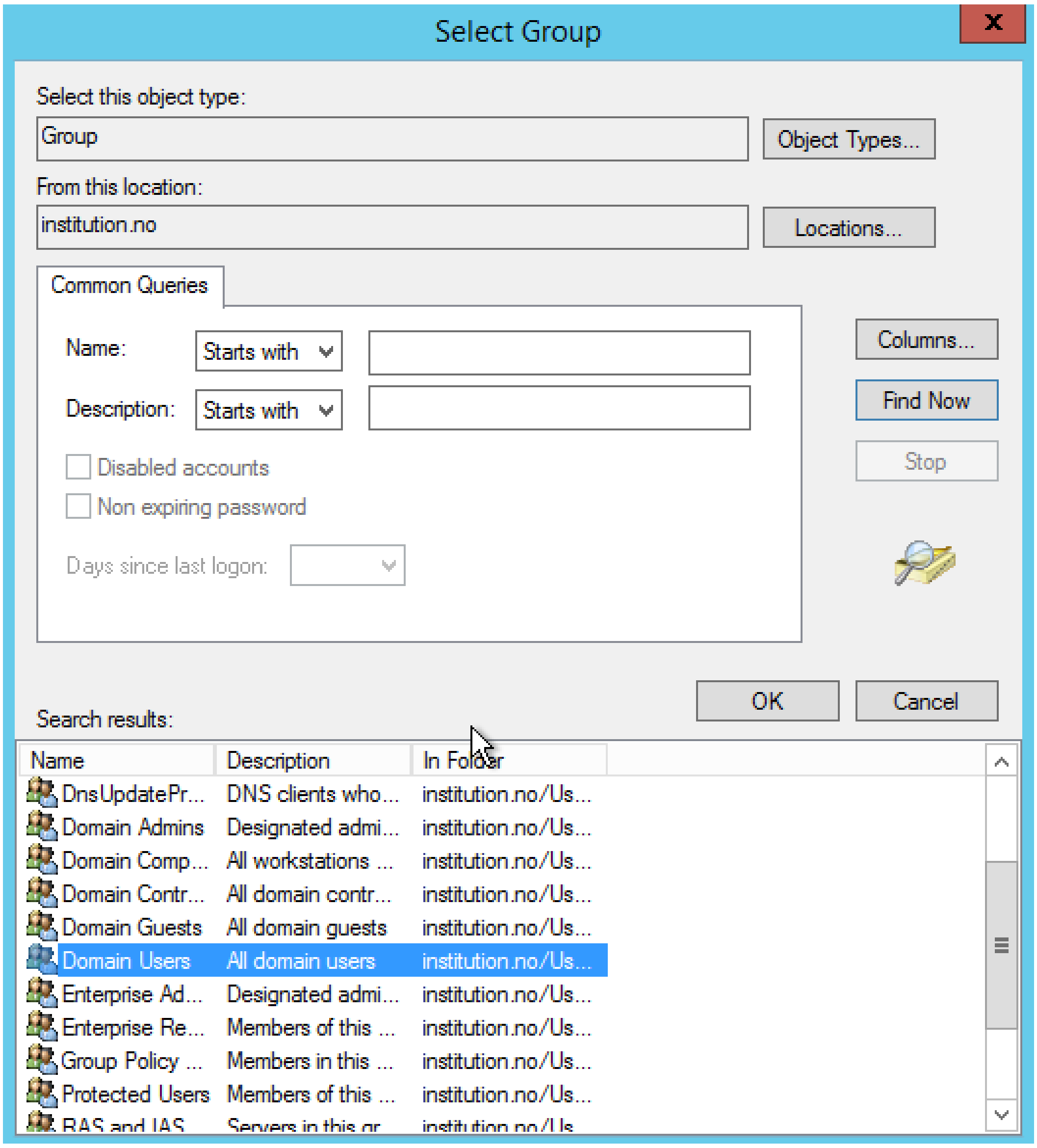
Then click **Add**, to specify the conditions for matching this request.

Here you define the User Group in your AD that are allowed to authenticate. So select **UserGroups** and click **Add**.



Select condition
Select a condition, and then click Add.
Groups
Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
ization Protocol (HCAP) location groups
between NPS and some third party
this condition.
Add...
Cancel
User Groups
Specify the group membership required to match this policy.
Groups
Add Groups...
Remove
OK
Cancel
Add...
Edit...
Remove
ous
Next
Finish
Cancel

Click **Add Groups ...** > **Advanced** > **Find Now**. This gives a list to choose from:



Select this object type: Group

From this location: institution.no

Name: Starts with

Description: Starts with

□ Disabled accounts

□ Non expiring password

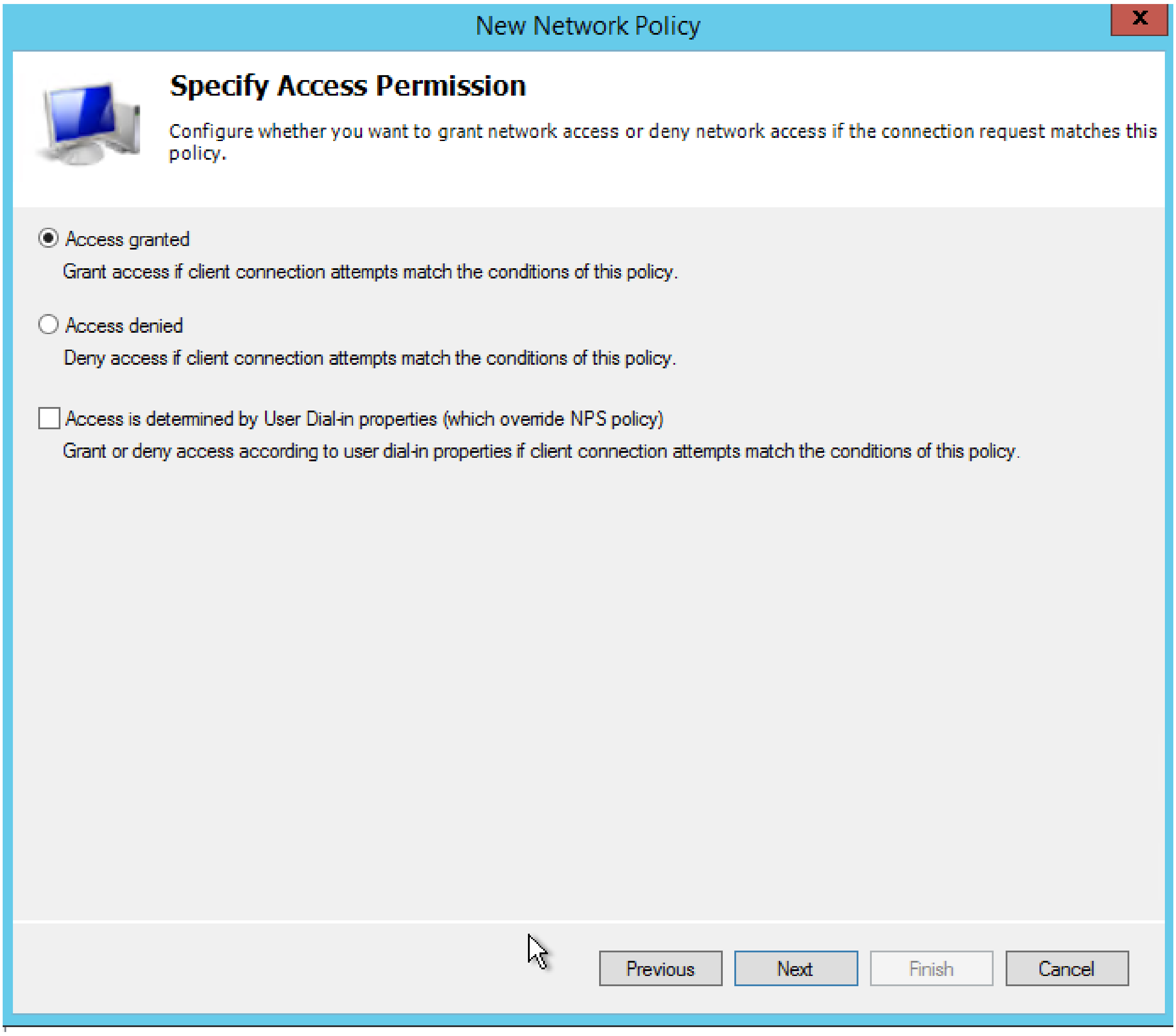
Days since last logon:

Search results:

Name	Description	In Folder
DnsUpdatePr...	DNS clients who ...	institution.no/Us...
Domain Admins	Designated admi...	institution.no/Us...
Domain Comp...	All workstations ...	institution.no/Us...
Domain Contr...	All domain contr...	institution.no/Us...
Domain Guests	All domain guests	institution.no/Us...
Domain Users	All domain users	institution.no/Us...
Enterprise Ad...	Designated admi...	institution.no/Us...
Enterprise Re...	Members of this ...	institution.no/Us...
Group Policy ...	Members in this ...	institution.no/Us...
Protected Users	Members of this ...	institution.no/Us...
RAS and IAS	Servers in this gr...	institution.no/Us...

Here “All domain users” are selected as an example. You could establish a group just for eduroam users.

Click **OK** three times to get back to Specify Condition for the new Network Policy. Click **Next**.



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.

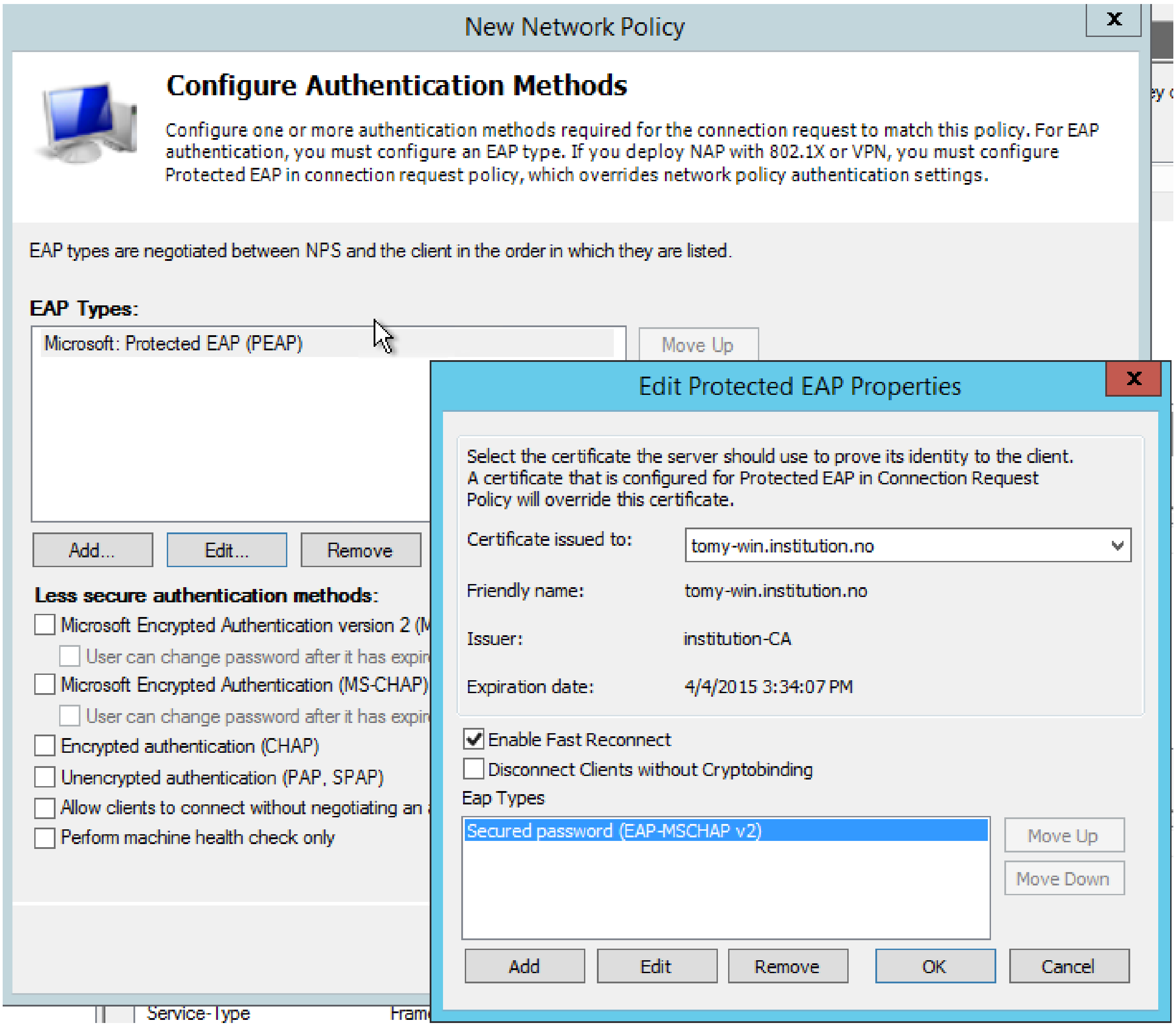
○ Access denied

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.

Click **Next.**



New Network Policy

Configure Authentication Methods

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

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

EAP Types:

Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

- □ Microsoft Encrypted Authentication version 2 (M
  - □ User can change password after it has expir
- □ Microsoft Encrypted Authentication (MS-CHAP)
  - □ User can change password after it has expir
- □ Encrypted authentication (CHAP)
- □ Unencrypted authentication (PAP, SPAP)
- □ Allow clients to connect without negotiating an a
- □ 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 to: tomy-win.institution.no

Friendly name: tomy-win.institution.no

Issuer: institution-CA

Expiration date: 4/4/2015 3:34:07 PM

☑ Enable Fast Reconnect

□ Disconnect Clients without Cryptobinding

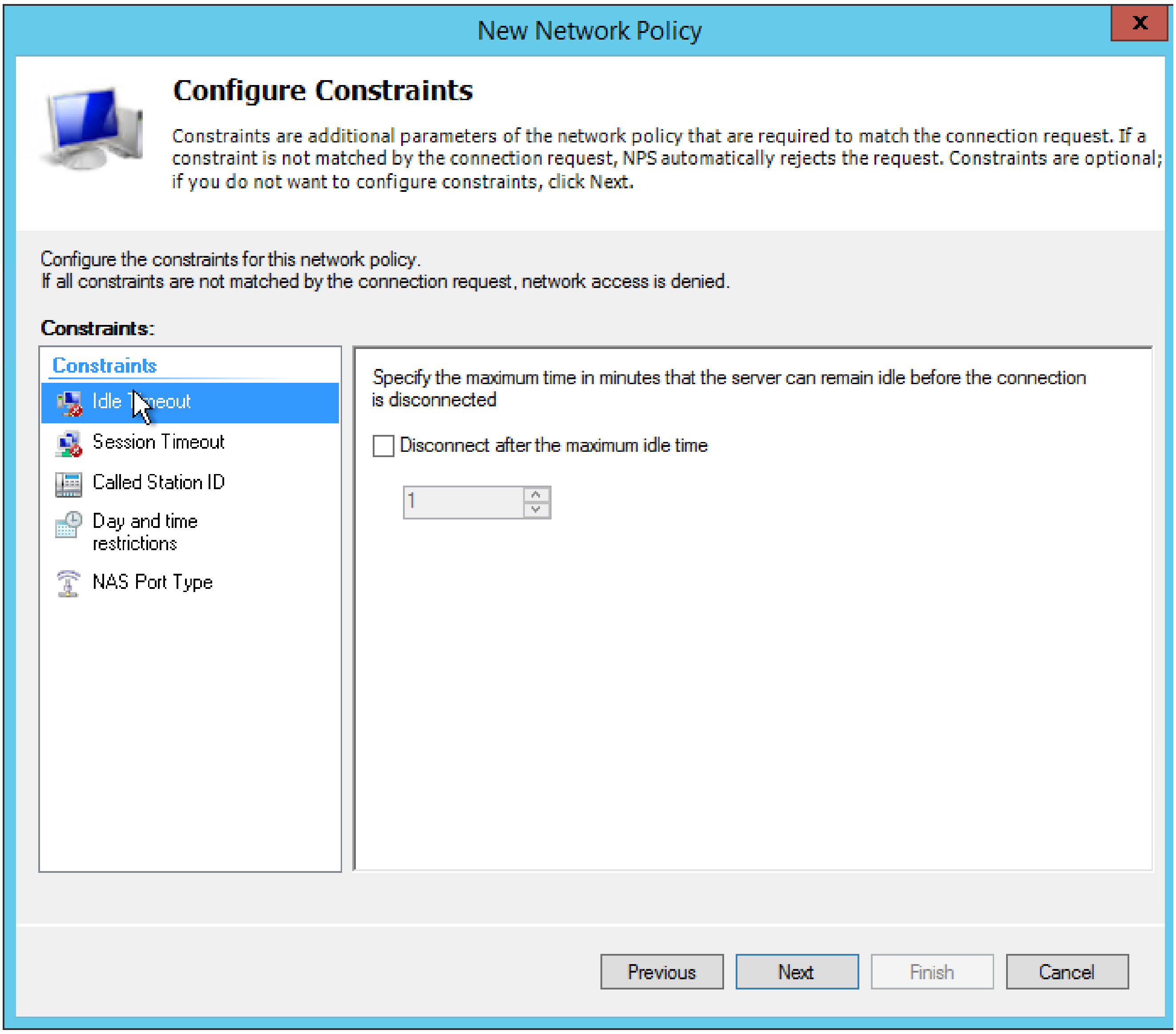
Eap Types

Secured password (EAP-MSCHAP v2)

De-select all “Less secure authentication methods” and Add “Microsoft: Protected EAP (PEAP)”, just as you did for the Connection Request Policy.

Note: PEAP (and certificate to use) was configured in **Connection Request Policy to Override Network Policies** for all local realms, so this setting should never be used. However since an authentication method must be set – we choose to select the most secure.

Click **OK** – then **Next**.



New Network Policy

Configure Constraints

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

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

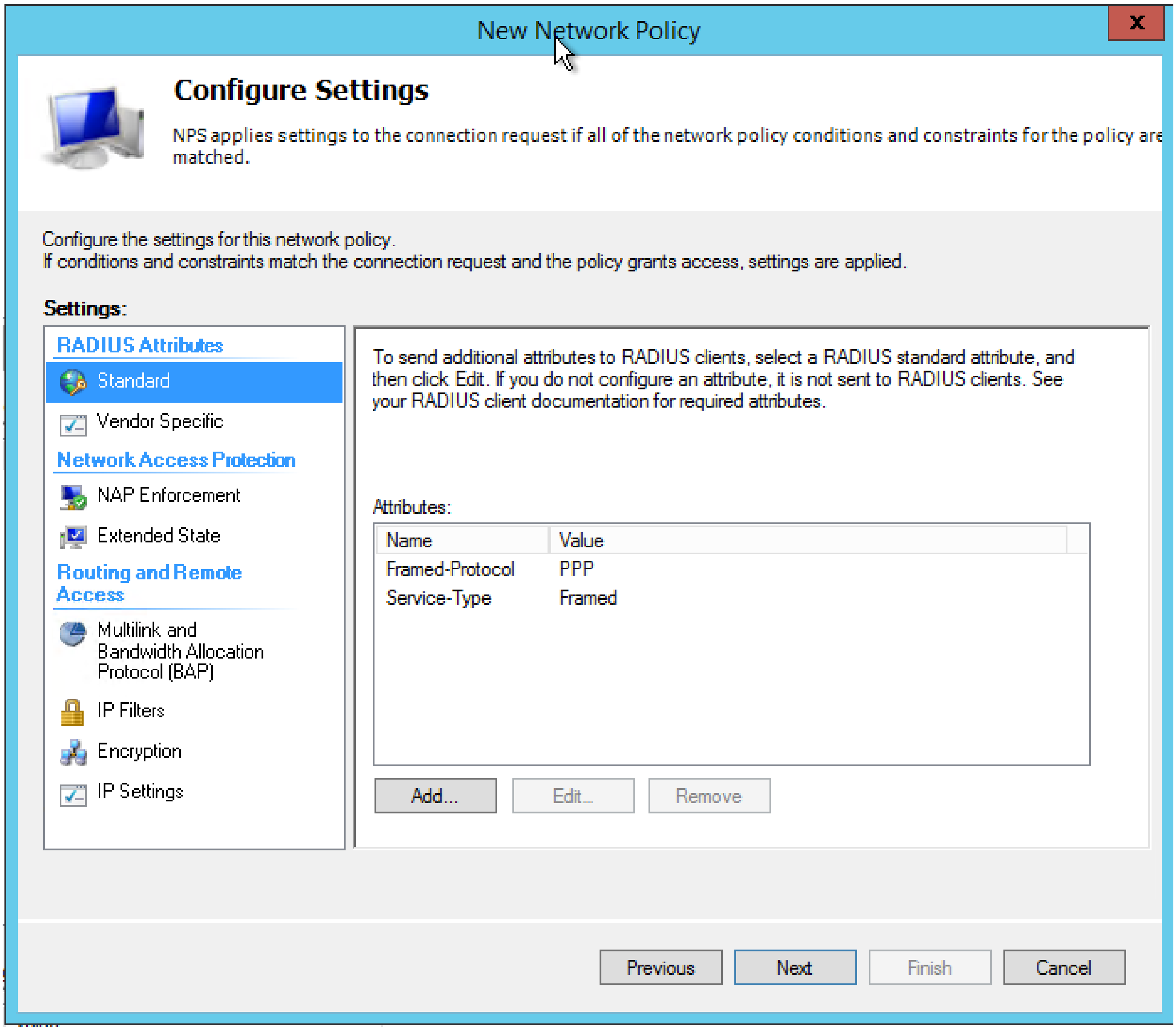
Constraints:

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

□ Disconnect after the maximum idle time

1

Leave this as a default – click **Next.**



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.

