

# Microsoft NPS Configuration Guide

## eduroam (UK)

---

Last Update: 12<sup>th</sup> April 2018

# Contents

1. Introduction.....	4
2. Limitations of Network Policy Server .....	5
3. Installing NPS .....	6
4. Certificates and Certificate Authority .....	10
5. Install and configure a Standalone Certificate Authority.....	12
6. Change the Certificate Authority - Validity period .....	22
7. Change the Certificate Authority - CRL Distribution Points .....	23
8. Creating the Server Certificate .....	25
9. Signing your certificate requests with your CA .....	33
10. Import the Server Certificate .....	39
11. Configure NRPS Shared Secrets Template .....	41
12. Add NRPS as RADIUS Clients .....	42
13. Add local Access Points / Wireless Infrastructure RADIUS Clients .....	44
14. Add NRPS as RADIUS Proxy Servers .....	45
15. Add a Connection Request Policy for your roaming users .....	48
16. Add a Connection Request Policy for local users .....	52
17. Add a Connection Request Policy for eduroam visitors .....	57
18. Reorder Connection Request Policies .....	60
19. Create Network Policy.....	61
20. Register server in Active Directory.....	68

## Changelog

Version	Modification	Author	Date
0.1	Original version posted to eduroam (UK) community site	Edward Wincott and eduroam (UK) team.	24 February 2015
0.2	Updated with further details and sections about CAs and Certificates.	Edward Wincott and Jon Agland	9 <sup>th</sup> March 2018
0.5 (current release)	Updated screenshots to 2016 versions. Re-order guide and replace all screenshots Change guidance on EAP override in Connection Request Policies Update userPrincipalName / Network Access Identifier considerations	Jon Agland	12 <sup>th</sup> April 2018

# 1. Introduction

This guide describes the setup of Microsoft Network Policy Server as your Organisational RADIUS Server (ORPS) for use with eduroam in the UK. Whilst the ORPS is the key component of your eduroam deployment there are a number of other important elements and this guide must be read in conjunction with the following documents:

- i) Implementing eduroam Roadmap <https://community.ja.net/library/janet-services-documentation/implementing-eduroam-roadmap>
- ii) the eduroam(UK) Technical Specification <https://community.ja.net/library/janet-services-documentation/eduroamuk-technical-specification>
- iii) Attribute Filtering for Microsoft IAS and NPS: <https://community.ja.net/library/janet-services-documentation/radius-attribute-filtering-microsoft-ias-and-nps>

There are also additional technical reference documents and advisory notices published in the Jisc Community Library web site with which the eduroam sys admin should familiarise him or herself.

Whilst this guide is sufficient to enable you to set up a basic eduroam deployment, it does not cover setup of further (non-eduroam) VLANs and dynamic assignment of users to such VLANs, which you may wish to implement for the support of your local users connecting with their own devices or for connecting local users to VLANs giving access to restricted resources and/or which could have content filtering applied.

For Home sites, you will also need to consider 'on-boarding' of user devices, most effectively achieved through the use of automation tools such as **eduroam CAT** which generates installer utilities. If there are difficulties with internet access via mobile data, then possibly setting up a 'walled garden' service to provide users with access to your CAT installer utilities is also possible see **Walled Garden for on-boarding user devices to eduroam**

This guide does not cover logging and accounting, which is covered in Section 6 of the GÉANT guide: **CBP-13 Using Windows NPS as RADIUS in eduroam**

The examples in this document are collected from a mix of both Windows Server 2016, although will be relevant to older versions such as Windows Server 2012 and Windows Server 2008 R2 Enterprise. The dialogue screens differ slightly between the two versions, but the configuration items are very similar.

## Pre-requisites:

It is assumed that you have provisioned a suitable server platform, installed Microsoft Windows Server and that suitable connectivity is in place to your wireless access points/controller and to the internet and that the server has a fully qualified domain name and fixed IP address reachable by the eduroam(UK) national proxy servers. It is also assumed that you have a basic setup of Active Directory.