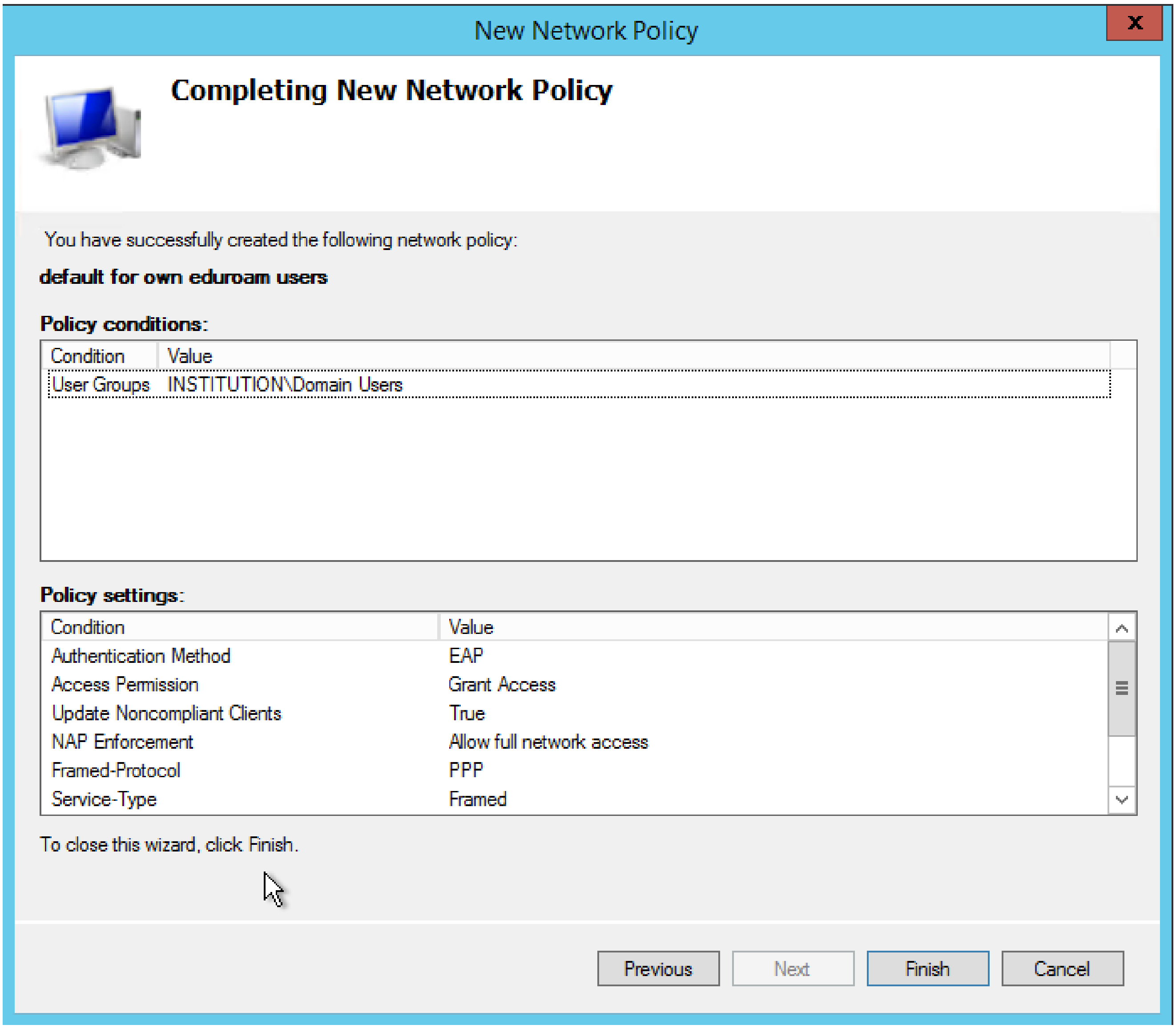
Settings:

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

This is where VLAN attributes can be set for local users. Leave as default for this policy (we should not set VLAN for our users at remote sites!). Click **Next.**



Completing New Network Policy

You have successfully created the following network policy:

default for own eduroam users

Policy conditions:

Condition	Value
User Groups	INSTITUTION\Domain Users

Policy settings:

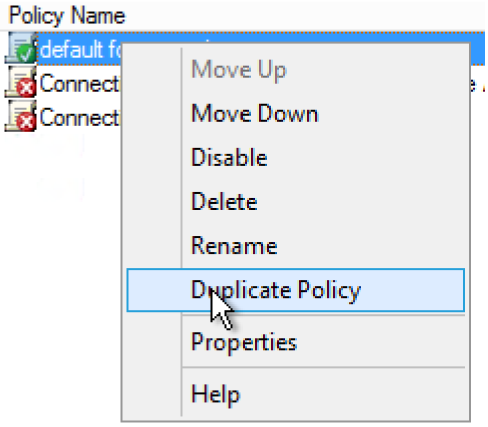
Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

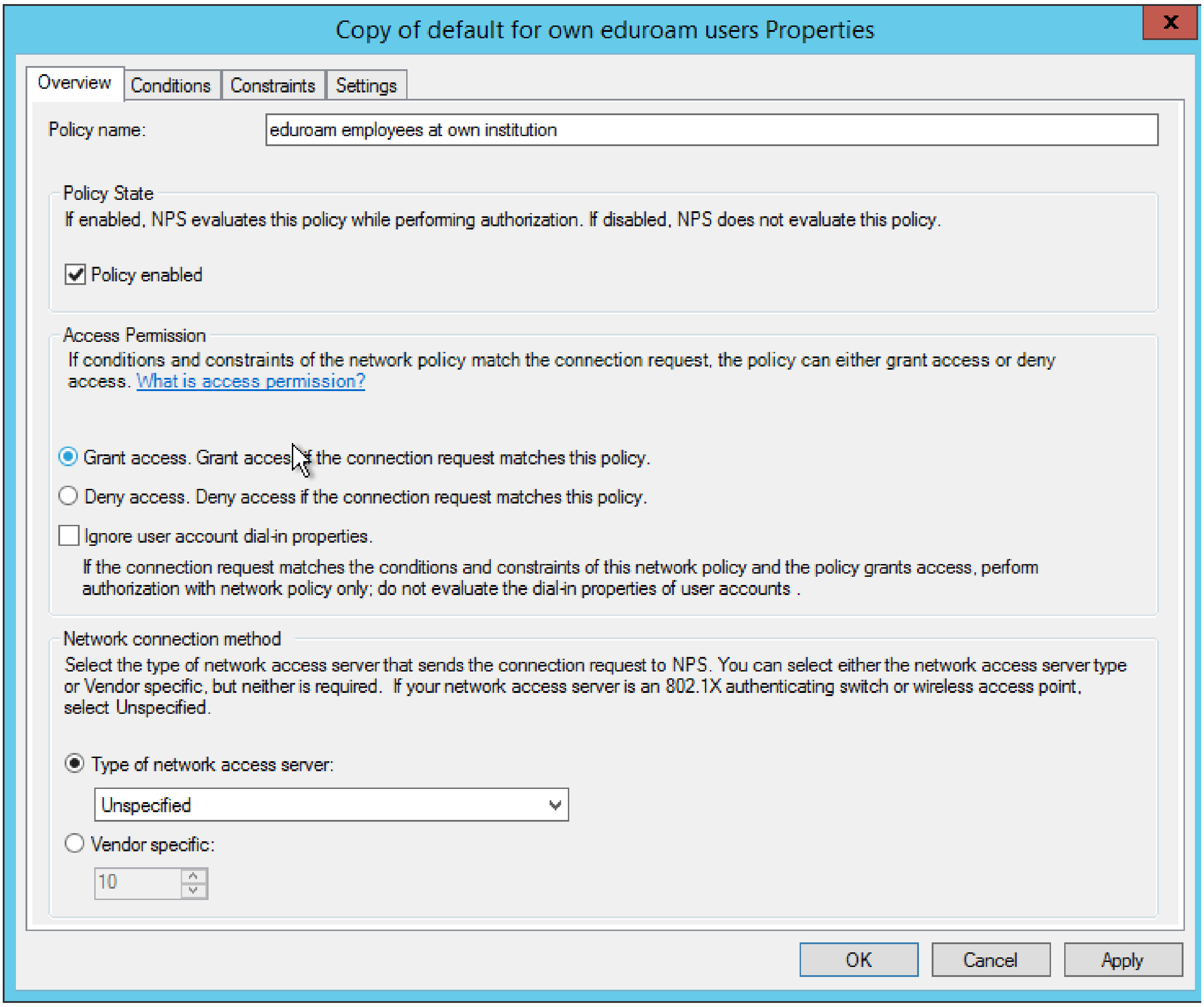
Check the settings and click **Finish**.

You should now be able to use eduroam at your site. Please check before adding more configurations. Local eduroam users will now all be placed in the VLAN (or possibly interface group) set on your controller or Access Points. Please also note that some Wireless controllers require you to enable “AAA Override” to allow VLAN (or interface group) to be set from RADIUS.

Now to place own users (or perhaps just some of them, e.g. employees) into a different VLAN. First duplicate the above Network Policy:



Then double click on the duplicate to edit:



Copy of default for own eduroam users Properties

Policy name: eduroam employees at own institution

Policy State

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

☑ Policy enabled

Access Permission

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

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

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

□ Ignore user account dial-in properties.

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

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

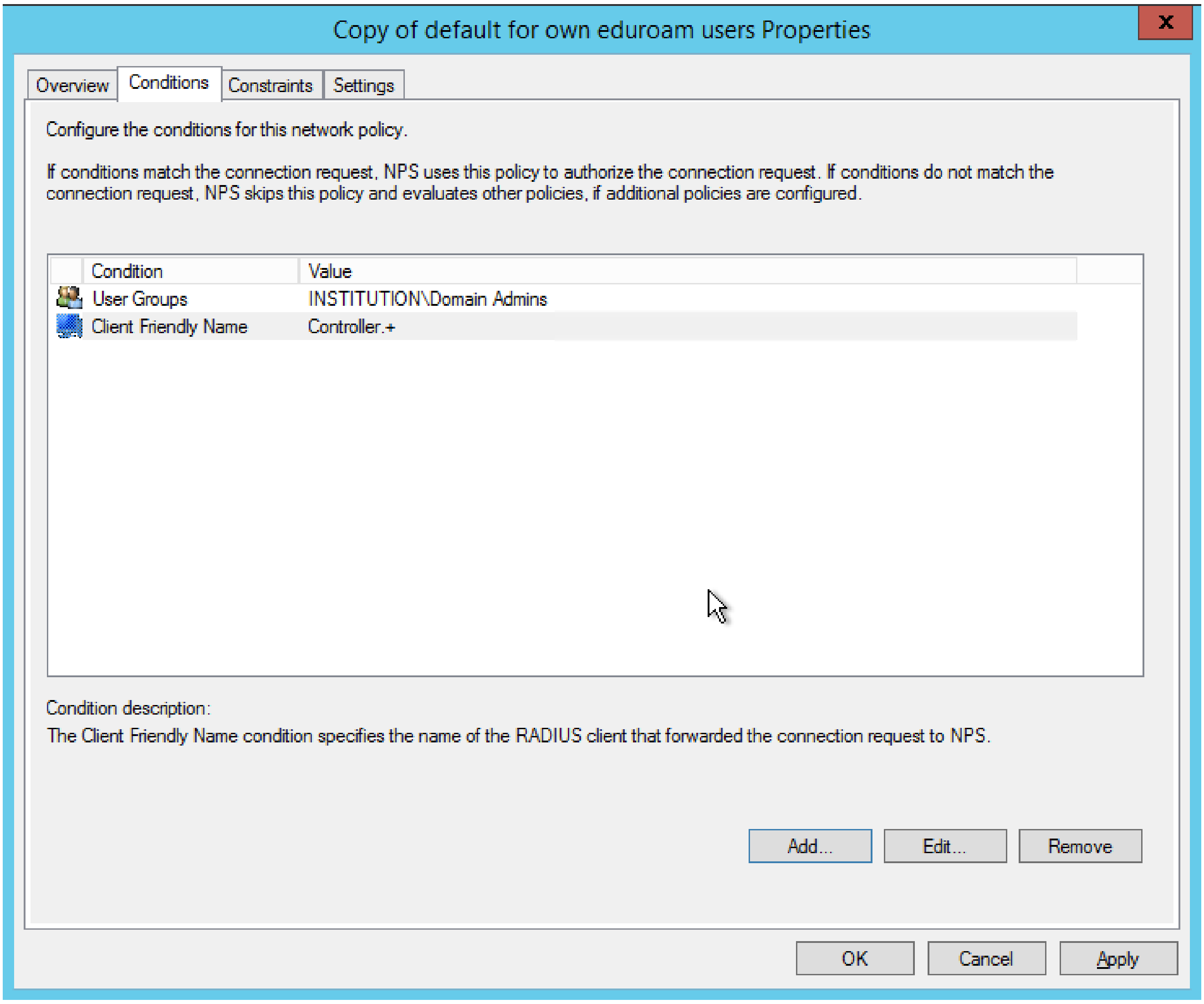
● Type of network access server:

Unspecified

○ Vendor specific:

10

Give the policy a new name and tick **Policy enabled** to enable the policy. Select the **Conditions** tab:



Copy of default for own eduroam users Properties

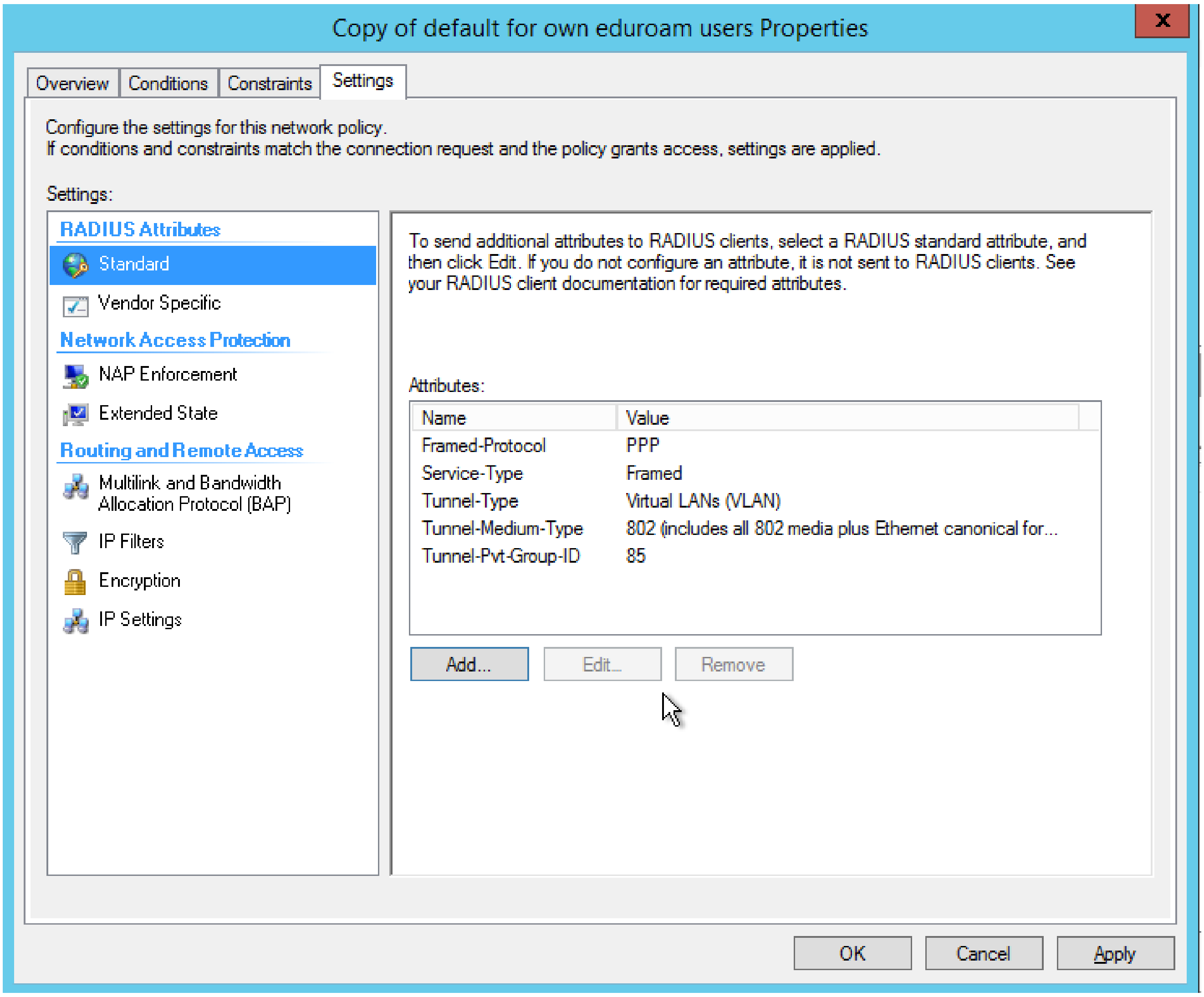
Configure the conditions for this network policy.

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	INSTITUTION\Domain Admins
Client Friendly Name	Controller.+

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

In this example, conditions are set to be Domain Admins and the Client Friendly Name so that request must be from one of the local Controllers. Next select the **Settings** tab:



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

Settings:

RADIUS Attributes
- Standard
- Vendor Specific

Network Access Protection
- NAP Enforcement
- Extended State

Routing and Remote Access
- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

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

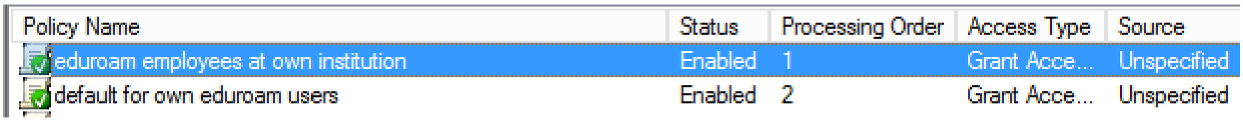
Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	85

Add RADIUS attributes as shown above to assign VLAN to users matching this policy. Your VLAN id of course must match your infrastructure. Although at the time of writing this has not been tested; **Tunnel-Pvt-Group-ID** should also be possible to use to set an Interface Group Name.

Click **OK.**

The order of Policies are important – right click on a policy and chose to move it up or down. Make sure the order is as below:



Policy Name	Status	Processing Order	Access Type	Source
eduroam employees at own institution	Enabled	1	Grant Acce...	Unspecified
default for own eduroam users	Enabled	2	Grant Acce...	Unspecified

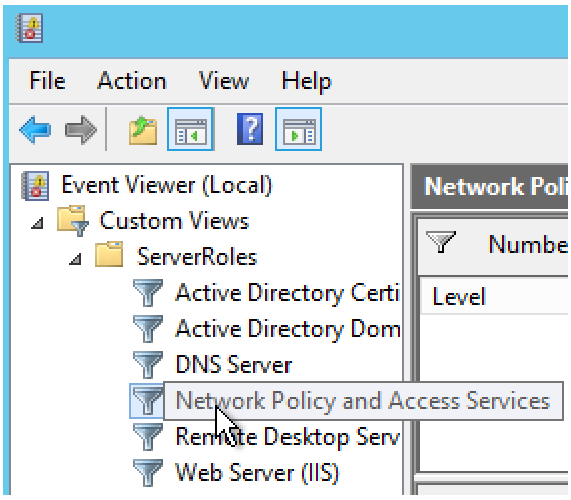
You may add more Network Policies for other user groups, Machine Groups or combinations of these – if you have followed this guide you will know how to do this now.

6 Logging / Accounting

To see NPS events open Event Viewer. (Or view events directly in Server Manager)

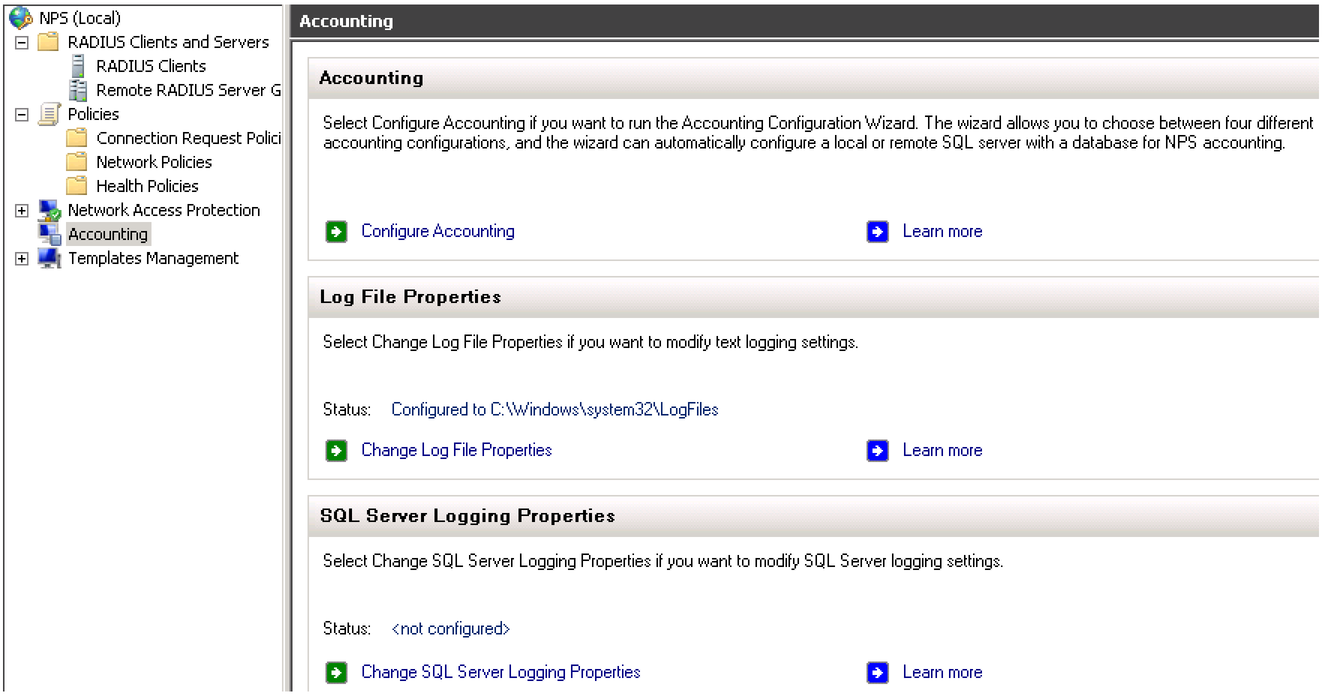
In Windows 2012: **Server Manager** > **Tools** > **Event Viewer**.

In Windows 2008: **Start** > **Administrative Tools** > **Event Viewer**.



You will find the NPS related log under **Custom Views** > **ServerRoles** > **Network Policy and Access Services**.

Another source of information is accounting, by default accounting is enabled logging to a file:



Accounting

Accounting

Select Configure Accounting if you want to run the Accounting Configuration Wizard. The wizard allows you to choose between four different accounting configurations, and the wizard can automatically configure a local or remote SQL server with a database for NPS accounting.

Configure Accounting   Learn more

Log File Properties

Select Change Log File Properties if you want to modify text logging settings.

Status: Configured to C:\Windows\system32\LogFiles

Change Log File Properties   Learn more

SQL Server Logging Properties

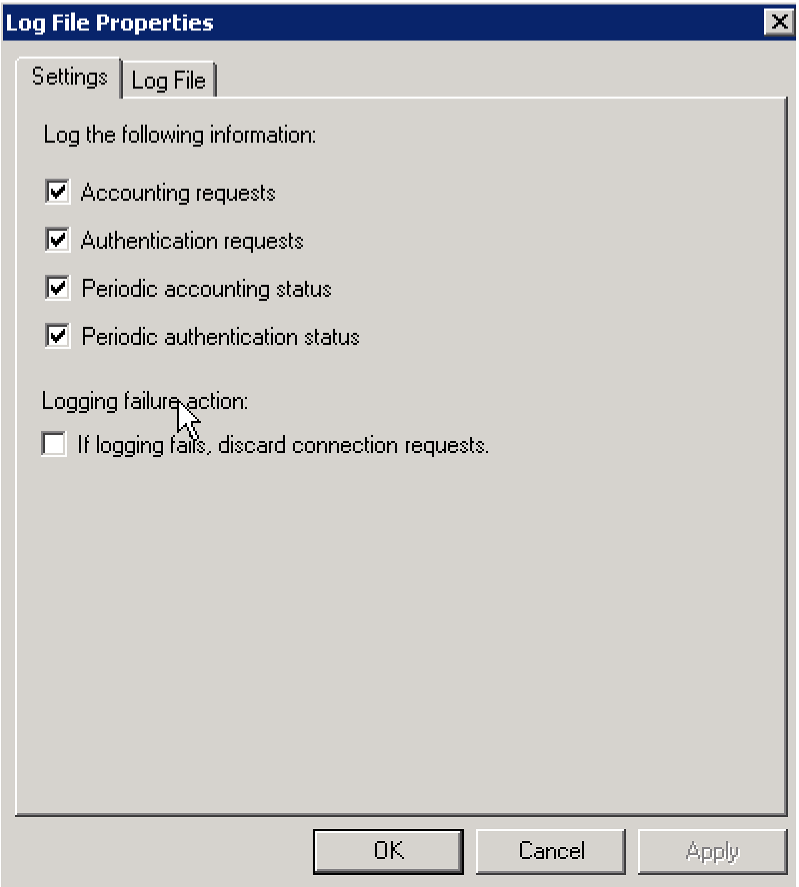
Select Change SQL Server Logging Properties if you want to modify SQL Server logging settings.

Status: <not configured>

Change SQL Server Logging Properties   Learn more

If you would like to run queries toward your authentication and accounting information and maybe produce some statistics from it, use the “Configure Accounting” Wizard to setup logging to the SQL database. You may combine this with logging to file.

If you choose to keep logging to a file consider these settings, click **Change Log File Properties**:



Log the following information:

☑ Accounting requests

☑ Authentication requests

☑ Periodic accounting status

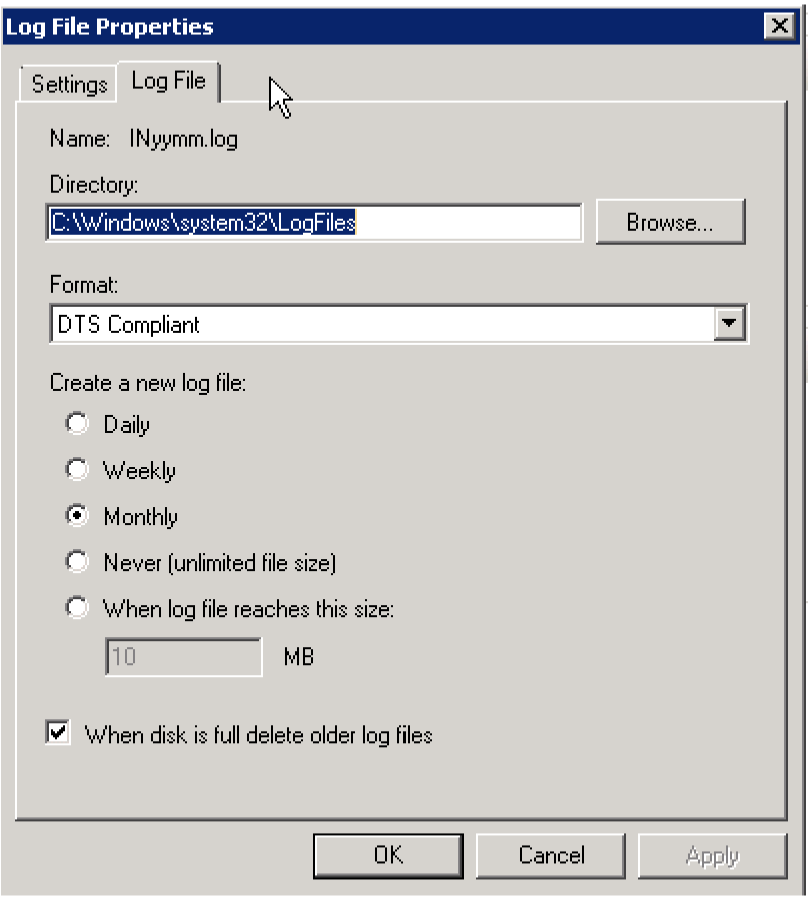
☑ Periodic authentication status

Logging failure action:

□ If logging fails, discard connection requests.

You might want to check that **If logging fails, discard connection requests** is unchecked.

Select the **Log File** tab:



Name: INyymm.log

Directory:
C:\Windows\system32\LogFiles

Format:
DTS Compliant

Create a new log file:

○ Daily
○ Weekly
● Monthly
○ Never (unlimited file size)
○ When log file reaches this size:
10 MB

☑ When disk is full delete older log files

Decide how often you want a new log file created – One month could produce a lot of data to search through.

Tip:

To improve the presentation of Log File presentation, a third-party tool like IAS log viewer can be used to track log files, produce statistics and assemble reports for users and accounting purposes. It is also possible to define traps for alarms and filter logs.

See http://www.deepsoftware.com/iasviewer/ for a list of features, shareware license information and downloads.

7 Troubleshooting tips

- Install Wireshark on your NPS server to be able to see all RADIUS traffic.
- Set up a Linux machine as a RADIUS client and install `wpa_supplicant` on it. This supplicant contains `eapol_test` (a program that communicates directly with the RADIUS server) and `rad_eap_test` (a script that use `eapol_test`). This provides a lot of information and is a useful tool for testing and troubleshooting. Here is an example command using the script:
    - ./rad_eap_test -c -H 192.168.1.10 -P 1812 -S sharedsecret -M 22:44:66:33:22:55 -u anon1234@win-ng.uninett.no -p password -e PEAP -m WPA-EAP | grep 'RADIUS message:'
- Use the CAT tool to setup clients in your realm / institution – it could save a lot of time doing troubleshooting and also contains a possibility to check your realm from a remote site. Any questions about this tool should be directed to your NRO.

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 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 a certificate (self-signed or not) it is 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.

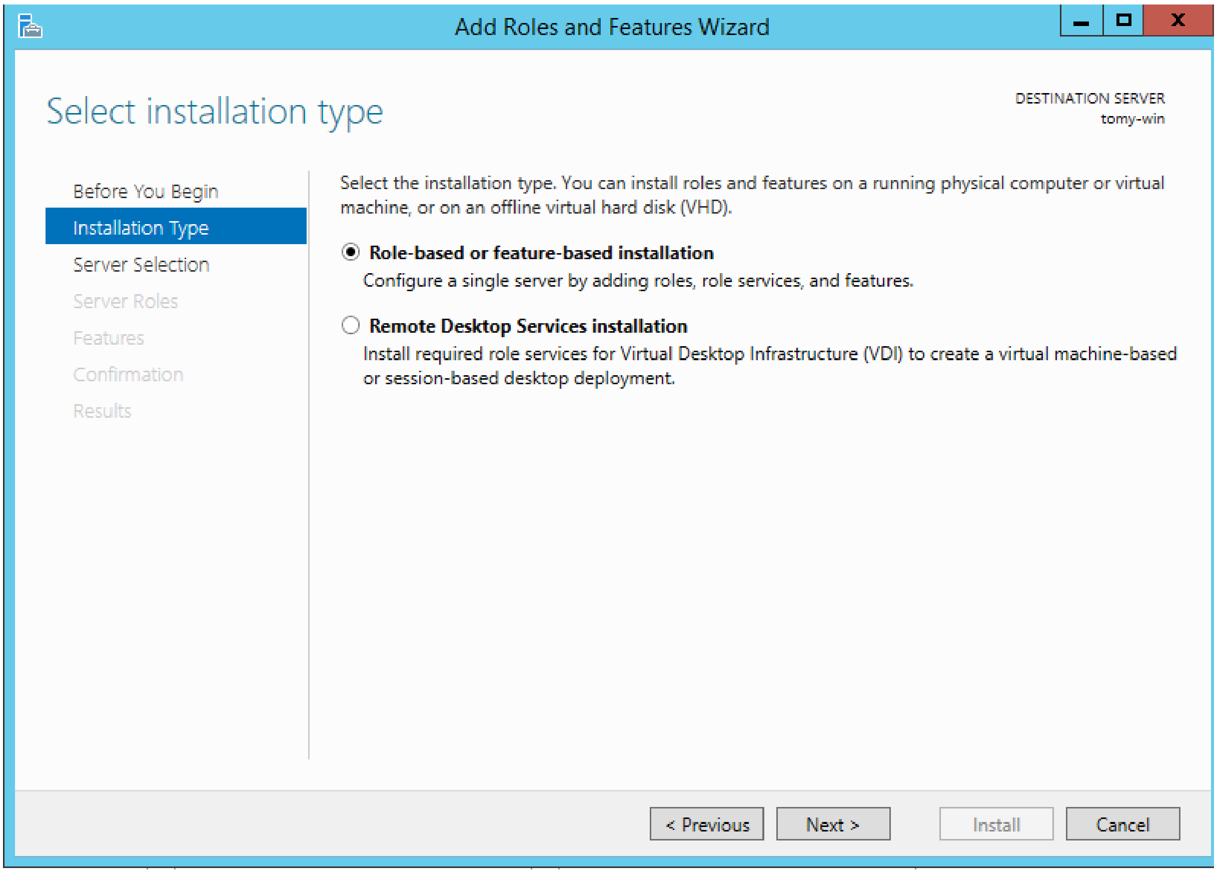
The following is showing how to setup your own CA (on your Domain Controller), create a CA certificate, distribute it to your clients and finally request (from your own CA) and install a server certificate for NPS. If you already have a CA set up and a CA certificate, please jump to the relevant section below.

(For an alternative method see [UFS112] "Recommended Security Solution for Wireless Networks" for setting up your own CA and acquire a certificate form your own CA using Linux.)

Prerequisites – Windows Active Directory Domain Controller must be running on this server or this server is part of an AD domain.

A.1 Install and configure Windows server as a CA Server

Add Roles and Features Wizard:



Select installation type

DESTINATION SERVER
tomy-win

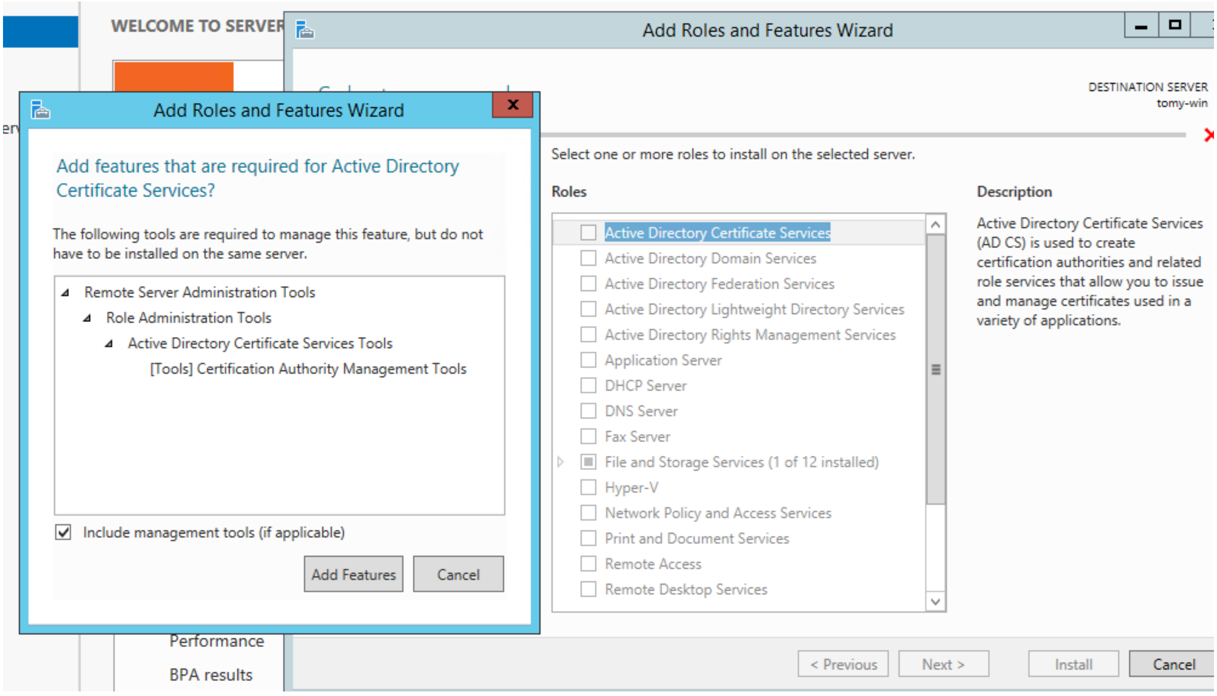
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Select **Active Directory Certificate Services**:

And add required features (as suggested). Select **Add Features**.



Add Roles and Features Wizard

Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)

DESTINATION SERVER
tomy-win

Select one or more roles to install on the selected server.

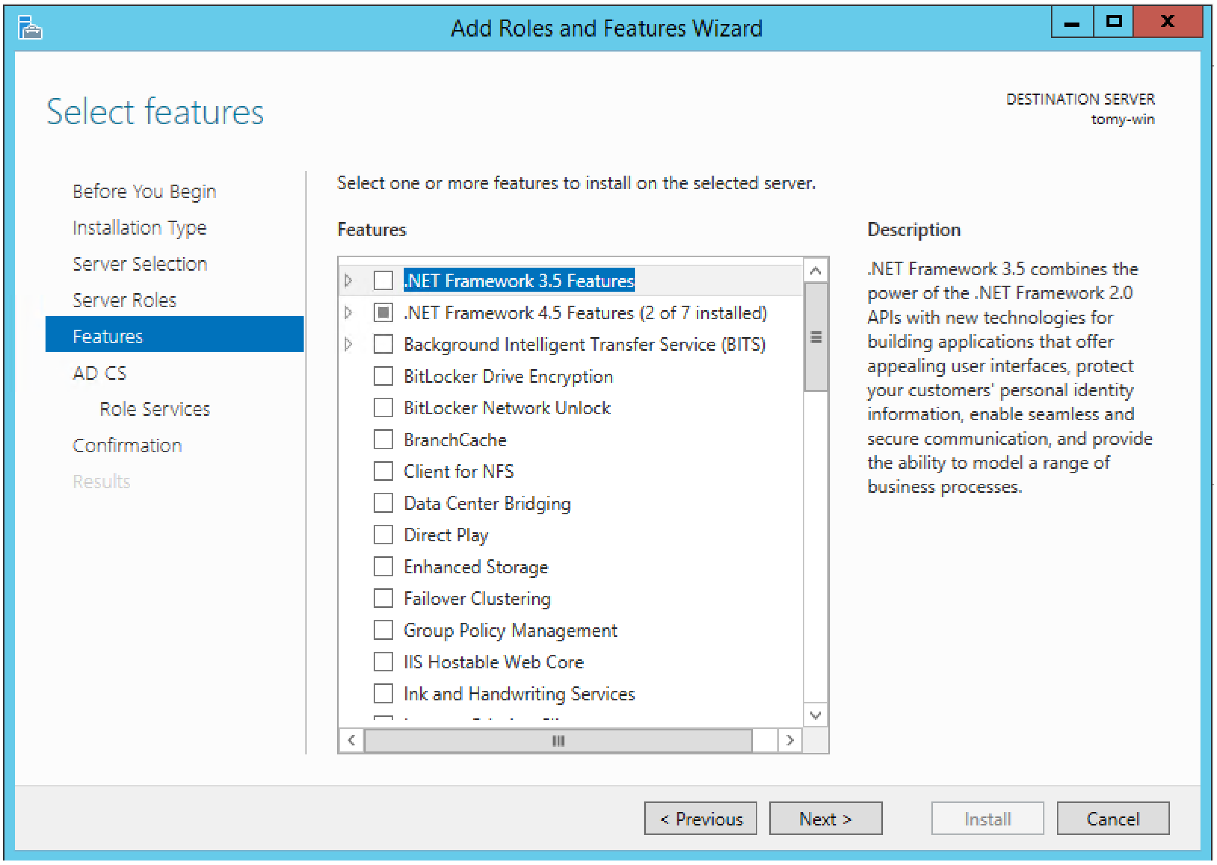
Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

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

Press **Next**:



Add Roles and Features Wizard

Select features

DESTINATION SERVER
tomy-win

Select one or more features to install on the selected server.