# Acknowledgements

This guide contains material drawn in part from the Best Practice Document 'Using Windows® NPS as RADIUS in eduroam' published by the GÉANT Association and such material is included in this guide under the free license terms specified on page (ii) of that document. Copyright of such material remains the property of GÉANT.

## 2.Limitations of Network Policy Server

Network Policy Server (NPS) is the Microsoft Windows implementation of a Remote Access Dial-in User Service (RADIUS) server and proxy. NPS is a popular choice amongst organisations deploying eduroam due to its accessibility, familiar graphical user interface and low cost. However, it should be recognised that for use as your organisational RADIUS proxy server (ORPS) it has certain limitations and lesser flexibility than the likes of FreeRADIUS and Radiator etc.

The limitations mean that whilst a perfectly serviceable solution can be put in place, your eduroam deployment will not meet all of the best practice recommendations described in the eduroam(UK) Technical Specification and certain 'warn' flags will be indicated in the eduroam(UK) Support portal.

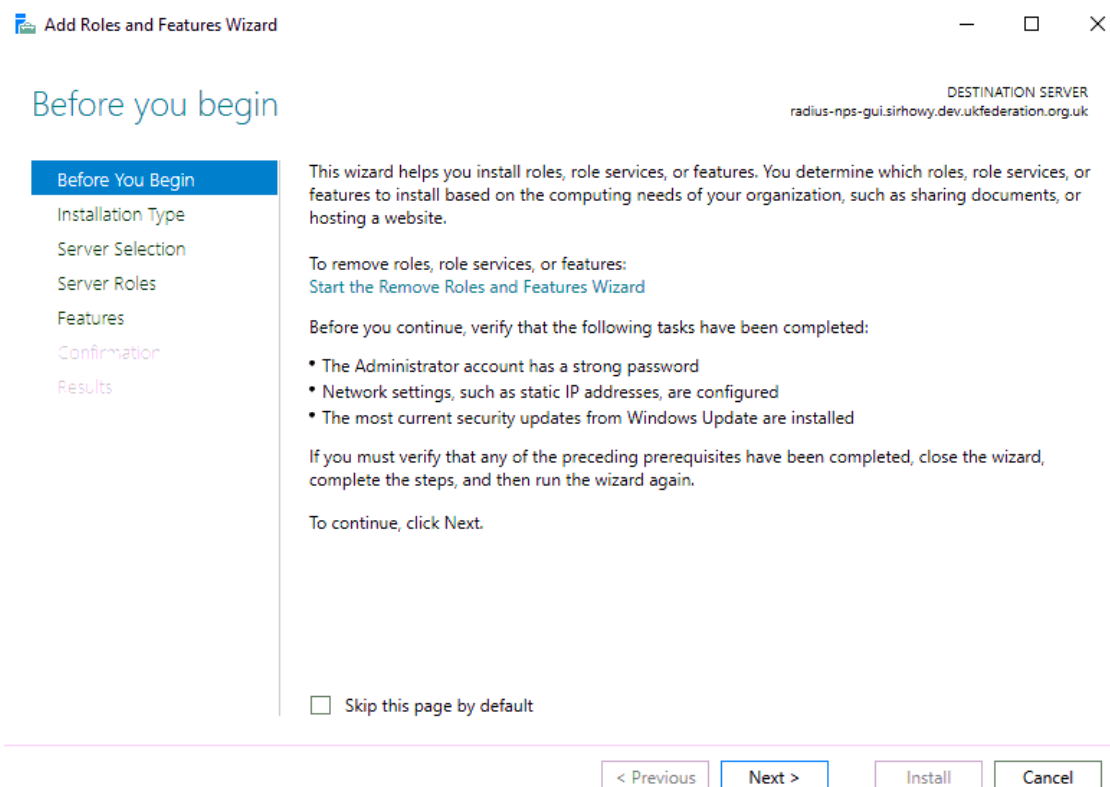
The following limitations are addressed, where applicable, in the instructions contained later in this guide:

- You cannot add RADIUS attributes into outbound authentication requests your ORPS sends to the eduroam(UK) national proxies (NRPSs). In particular adding an 'Operator-Name' attribute to indicate the organisation where a visitor is connecting is not possible in NPS. Since the presence of Operator-Name is desirable for troubleshooting purposes (and also for working with CUI) it is on the eduroam(UK) development roadmap to introduce Operator-Name insertion at the NRPS, therefore this limitation can be mitigated.
- NPS does not support Status-Server and will not respond to Status Server requests. Status-Server is the best practice method for RADIUS servers to check the availability of peered servers, the alternative being to utilise retries and timeouts. It is on the eduroam(UK) development roadmap to introduce Status-Server checks with ORPS, but NPS servers will not be able to benefit from this and will continue to rely on current methods.
- RADIUS attributes cannot be stripped from authentication requests by NPS. They can only be overwritten. It is desirable for your ORPS to be able to strip or overwrite attributes, for instance an Access-Accept returned for a visitor by the user's home organisation may contain VLAN attributes that are only relevant for that user on the home campus (to enable the user to be connected to a group VLAN), but such VLAN attributes may cause problems on your network. To avoid these problems you will need to explicitly set VLAN values applicable to your environment if you work with VLANs and set other values to prevent invalid attributes.
- The 'outer' username (used in phase 1 of the authentication process to identify the user's home organisation) can be rewritten (via the Connection Request Policy) as an 'anonymous@realm', whereas the 'inner' username (the encrypted identifier used for user authentication) which is handled by the Network Policy, cannot be modified. (Nb. often users configure inner and outer identities to be the same).
  - The effect of this is that your users will have to use their respective userPrincipalName to authenticate as their user@realm -their Network Access Identifier (RFC7542)-, in many case this looks similar to an e-mail address.
  - If your UPN suffix and resulting userPrincipalName's use an unregistered domain name such as those ending '.local', then you may be best to consider adding a UPN Suffix and changing the userPrincipalName for affected users. If not, there will additional requirements such as:
    - Additional Connection Request Policies, with Attribute rules see [using the pattern matching syntax in NPS](#)
    - Users being mandated to use separate inner and outer identities.

- In respect of your Home (IdP) service provision, using anonymous outer identities is not possible, unless Override network policy authentication settings is enabled in the Connection Request Policies. We recommend that this is used, but this may have an effect on “Constraints and Settings” in “Network Policies”.
- 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**. The Add Roles Wizard will open – read the information text and accept the default by clicking **Next**.



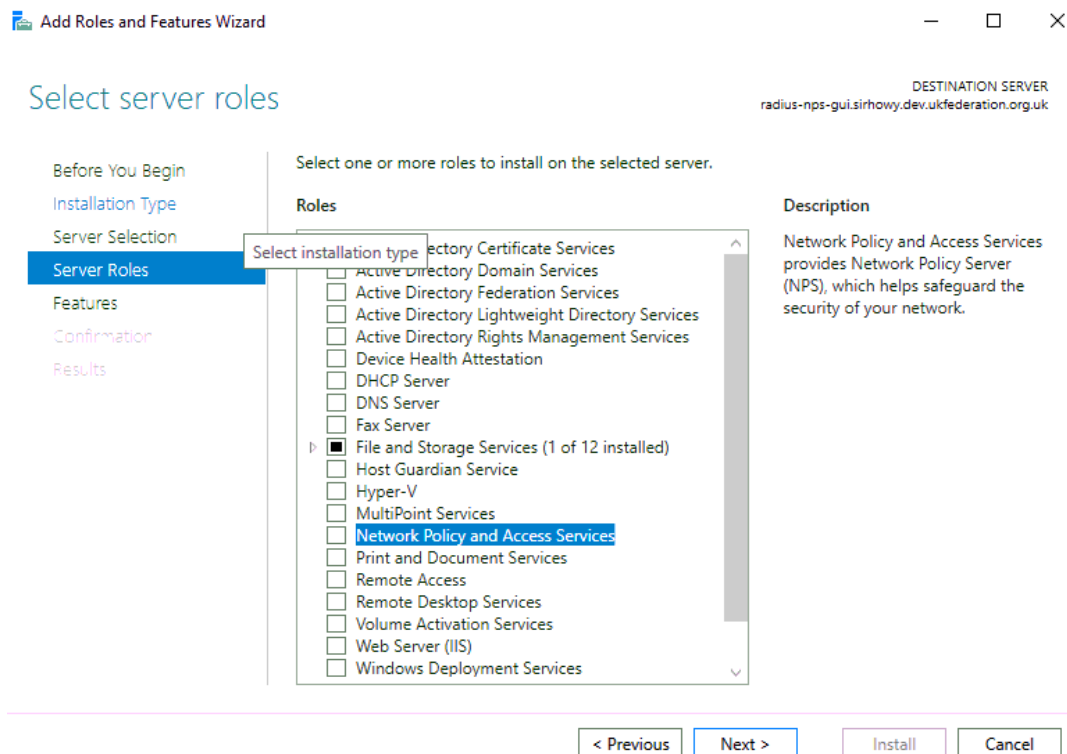
On the following screen you should choose **Role-based or feature-based installation**