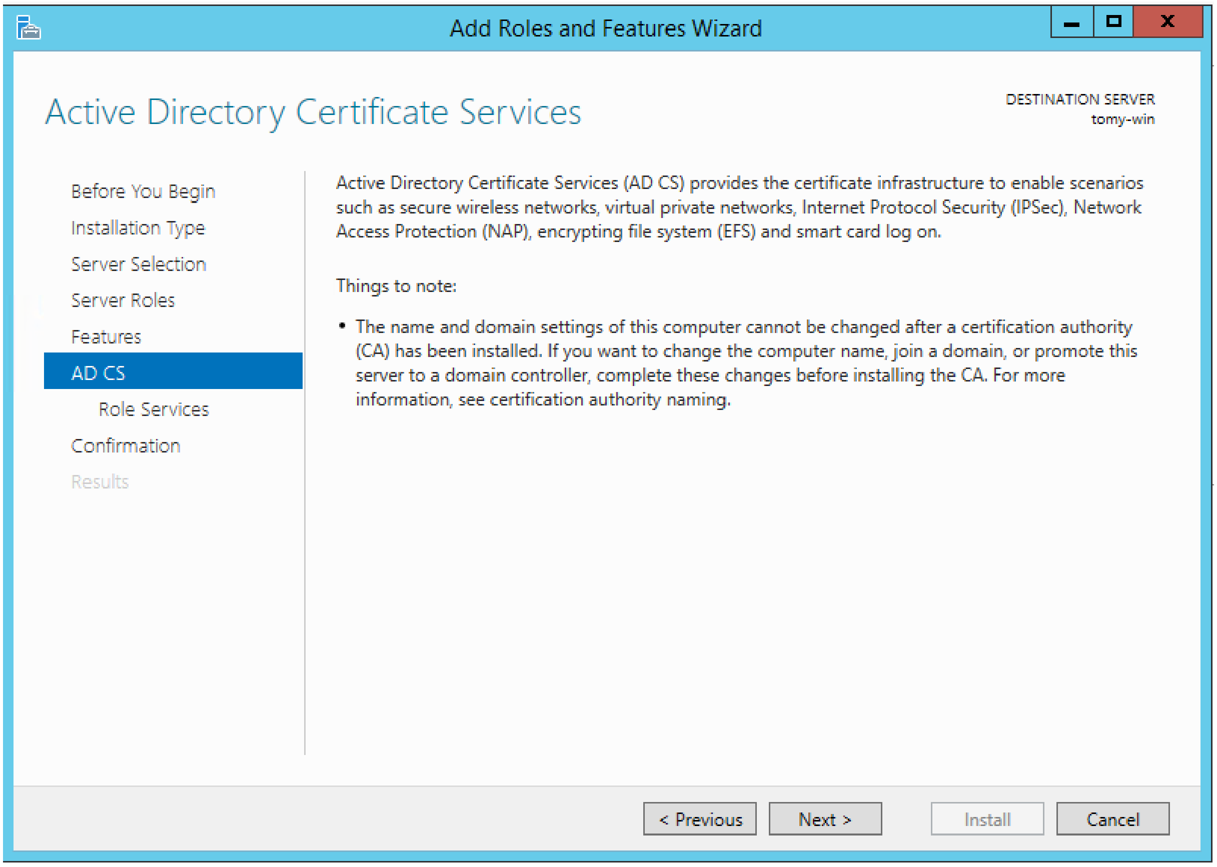
Features

- □ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Select **Review ADCS information text** from the scroll down list. Press **Next**:

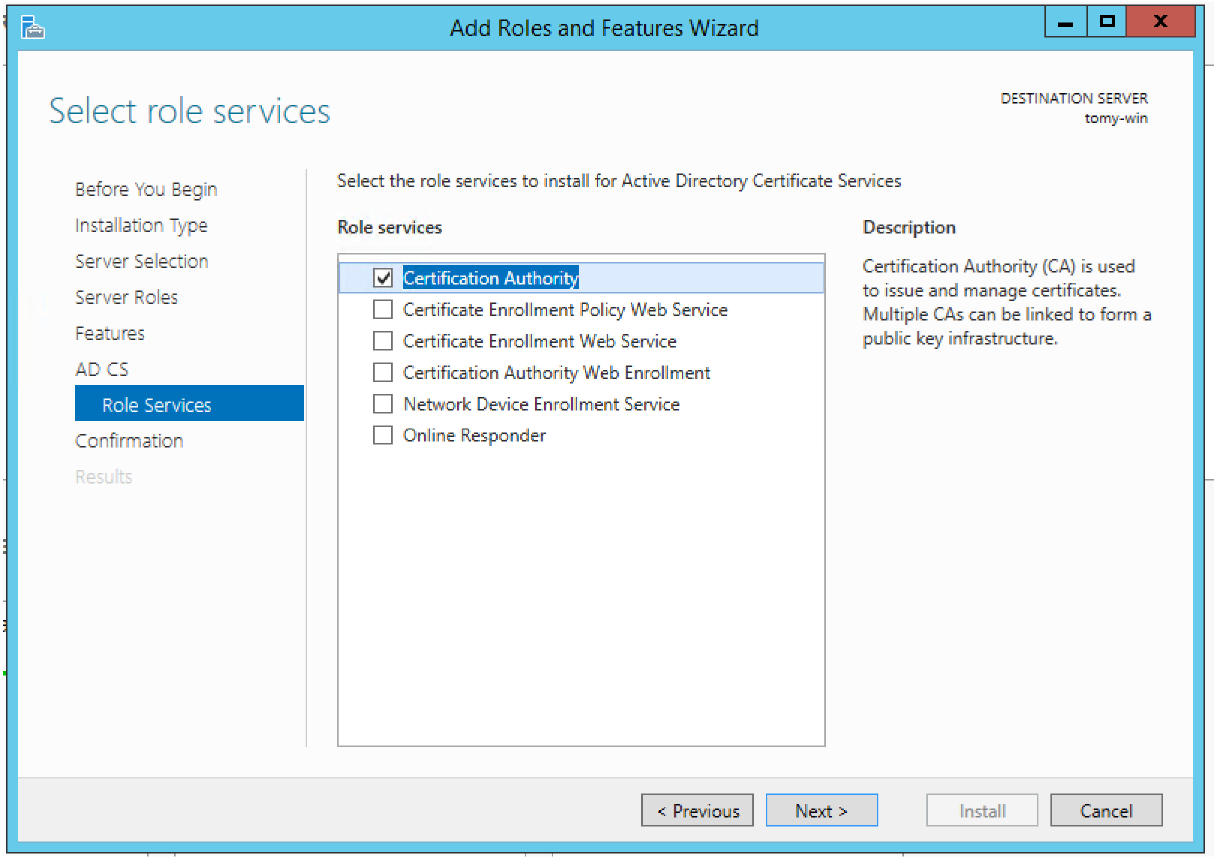


Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Press **Next**:



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
tomy-win

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD CS
- Role Services
- Confirmation
- Results

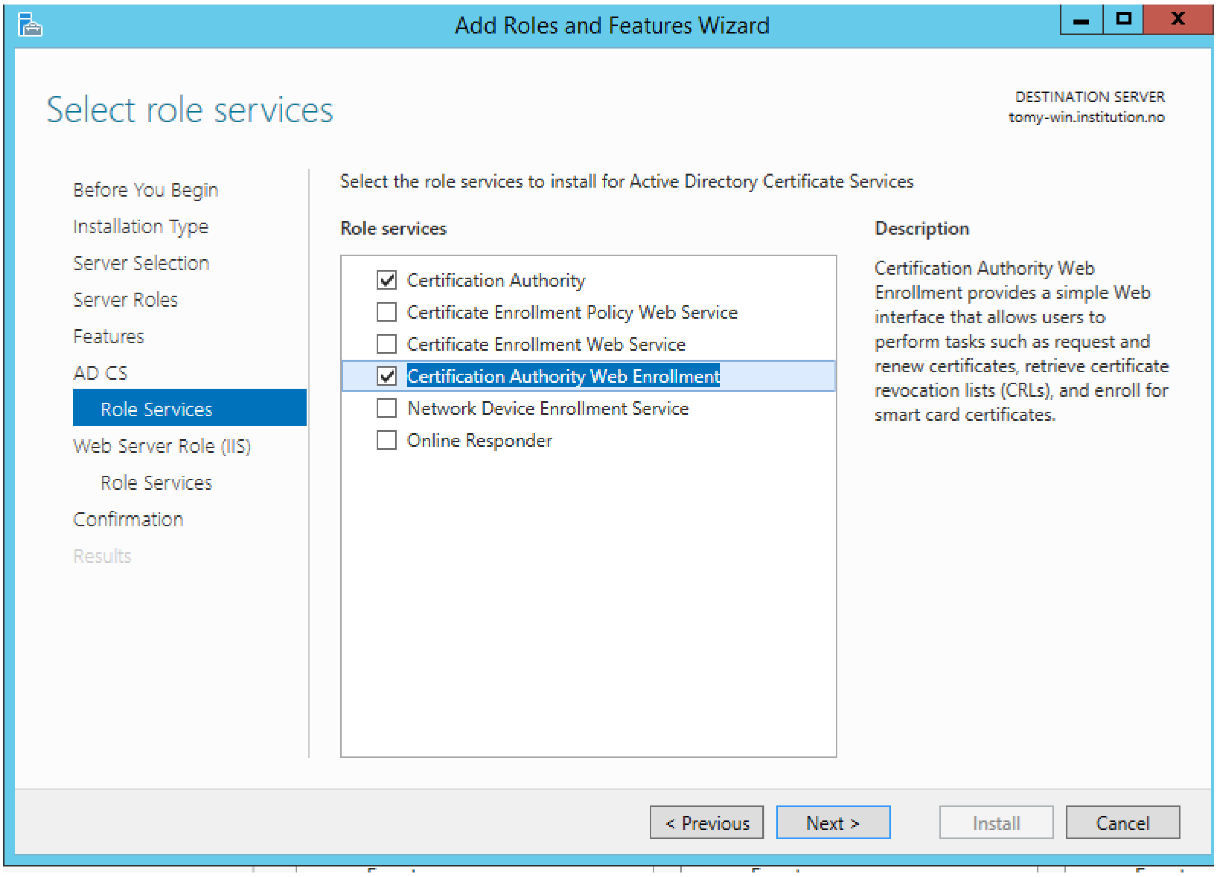
Select the role services to install for Active Directory Certificate Services

Role services

☑ Certification Authority
□ Certificate Enrollment Policy Web Service
□ Certificate Enrollment Web Service
□ Certification Authority Web Enrollment
□ Network Device Enrollment Service
□ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
tomy-win.institution.no

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD CS
  - Role Services
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

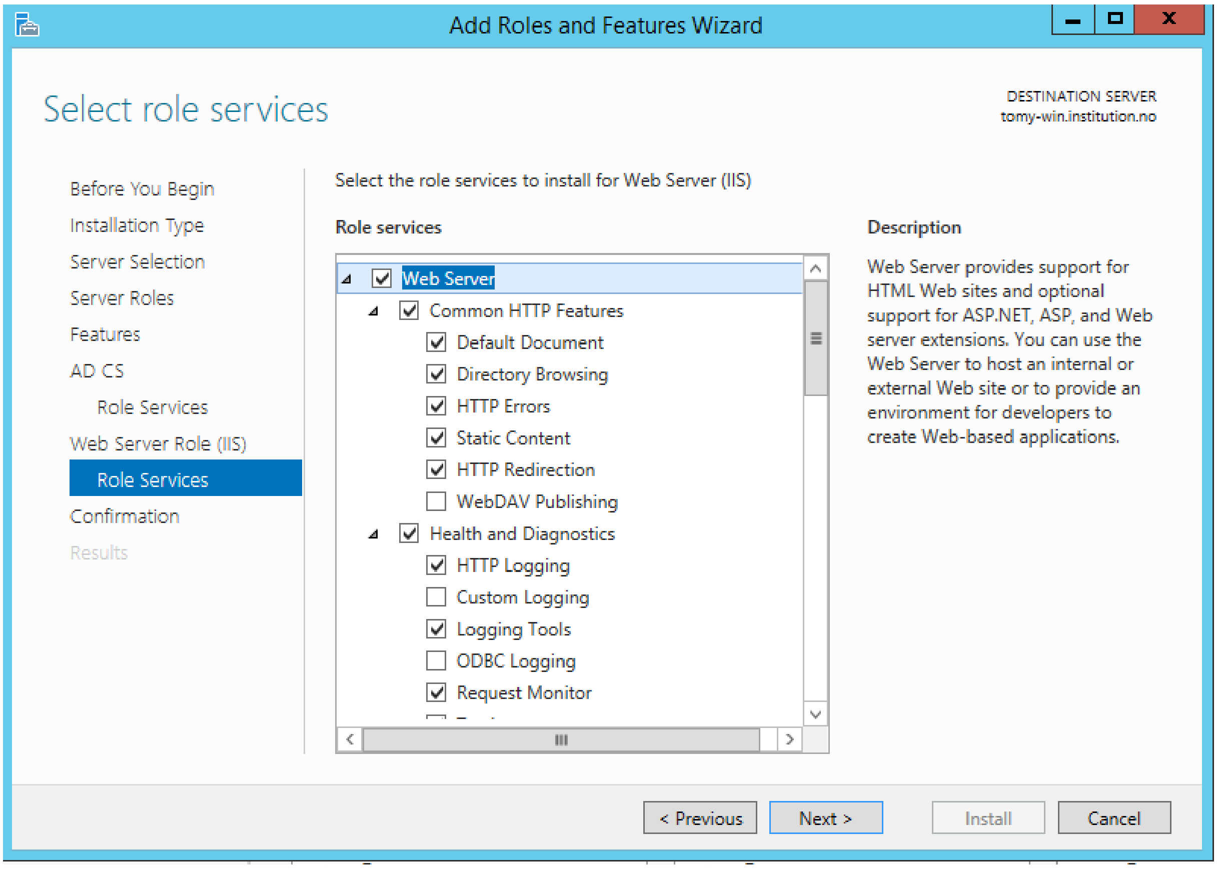
Select the role services to install for Active Directory Certificate Services

Role services

- ☑ Certification Authority
- □ Certificate Enrollment Policy Web Service
- □ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- □ Network Device Enrollment Service
- □ Online Responder

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.



Select role services

DESTINATION SERVER
tomy-win.institution.no

Select the role services to install for Web Server (IIS)

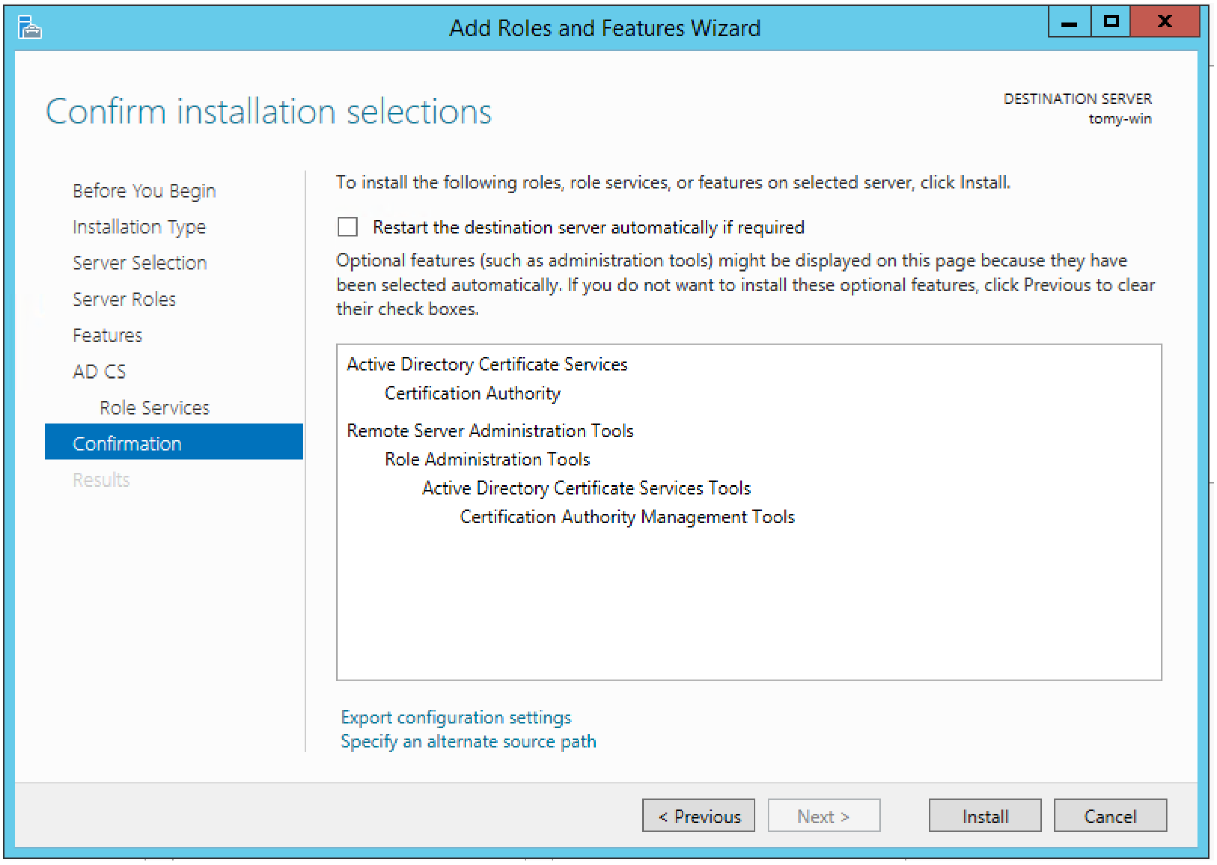
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - ☑ Logging Tools
    - □ ODBC Logging
    - ☑ Request Monitor

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

Then press **Install**:



Confirm installation selections

DESTINATION SERVER
tomy-win

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

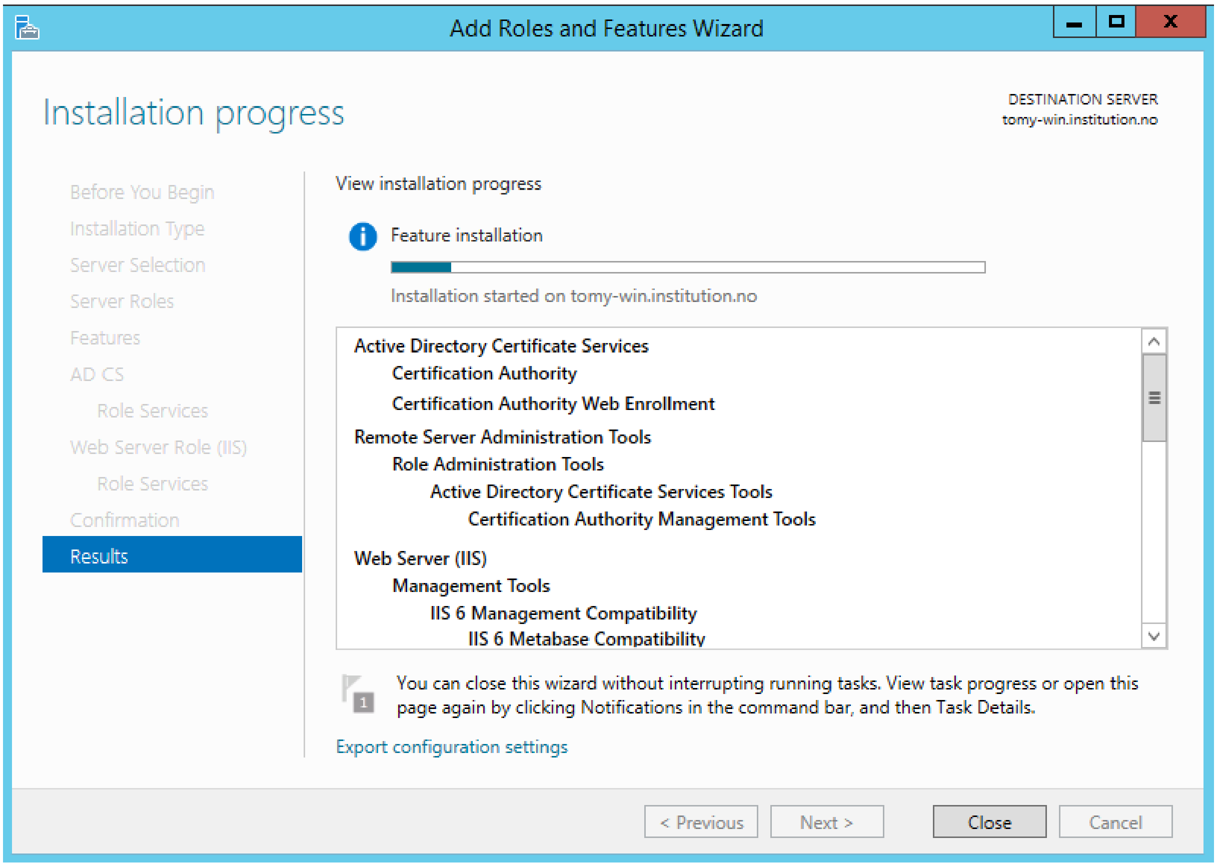
□ Restart the destination server automatically if required

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

Active Directory Certificate Services
    Certification Authority

Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools

Installation – **Close** once Installation succeeded:



Installation progress

DESTINATION SERVER
tomy-win.institution.no

View installation progress

Feature installation

Installation started on tomy-win.institution.no

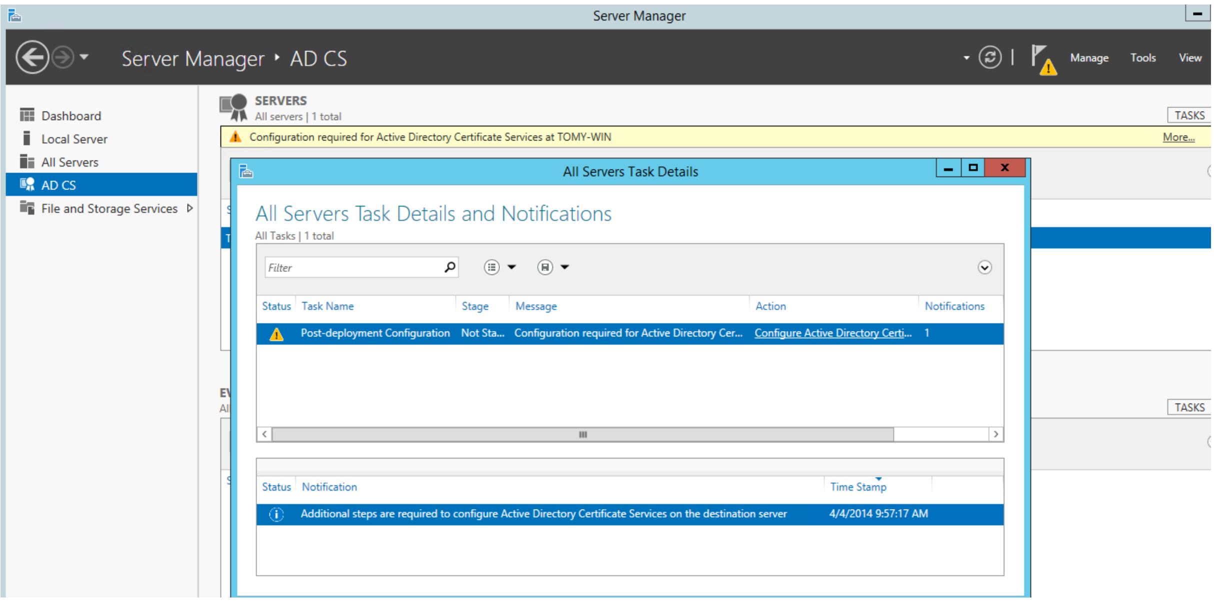
Active Directory Certificate Services
    Certification Authority
    Certification Authority Web Enrollment
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools
Web Server (IIS)
    Management Tools
        IIS 6 Management Compatibility
            IIS 6 Metabase Compatibility

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

In Server Manager – AD CS – it will notify that configuration is required for AD CS.