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select installation type'. On the left, a navigation pane lists: 'Before You Begin', 'Installation Type' (highlighted), 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area has a sub-heading '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)'. There are two radio button options: 'Role-based or feature-based installation' (selected) and 'Remote Desktop Services installation'. The 'Role-based or feature-based installation' option has a description: 'Configure a single server by adding roles, role services, and features.' The 'Remote Desktop Services installation' option has a description: 'Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.' At the top right, it says 'DESTINATION SERVER radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

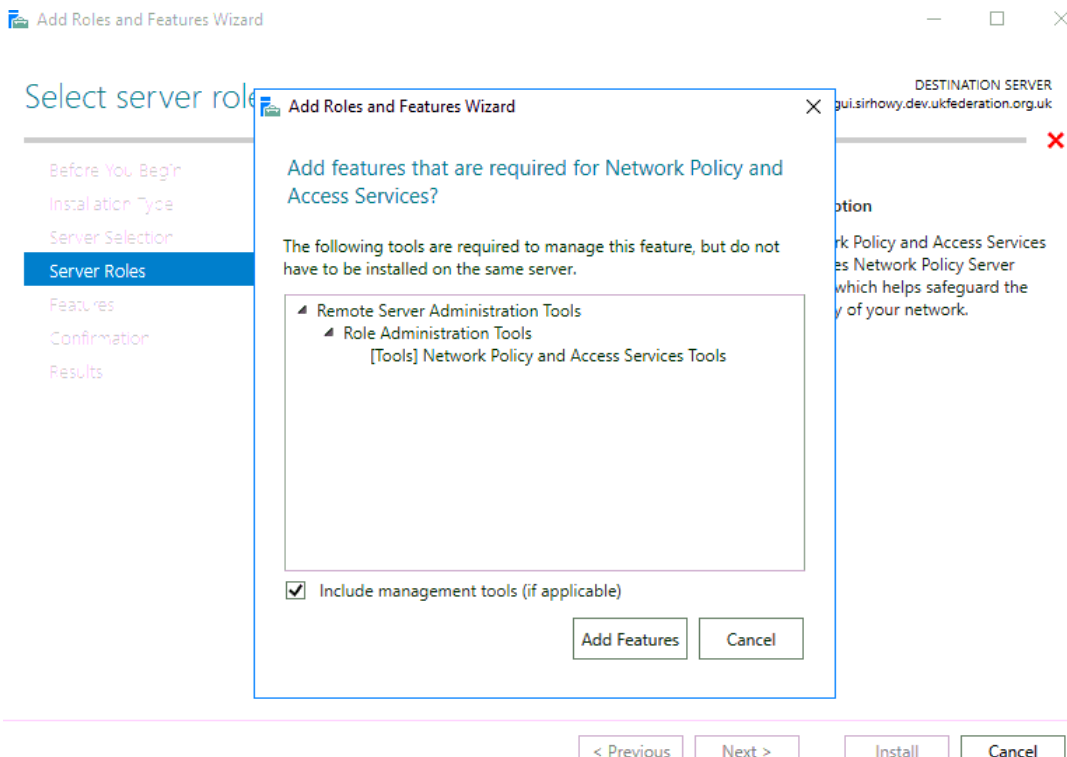
You wish to install **Select a server from the server pool** on. This is likely to be the server that you are currently using.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. On the left, a navigation pane lists: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area has a sub-heading 'Select a server or a virtual hard disk on which to install roles and features.' There are two radio button options: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Below the options is a section titled 'Server Pool'. It contains a 'Filter:' text box. Below that is a table with three columns: 'Name', 'IP Address', and 'Operating System'. The table has one row: 'radius-nps-gui.sirhowy.d...' | '172.16.196.24' | 'Microsoft Windows Server 2016 Standard'. Below the table, it says '1 Computer(s) found'. At the bottom, there is a paragraph: 'This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the top right, it says 'DESTINATION SERVER radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

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

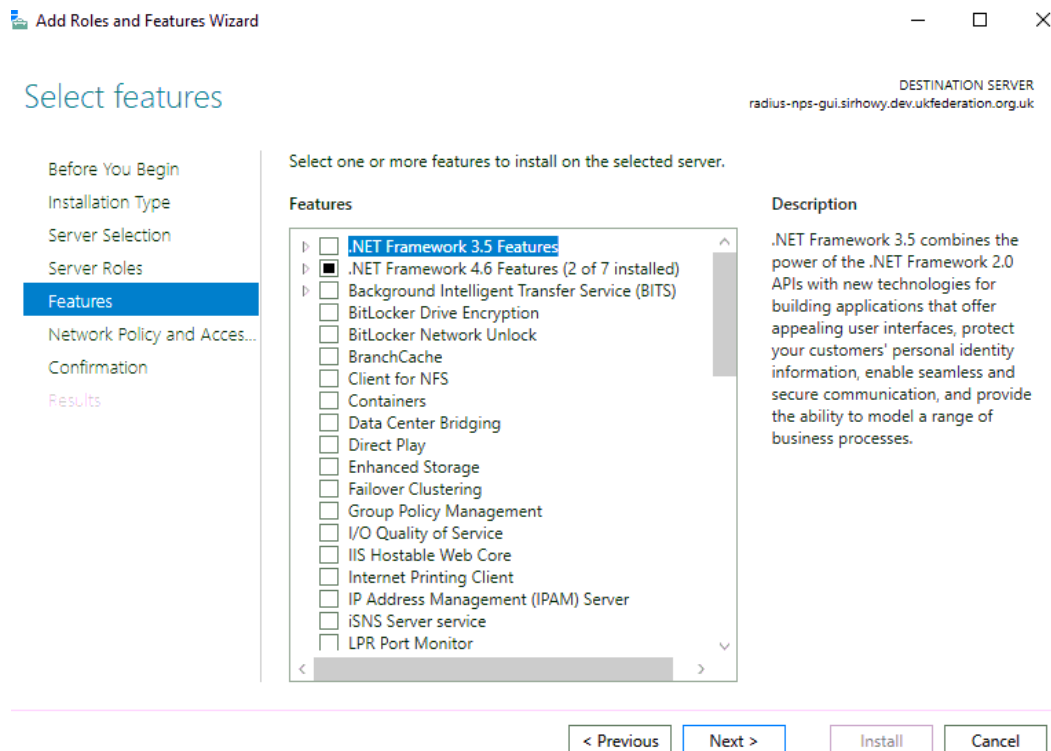


The following dialogue will appear, click **Add Features**, when you return to the **Add Roles and Features Wizard** click **Next**