Click on **More…**



SERVERS
All servers | 1 total

Configuration required for Active Directory Certificate Services at TOMY-WIN More...

All Servers Task Details and Notifications

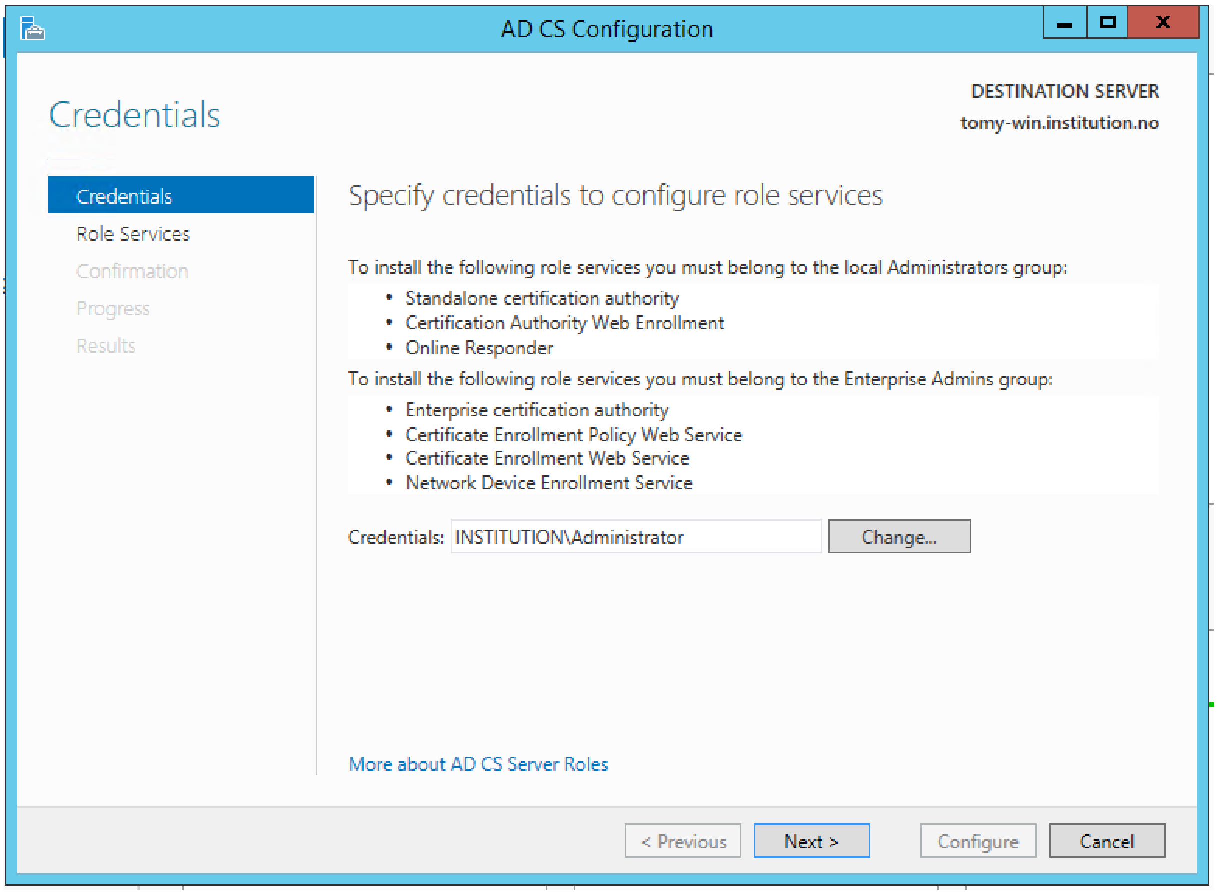
All Tasks | 1 total

Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Cer...	Configure Active Directory Certi...	1

Status	Notification	Time Stamp
ⓘ	Additional steps are required to configure Active Directory Certificate Services on the destination server	4/4/2014 9:57:17 AM

Press **Configure Active Directory Certification Services**

Read the text and press **Next**:



DESTINATION SERVER
tomy-win.institution.no

Credentials

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

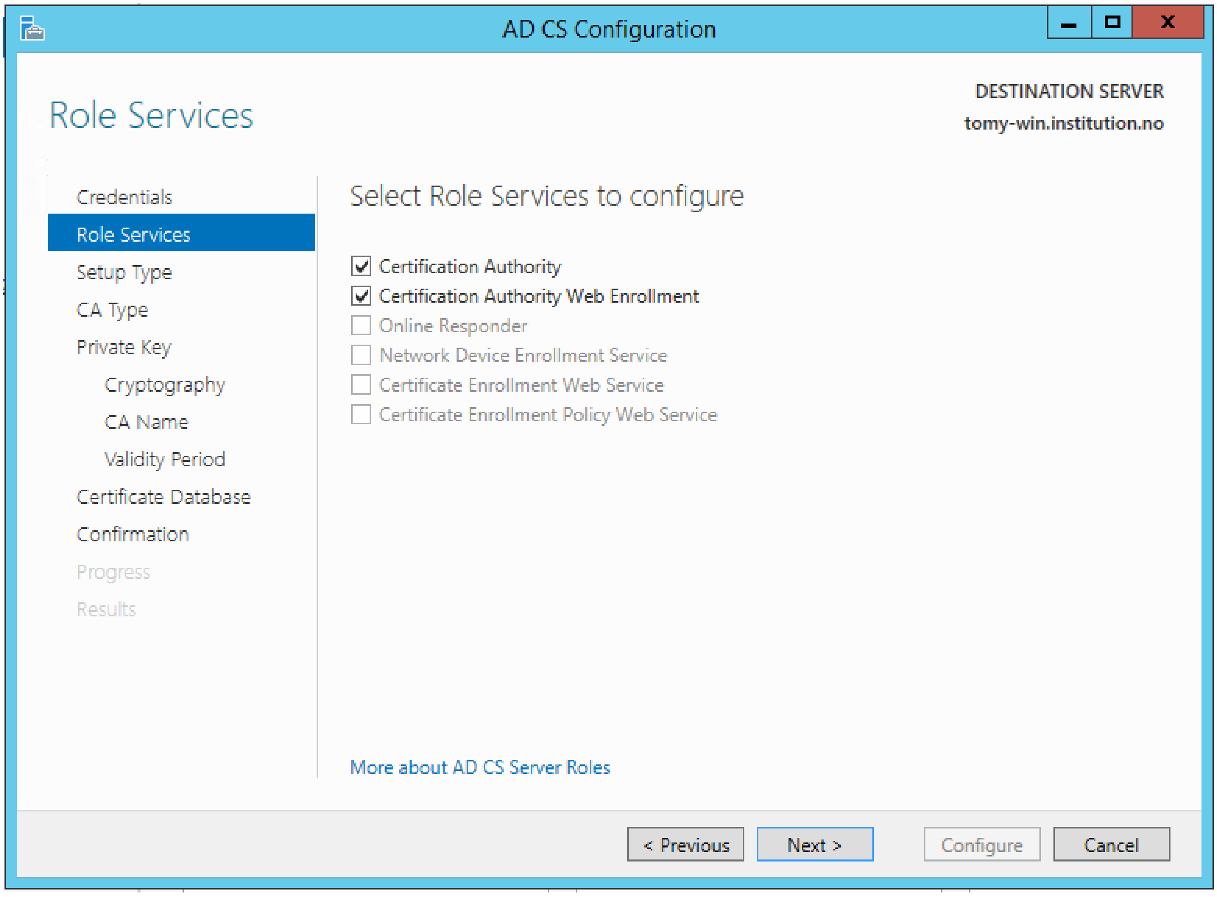
To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: INSTITUTION\Administrator

Select **Role Certification Authority**:

Then **Next.**



AD CS Configuration

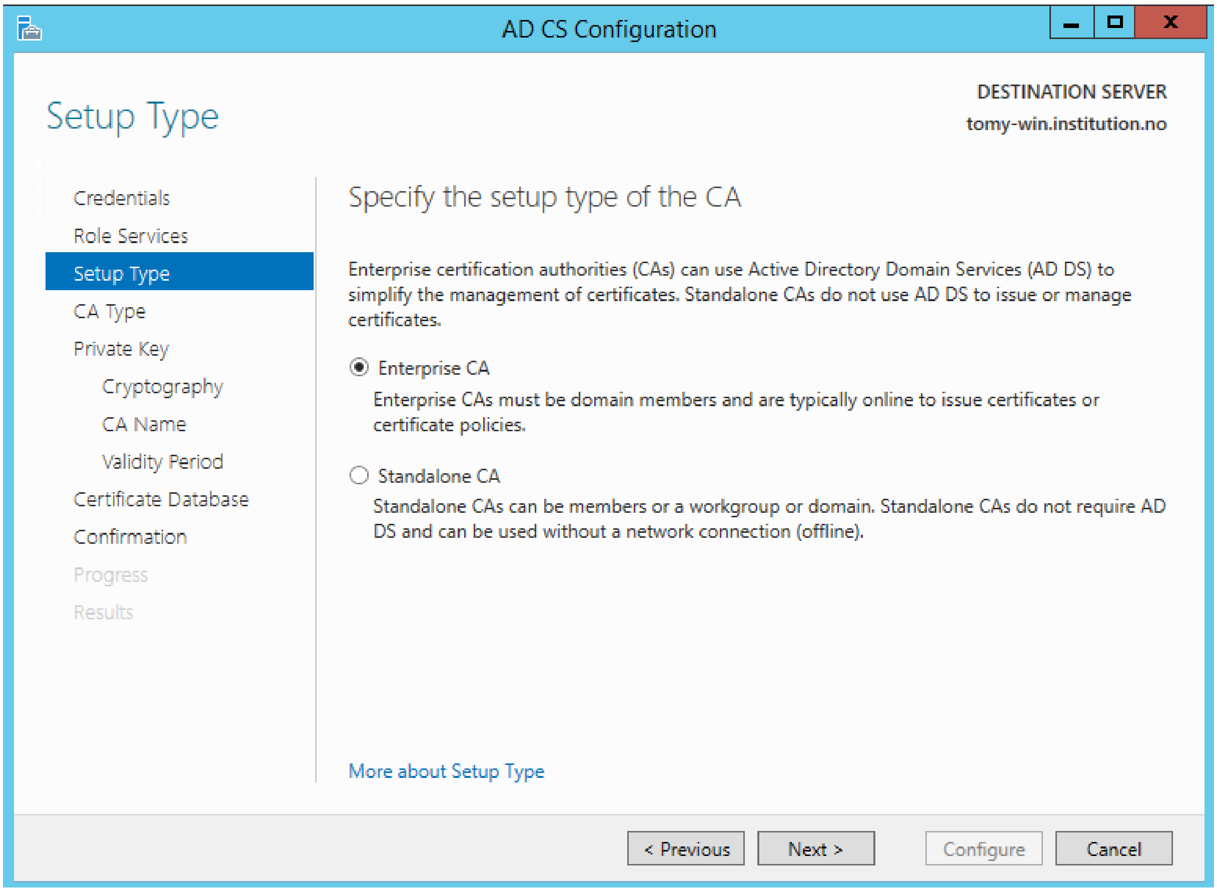
Role Services

DESTINATION SERVER
tomy-win.institution.no

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

In Setup Type, select **Enterprise CA**:



Setup Type

DESTINATION SERVER
tomy-win.institution.no

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

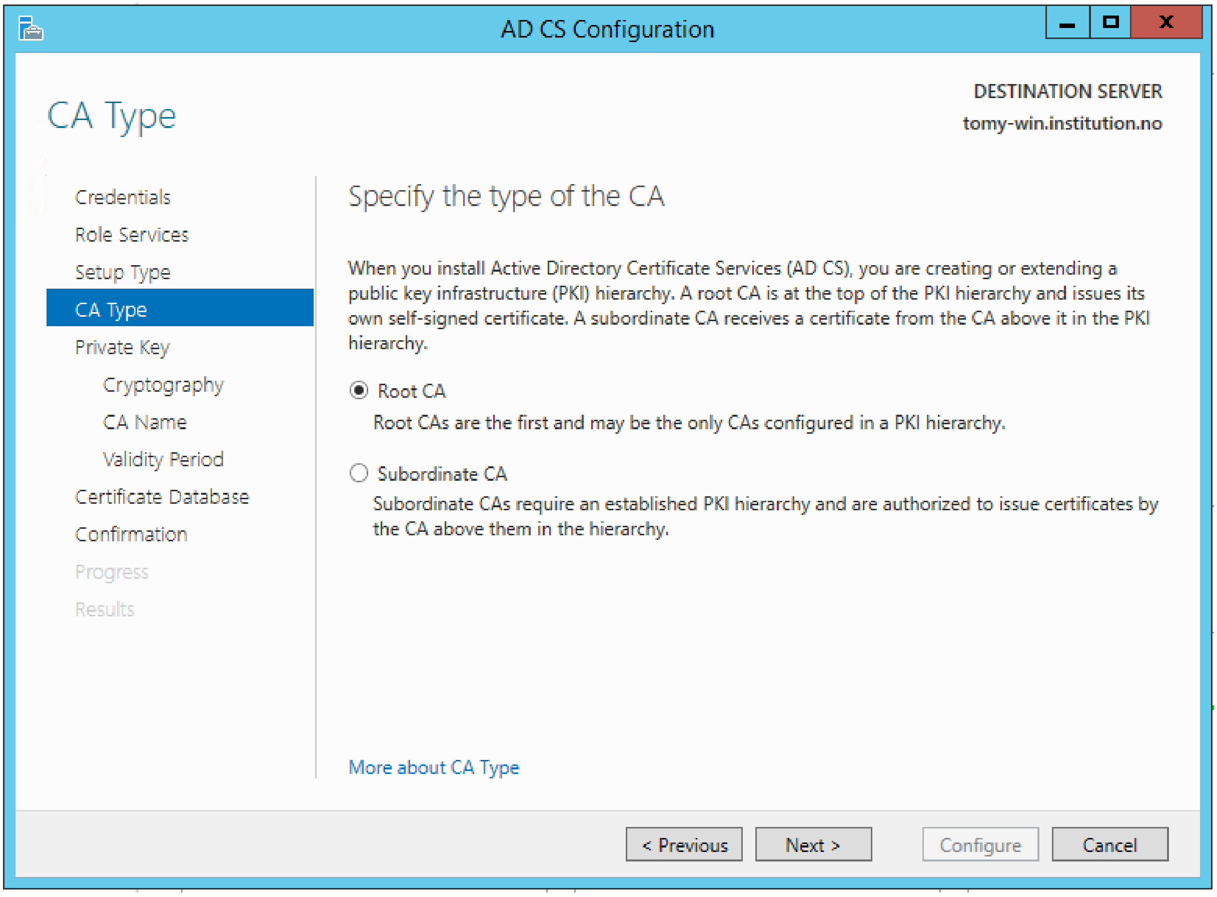
● Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

In CA Type, select **Root CA**:



CA Type

DESTINATION SERVER
tomy-win.institution.no

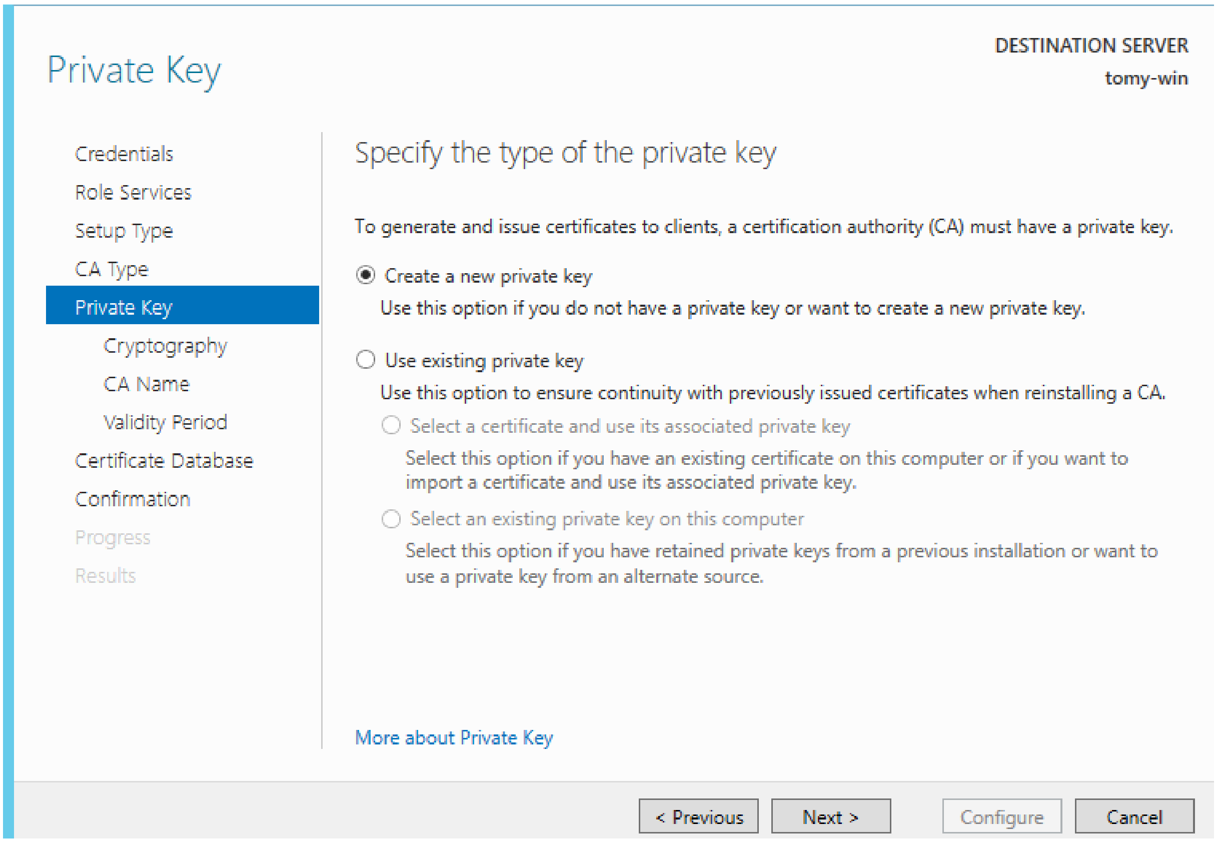
Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

In Private Key, select **Create a new private key**:



Private Key

DESTINATION SERVER
tomy-win

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key

Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key

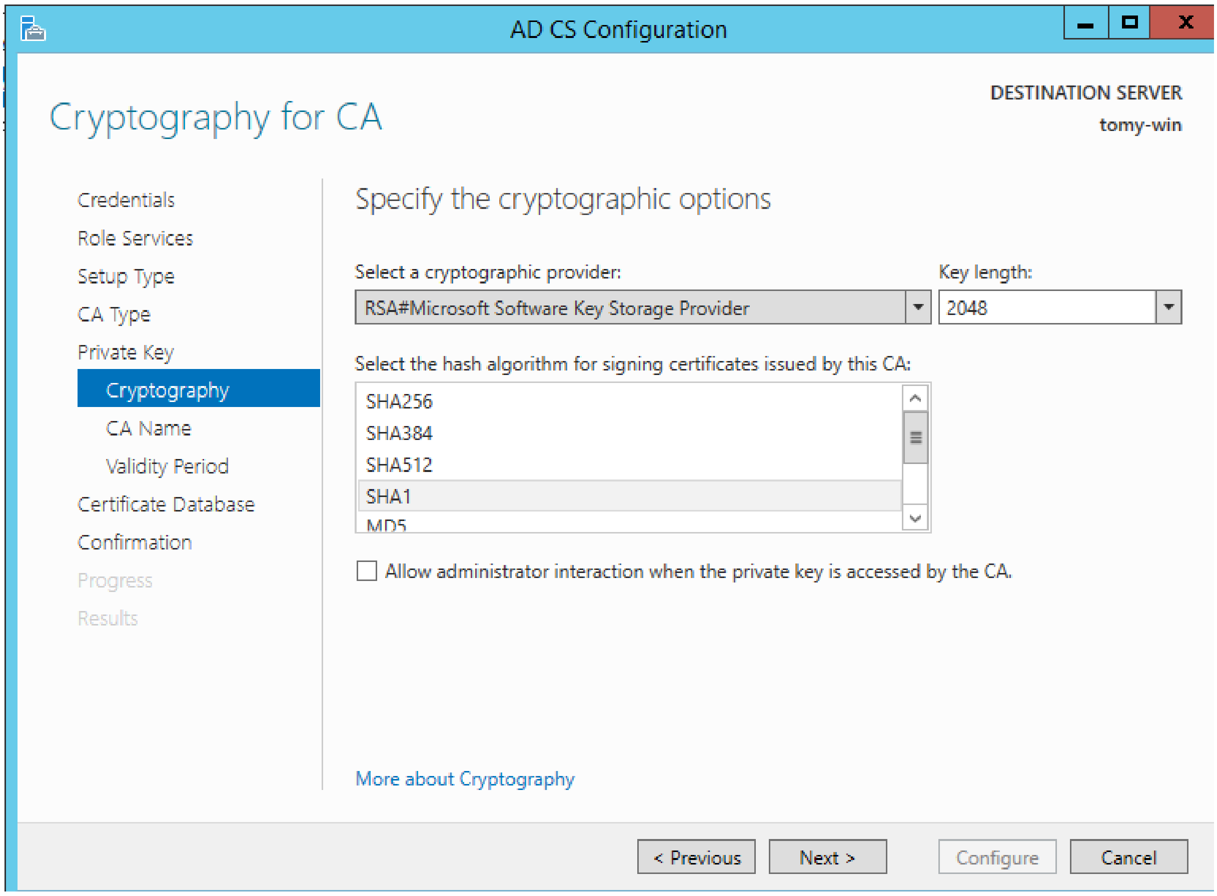
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about Private Key

In Cryptography, accept the suggested cryptographic options:



AD CS Configuration

Cryptography for CA

DESTINATION SERVER
tomy-win

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

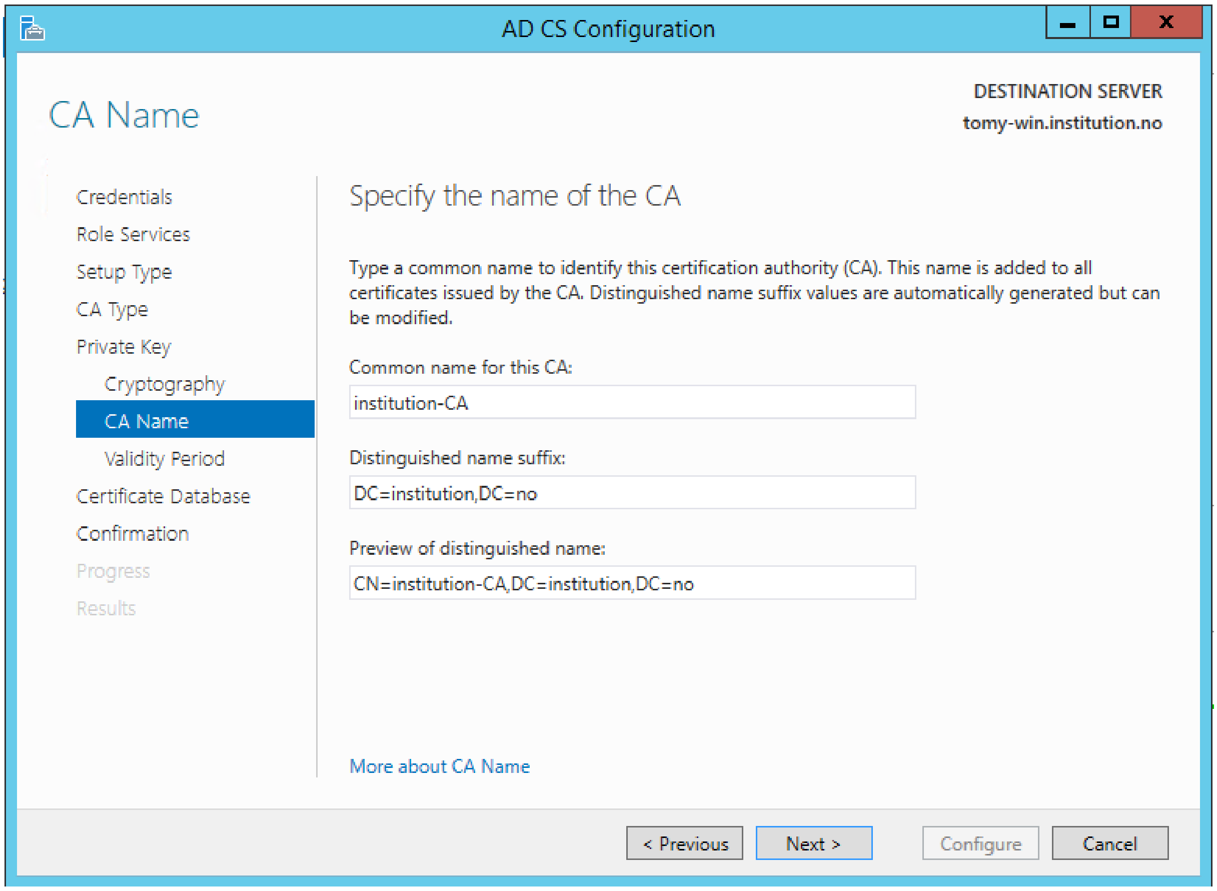
Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

In CA Name, accept the default Common name for CA (servername-CA.domain):



CA Name

Specify the name of the CA

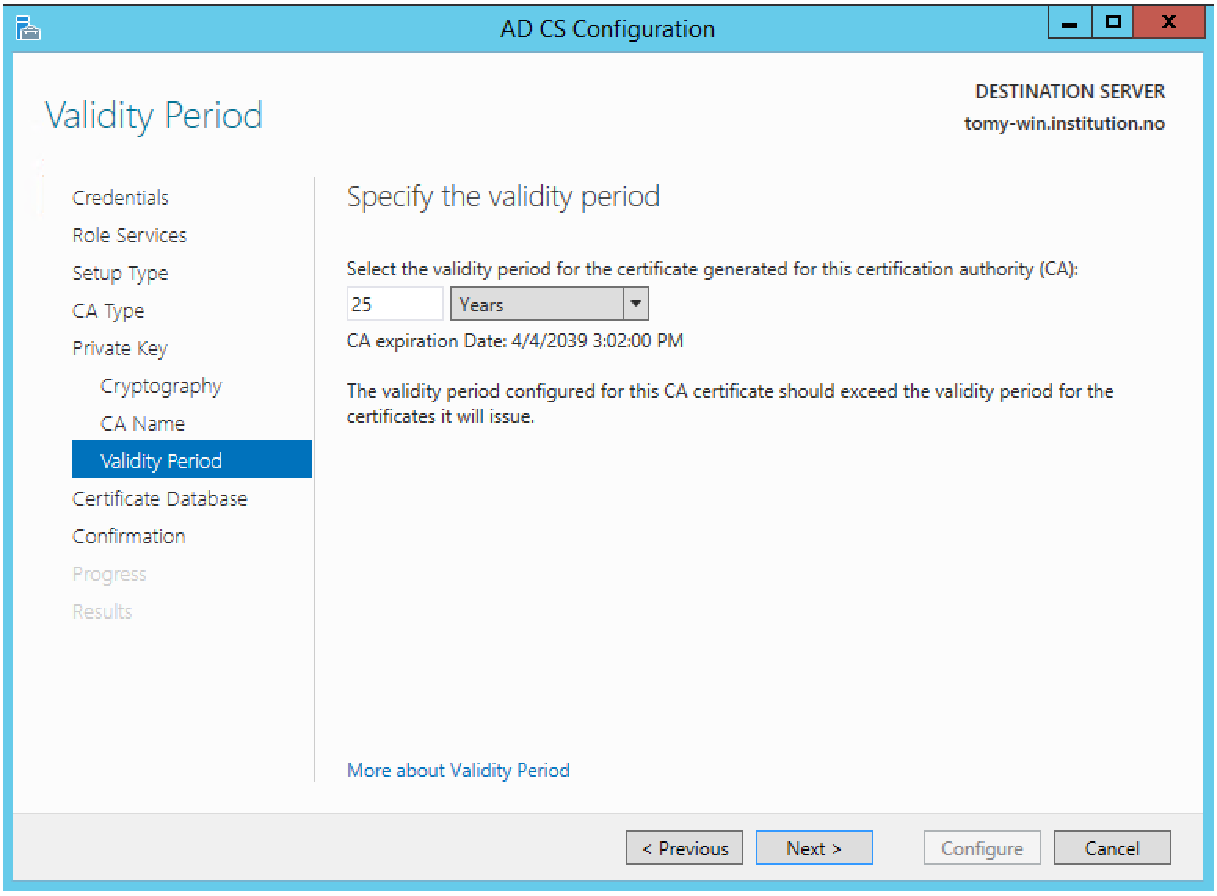
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: institution-CA

Distinguished name suffix: DC=institution,DC=no

Preview of distinguished name: CN=institution-CA,DC=institution,DC=no

Choose a long validity period (this is when the CA expires, it is also when all eduroam clients will need new CA cert):



Specify the validity period

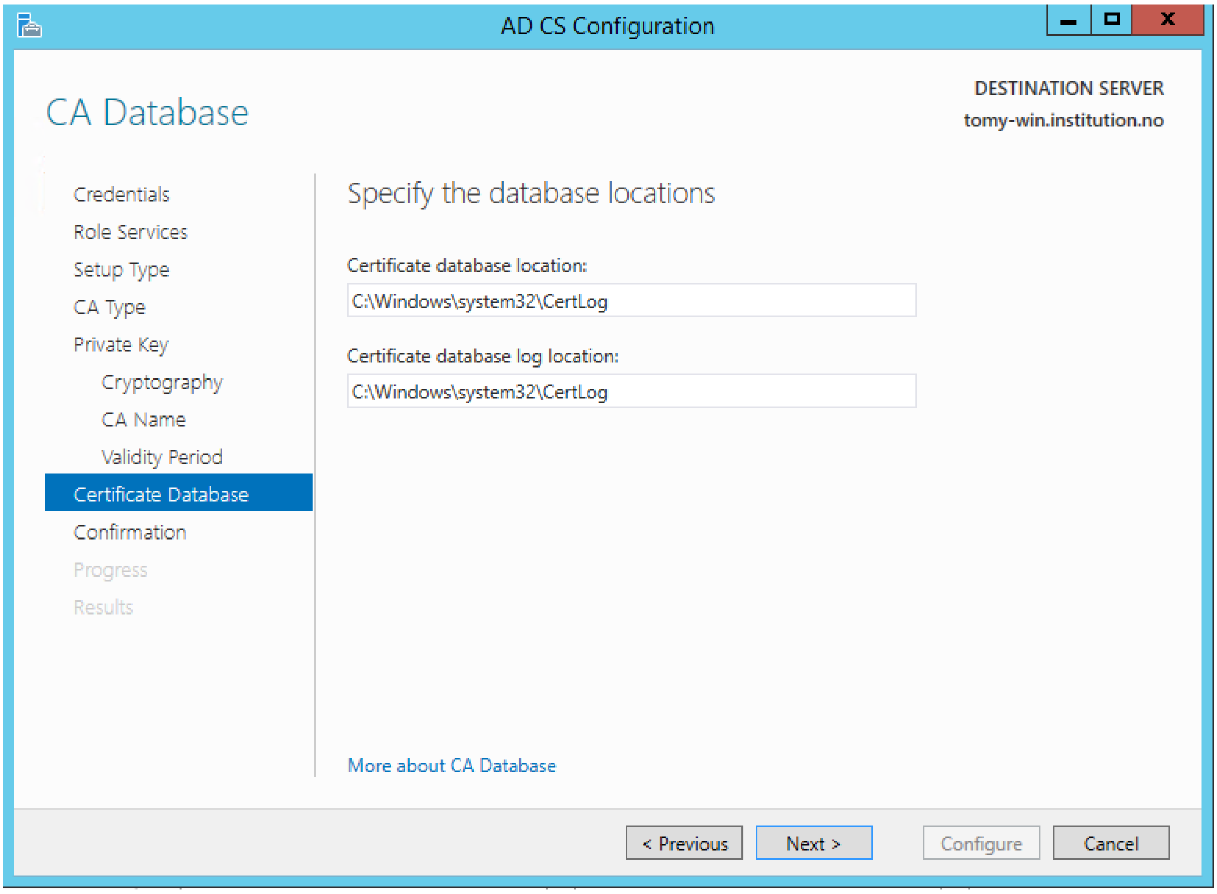
Select the validity period for the certificate generated for this certification authority (CA):

25 Years

CA expiration Date: 4/4/2039 3:02:00 PM

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

In Certificate Database, accept the default database locations:

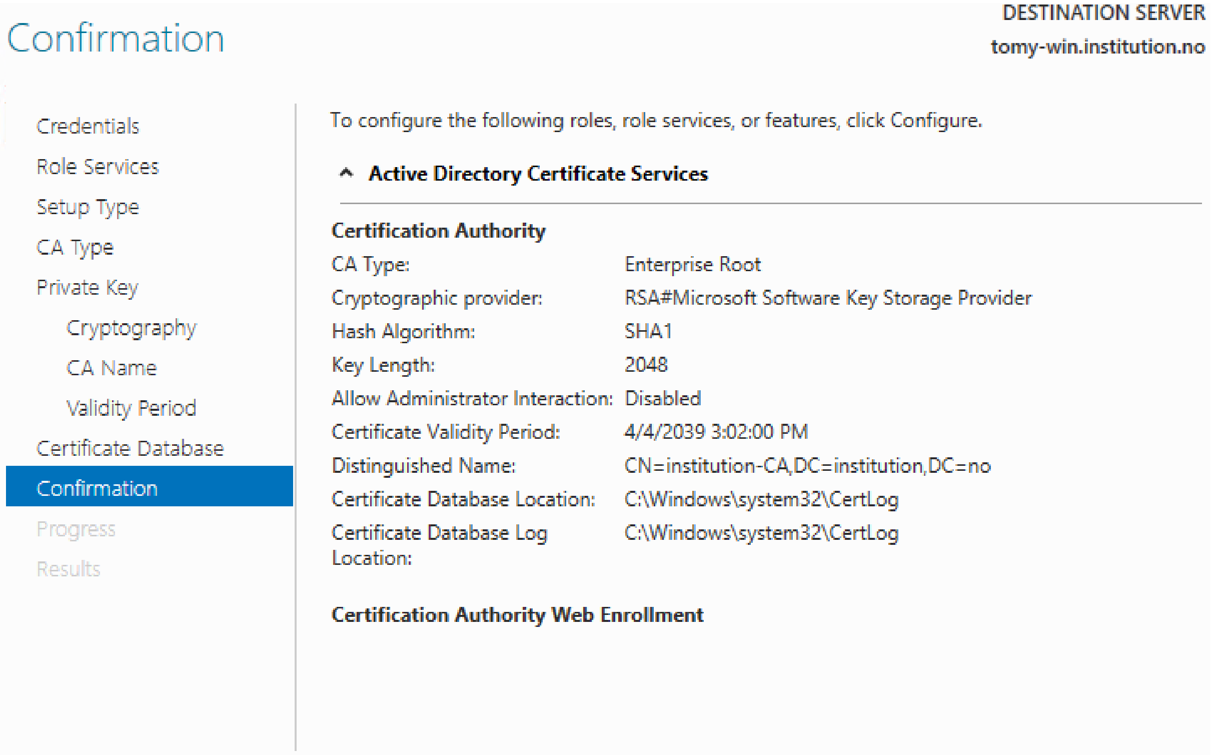


Specify the database locations

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

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

Review the configuration and press **Configure**:



Confirmation

DESTINATION SERVER
tomy-win.institution.no

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	4/4/2039 3:02:00 PM
Distinguished Name:	CN=institution-CA,DC=institution,DC=no
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Certification Authority Web Enrollment

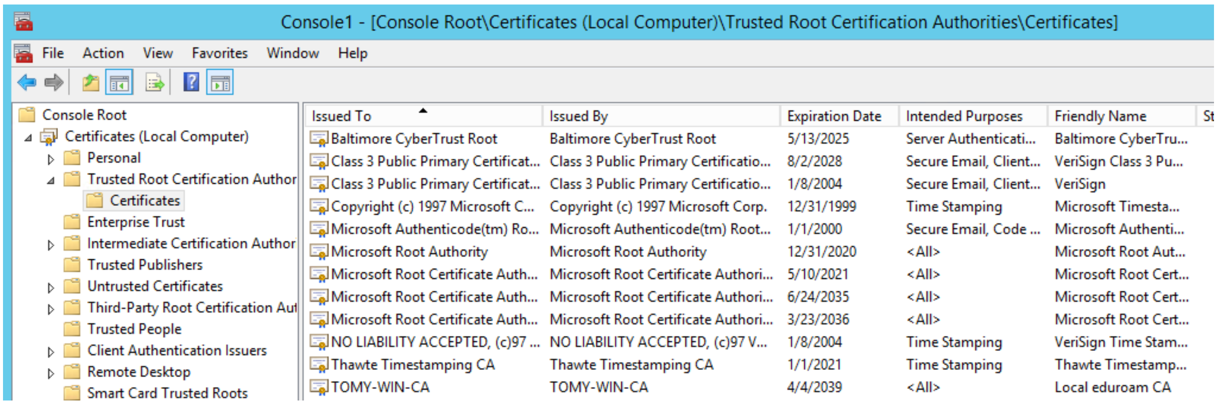
Note:

Some clients (Win XP and above) require the certificate extension "TLS Web Server Authentication" (OID 1.3.6.1.5.5.7.3.1) to be present.

This is how to achieve this:

Open MMC on your server – **File** > **Add snap** > **Certificates**.