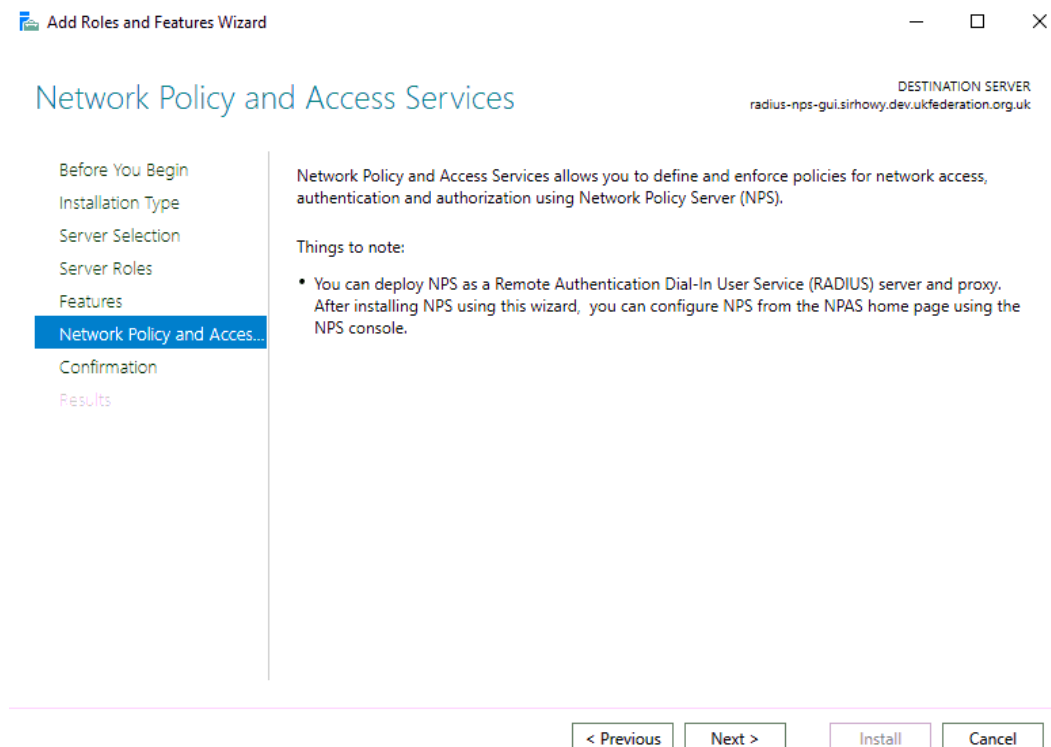




No additional features are required, click **Next**



Read this page, and click **Next**



Hit **Install** on the confirmation dialogue, it is unlikely you will need to restart the server.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Confirm installation selections'. On the right, it says 'DESTINATION SERVER' with the URL 'radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. A left-hand navigation pane lists steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'Network Policy and Acces...', 'Confirmation' (highlighted in blue), and 'Results'. The main area contains the text: 'To install the following roles, role services, or features on selected server, click Install.' Below this is a checkbox labeled 'Restart the destination server automatically if required'. A paragraph follows: '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.' A box lists the following items: 'Network Policy and Access Services', 'Remote Server Administration Tools', 'Role Administration Tools', and 'Network Policy and Access Services Tools'. At the bottom of the main area are links: 'Export configuration settings' and 'Specify an alternate source path'. At the very bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

## 4. Certificates and Certificate Authority

Most organizations would like to act as a Home participant (IdP) and to authenticate its own users. PEAP-MSCHAPv2 and EAP-TLS authentication methods, in common with all other EAP methods (with the exception of EAP-PWD - which is not supported in NPS) require an X.509 server certificate to be installed on the authenticating RADIUS server. The certificate is used to establish the secure authentication tunnel and by the RADIUS server to identify itself to the user's device.

Should you decide to participate only as a Visited (Wi-Fi service provider for visitors only) participant, you don't need a certificate and your ORPS can act as a proxy to receive requests from Wi-Fi access points, to log, filter, and forward authentication requests to the eduroam(UK) infrastructure. Most organisations participate as both Home and Visited service providers and so the ORPS needs to have a server certificate.

PEAP-MSCHAPv2 is the most commonly used authentication method in the Microsoft environment since it utilises username and password credentials, which are easy to distribute and PEAP is straightforward to set up on NPS.