You will find the CA certificate here:

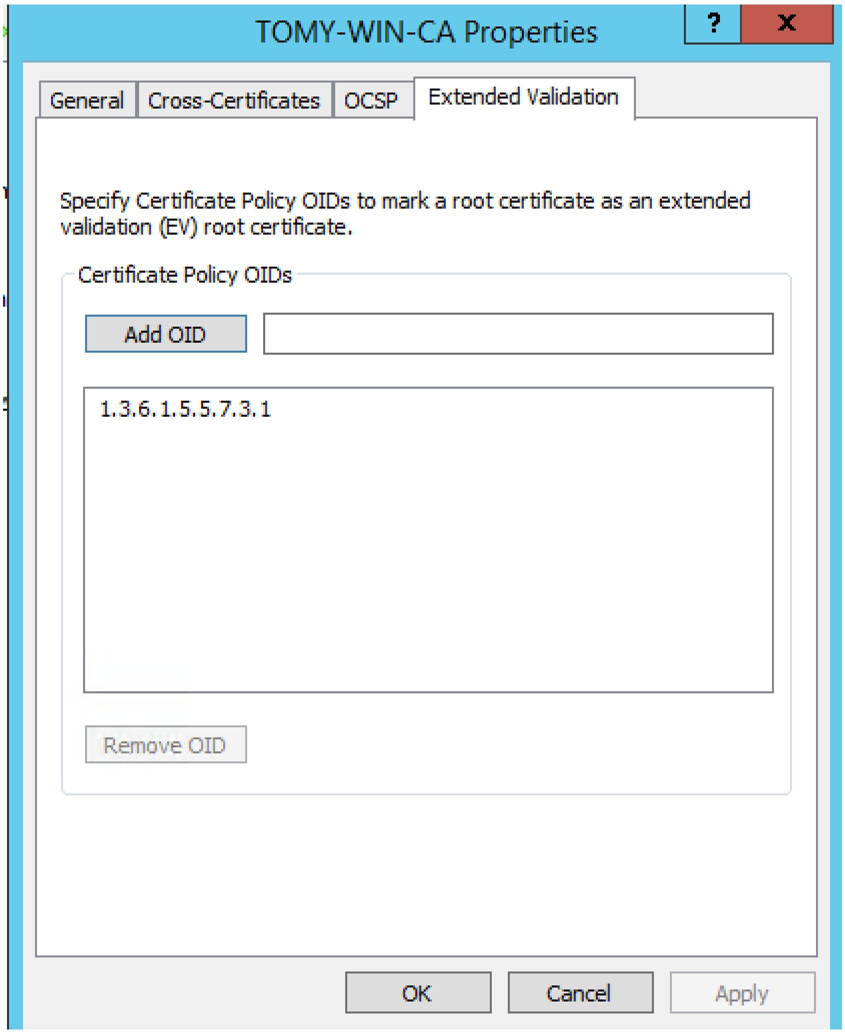


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	St
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Server Authenticati...	Baltimore CyberTru...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028	Secure Email, Client...	VeriSign Class 3 Pu...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/8/2004	Secure Email, Client...	VeriSign	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	Microsoft Timesta...	
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1/1/2000	Secure Email, Code ...	Microsoft Authenti...	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/10/2021	<All>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/24/2035	<All>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/23/2036	<All>	Microsoft Root Cert...	
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/8/2004	Time Stamping	VeriSign Time Stam...	
Thawte Timestamping CA	Thawte Timestamping CA	1/1/2021	Time Stamping	Thawte Timestamp...	
TOMY-WIN-CA	TOMY-WIN-CA	4/4/2039	<All>	Local eduroam CA	

Right click and choose **Properties** – go to the **Extended Validation** tab, then add the required OpenID (OID):

Click **OK**.



Specify Certificate Policy OIDs to mark a root certificate as an extended validation (EV) root certificate.

Certificate Policy OIDs

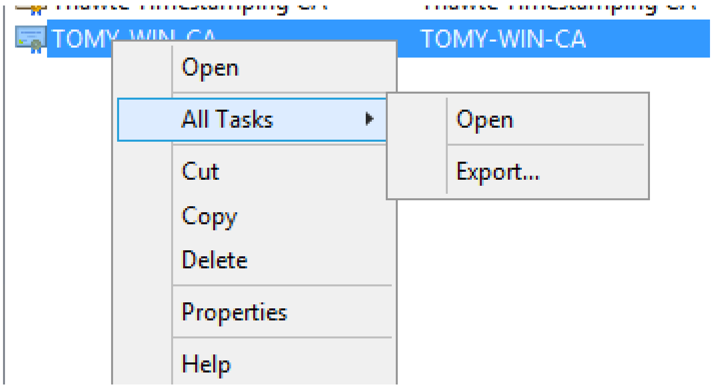
1.3.6.1.5.5.7.3.1

A.2 Distribute CA certificate to clients

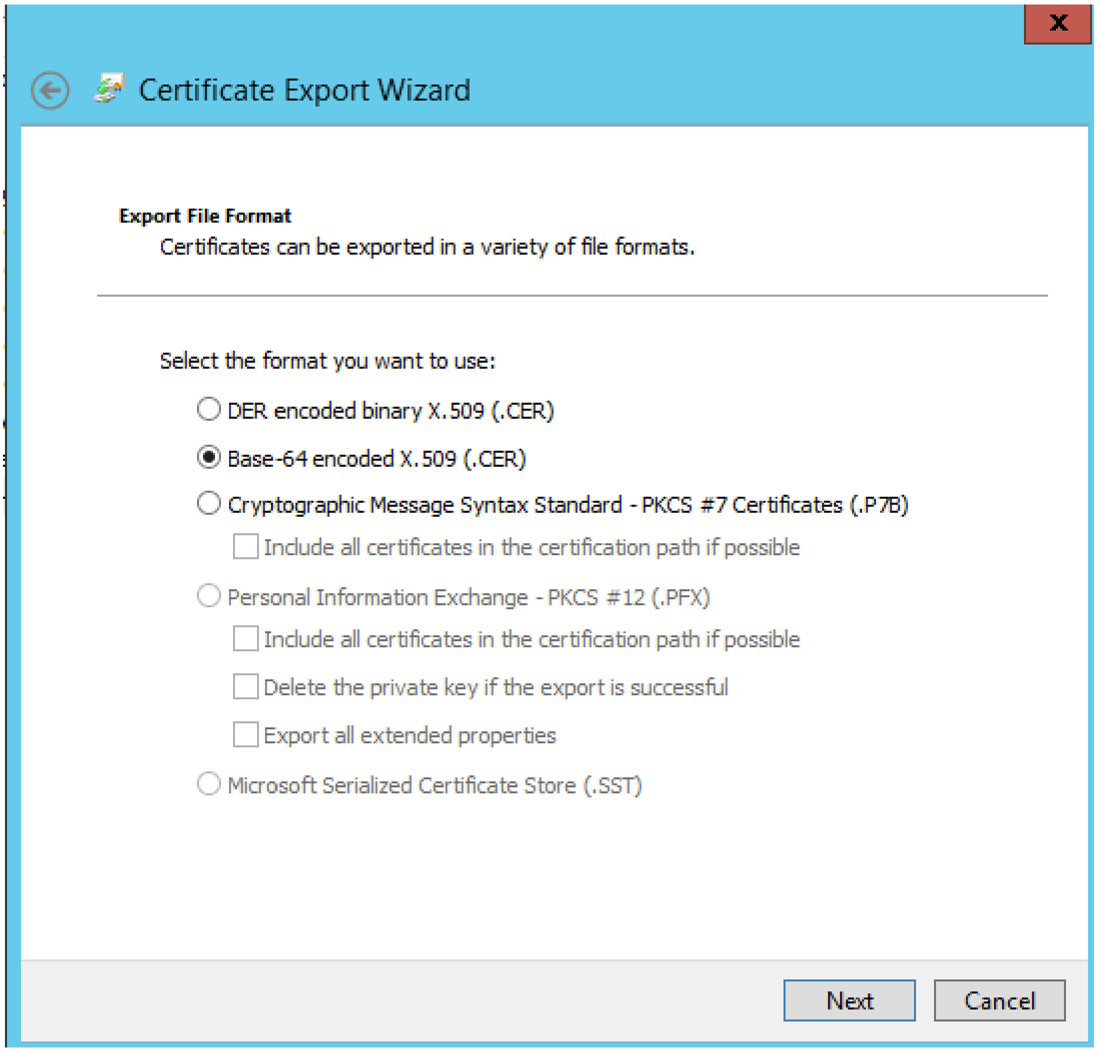
The CA root certificate must be present as Trusted Root Certification Authorities on all your eduroam clients. The recommended way is to distribute the CA certificate using CAT.

To have the CA transferred to CAT or otherwise to clients:

Right click the **CA** again and choose **Export**:



Next Select file format:


Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

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

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

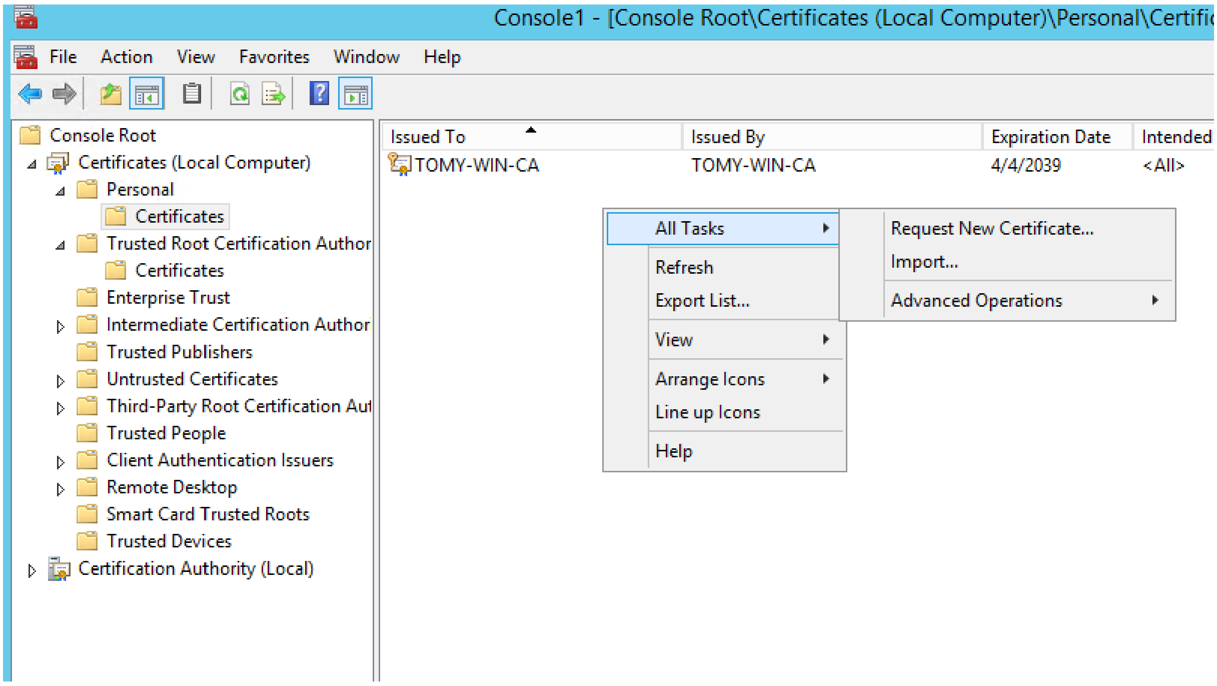
Save the file as for example <institution>_CA.cer – it is then ready for distribution. In a Win AD domain this can be done from the DC.

For clients outside the domain you need to go via CAT, distribute via email, intranet, USB memory stick or other method so that clients can install the CA Certificate.

A.3 Request and install server certificate for NPS

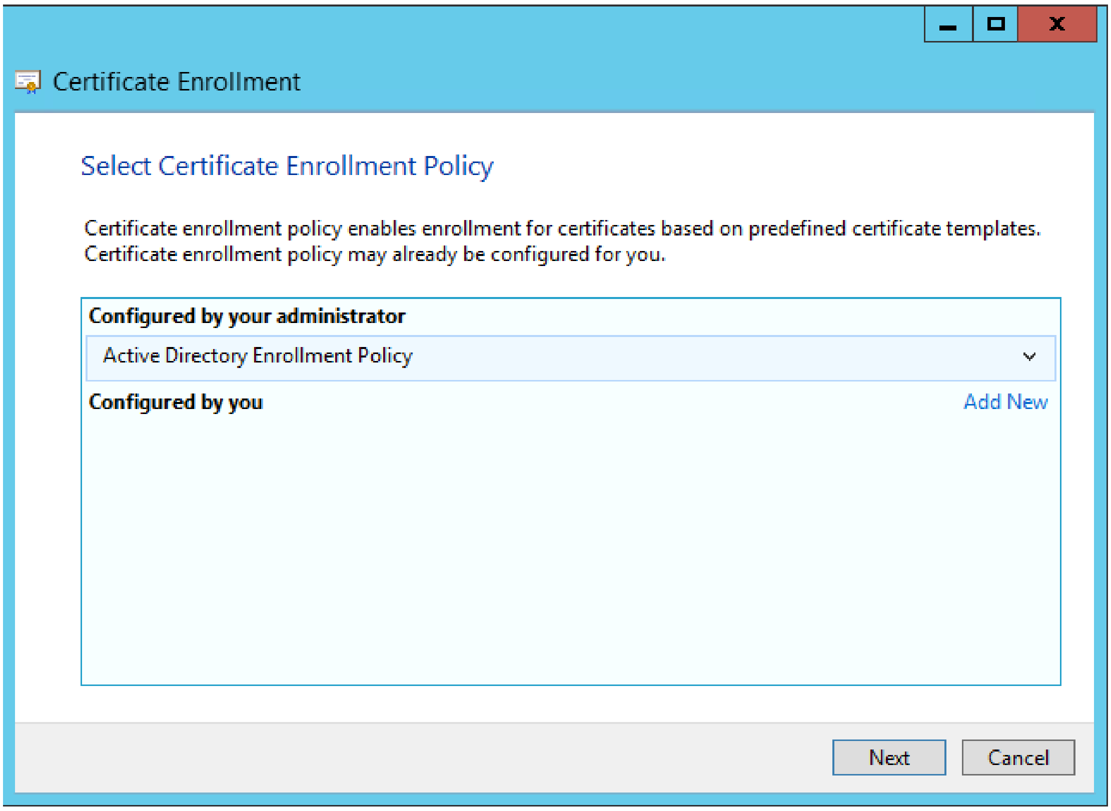
On the server running NPS:

1. Click **Start**, enter **mmc**, and press **Enter**.
2. Click **File** > **Add/Remove Snap-in**.
3. Choose **Certificates**, and click **Add**.
4. Choose **Computer account**, and click **Next**.
5. Select **Local Computer**, and click **Finish**.
6. Click **OK** to return to the Microsoft Management Console (MMC).
7. Expand the **Certificates (Local Computer**) and **Personal** folders, and click **Certificates**.
8. Right-click in the whitespace beneath the CA certificate, and choose **All Tasks** > **Request New Certificate**.



Issued To	Issued By	Expiration Date	Intended
TOMY-WIN-CA	TOMY-WIN-CA	4/4/2039	<All>

Click **Next**:


Certificate Enrollment

Select Certificate Enrollment Policy

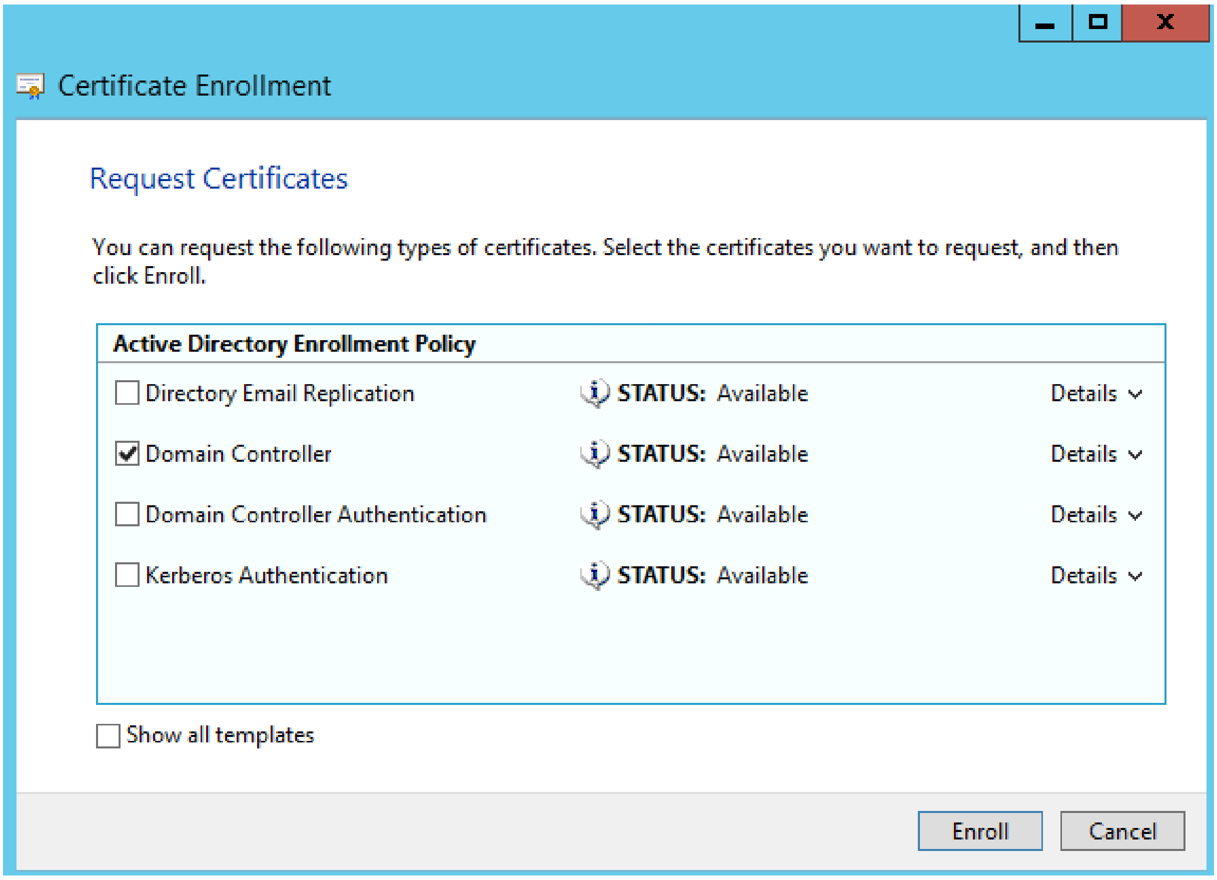
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates.
Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you

Select (tick) **Domain Controller**



Certificate Enrollment

Request Certificates

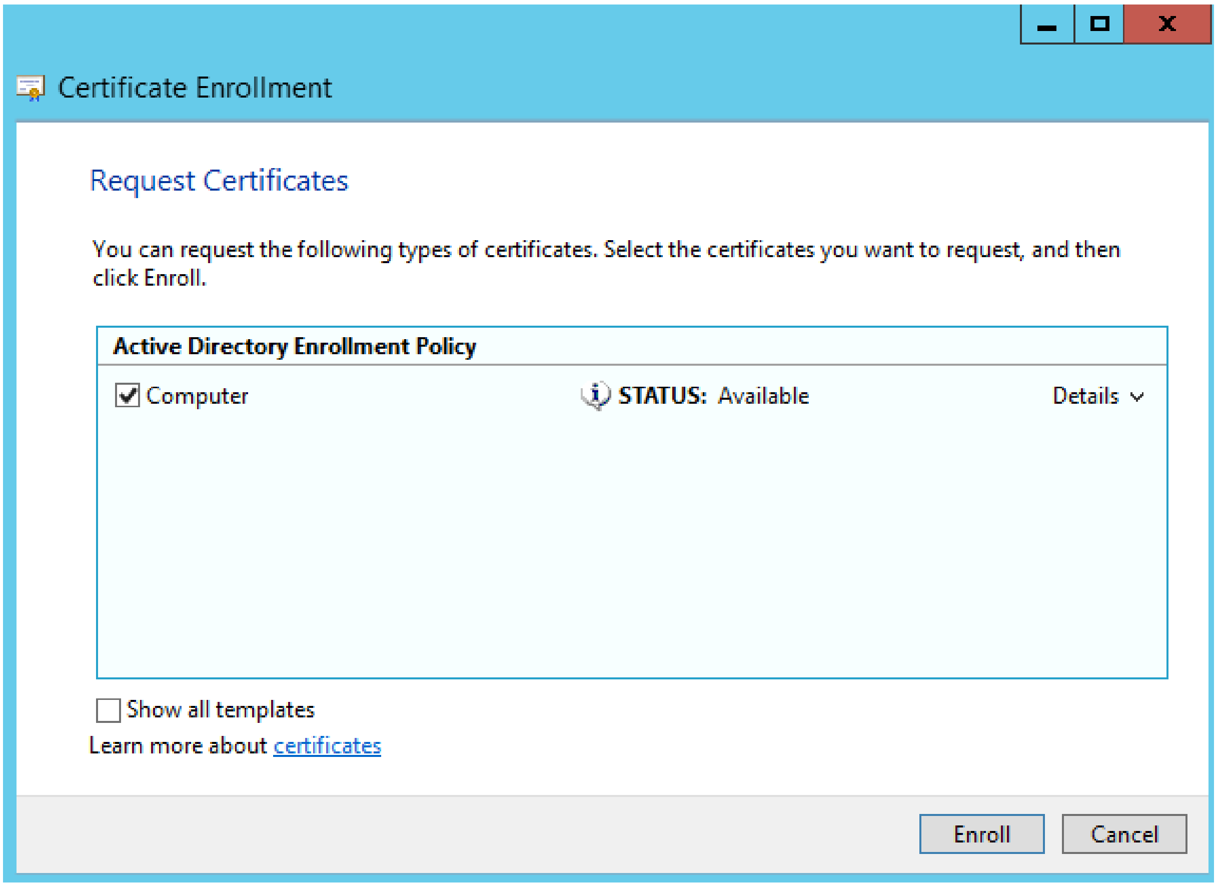
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Directory Email Replication	**STATUS:** Available	Details
☑ Domain Controller	**STATUS:** Available	Details
□ Domain Controller Authentication	**STATUS:** Available	Details
□ Kerberos Authentication	**STATUS:** Available	Details

□ Show all templates

Or select (tick) **Computer** – in the case of AD running on a separate server (this computer is an AD member running NPS):



Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

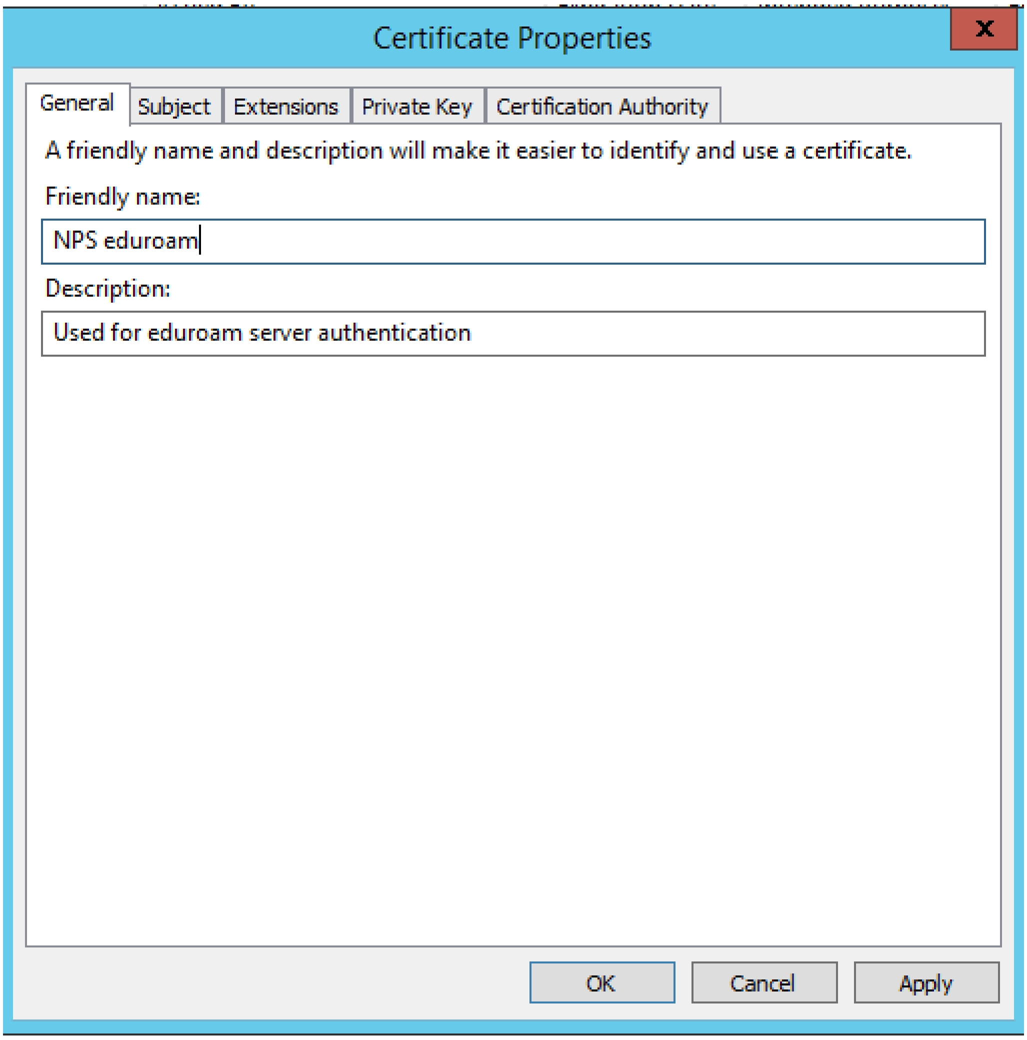
Active Directory Enrollment Policy

☑ Computer   **STATUS:** Available   Details ⌄

☐ Show all templates

Learn more about certificates

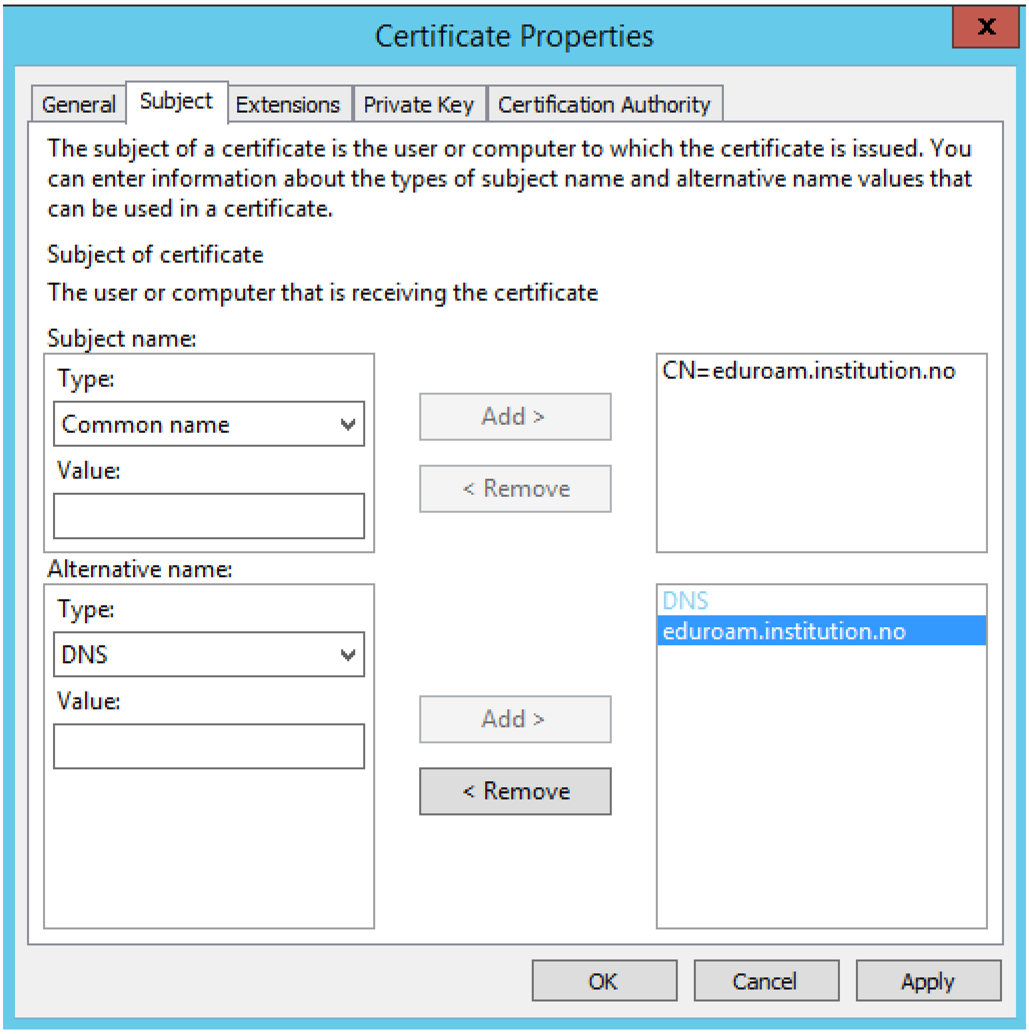
Before Clicking **Enroll** – click **Details** and adjust properties according to the screens below:



A friendly name and description will make it easier to identify and use a certificate.

Friendly name: NPS eduroam

Description: Used for eduroam server authentication



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:

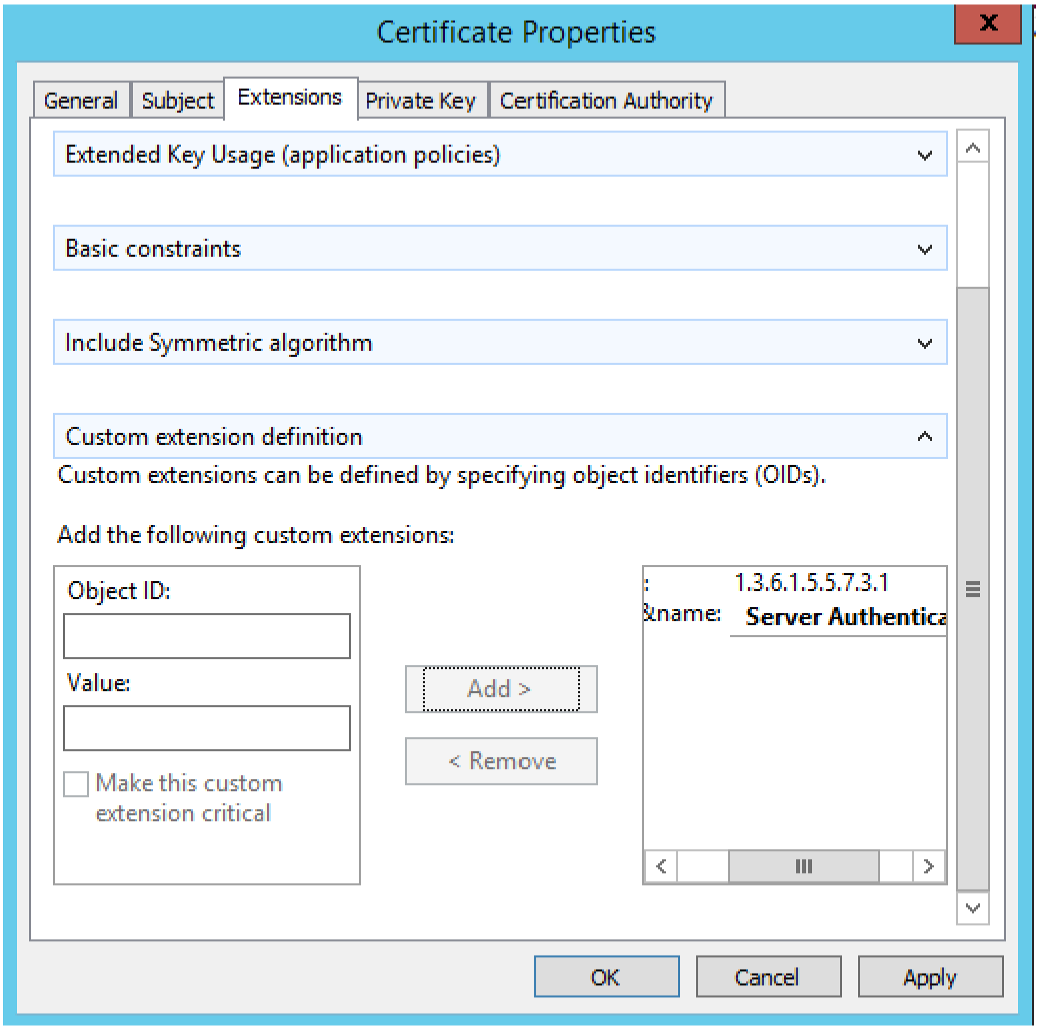
CN=eduroam.institution.no

Alternative name:

Type: DNS

Value:

DNS
eduroam.institution.no



Certificate Properties

General | Subject | Extensions | Private Key | Certification Authority

Extended Key Usage (application policies)

Basic constraints

Include Symmetric algorithm

Custom extension definition

Custom extensions can be defined by specifying object identifiers (OIDs).

Add the following custom extensions:

Object ID:

Value:

□ Make this custom extension critical

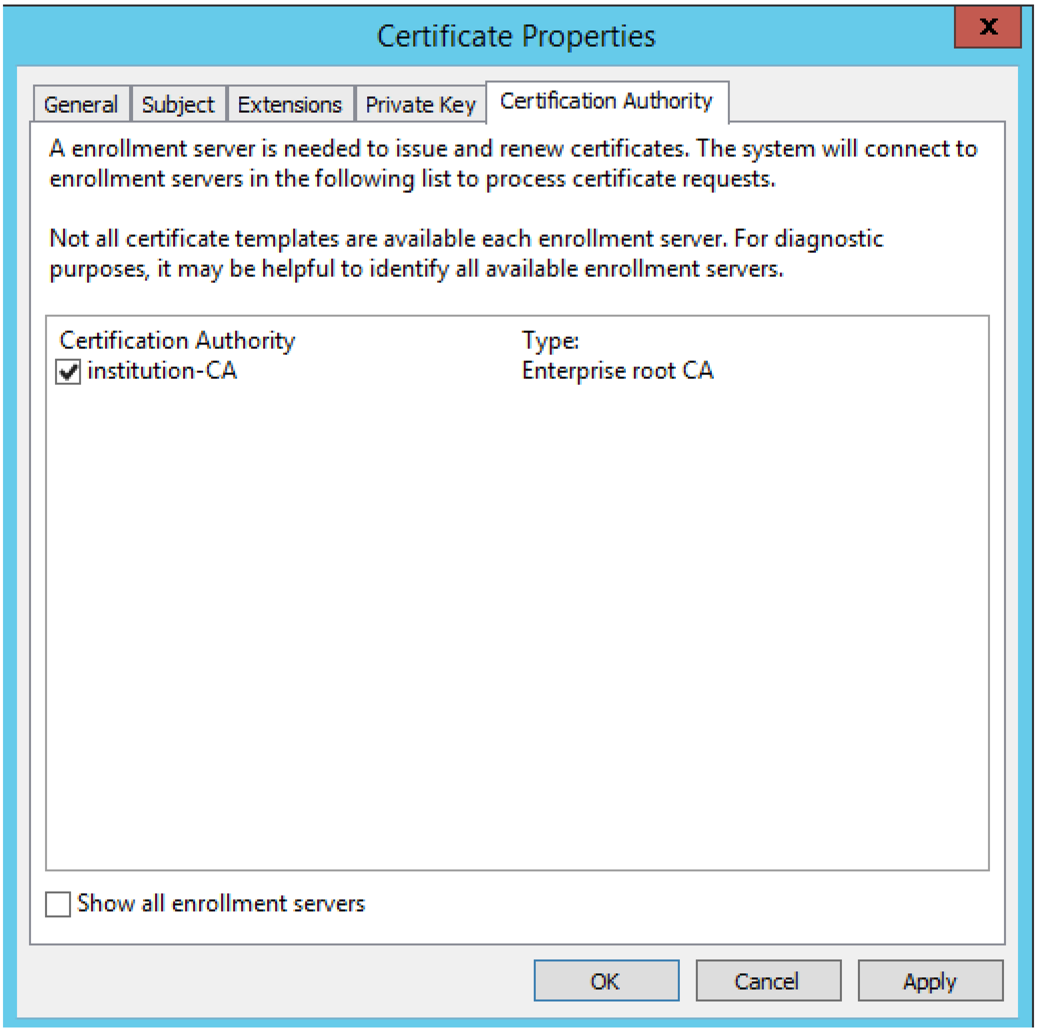
Add >

< Remove

: 1.3.6.1.5.5.7.3.1

&name: **Server Authentica**

OK | Cancel | Apply



A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests.

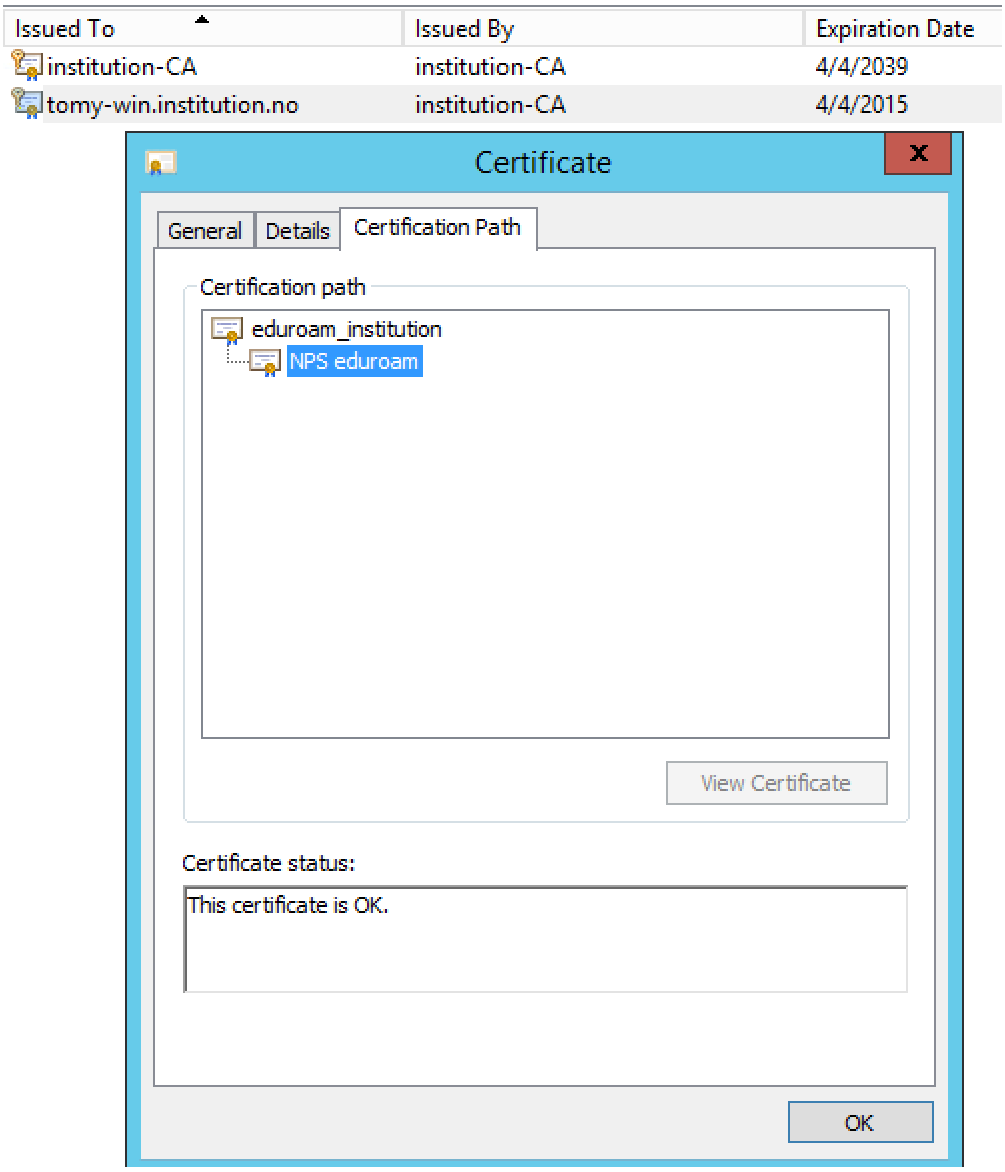
Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers.

Certification Authority	Type:
☑ institution-CA	Enterprise root CA

□ Show all enrollment servers

Then **Enroll** – and Finish.

In MMC you should now have both the CA and the server certificate:



Issued To	Issued By	Expiration Date
institution-CA	institution-CA	4/4/2039
tomy-win.institution.no	institution-CA	4/4/2015

Certification path

eduroam_institution
NPS eduroam

Certificate status:

This certificate is OK.

References

[PATTERN]	Pattern matching syntax for Windows Network Policy Server http://technet.microsoft.com/en-us/library/dd197583(v=ws.10).aspx
[TERENA]	EAP Server Certificate considerations https://confluence.terena.org/display /H2eduroam/EAP+Server+Certificate+considerations
[UFS112]	Recommended Security System for Wireless Networks http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs112.pdf

Other references not directly linked to this document:

Complete guide for deploying eduroam on-site or on campus
https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus

Guide to configuring eduroam using a Cisco wireless controller
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs127.pdf

Best Practice Document on “FreeRADIUS Database Connection”
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-freeradius-db.pdf

FreeRADIUS integration with AD
http://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO

Cisco example of setting up a Windows server with all components needed for 802.1X authentication
http://www.cisco.com/en/US/products/ps10315/products_configuration_example09186a0080bfb19a.shtml

Glossary

AD	Active Directory
CA	Certificate Authority (or Certification Authority)
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
EAP-PEAP	EAP - Protected Extensible Authentication Protocol
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunnelled Transport Layer Security
IdP	Identity Provider
IEEE 802.1X	Authentication mechanism for wired and wireless networks.
LDAP	Lightweight Directory Access Protocol
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol
NAS ID	Network Access Server IDentifier
NPS	Network Policy Server
NRO	National Roaming Operator
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Authentication Dial-In User Service; a protocol for authentication, authorisation and accounting

Complete BPDs are available at http://services.geant.net/cbp/Pages/Home.aspx

campus-bp-announcements@terena.org