PEAP (Protected Extensible Authentication Protocol) sets up a secure tunnel using TLS (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. 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 the public certificate of the Certification Authority (CA) installed already. This will issue and sign the NPS server's certificate. The CA certificate may be distributed using e-mail, a web page such as eduroam CAT (eduroam Configuration Assistant Tool), or a management system such as AD Group Policy. The client checks the validity of the RADIUS server's certificate using the CA certificate. The client should also check the name (CommonName and/or SubjectAltName) of the certificate.

You can use a server certificate from a public commercial certificate authority; such certificates are available from the very cost effective **Jisc Certificate Service** through which you will pay a fraction of the cost of commercial providers. This will save you having to set up your own 'local' CA service, manage certificates and distribute your public certificate to your users' devices. However commercial CAs certs do have an expiry date, so periodically a large administrative task will be encountered. If you are taking this option then you can skip to Section 8. Creating a Server Certificate.

If you set up your own 'local' CA, rather than using certificates from a large commercial CA, the possibility of phishing is reduced since commercial CA certificates are readily available and could be used in exploits such as Man-in-the-Middle attack, whereas as with a local CA you controls generation of the public CA certificate and can assure its use is restricted to your own servers. If you are taking this option you should continue into the next section; Section 5. Install and configure a Standalone Certificate Authority.

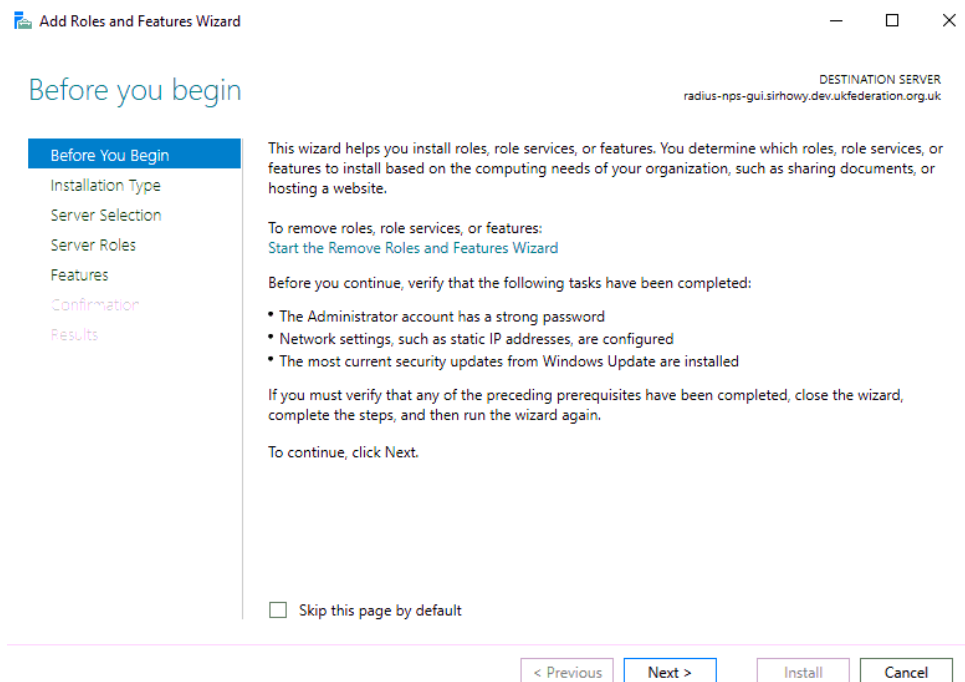
Other options such as using an existing Enterprise Certificate Authority are available too, but not documented here.

If taking that option ensure that your CAs lifetime is long for example 20+ years. This will be the certificate that goes onto end user devices, so you would like to avoid the need of replacement as little as possible. You should add a valid CRL Distribution point added, this will be a URL that should reference a domain name that you have control over and could feasibly host a file if required for example <http://www.camford.ac.uk/eduroam-ca.crl>. See Section 7. Change the Certificate Authority - CRL Distribution Points

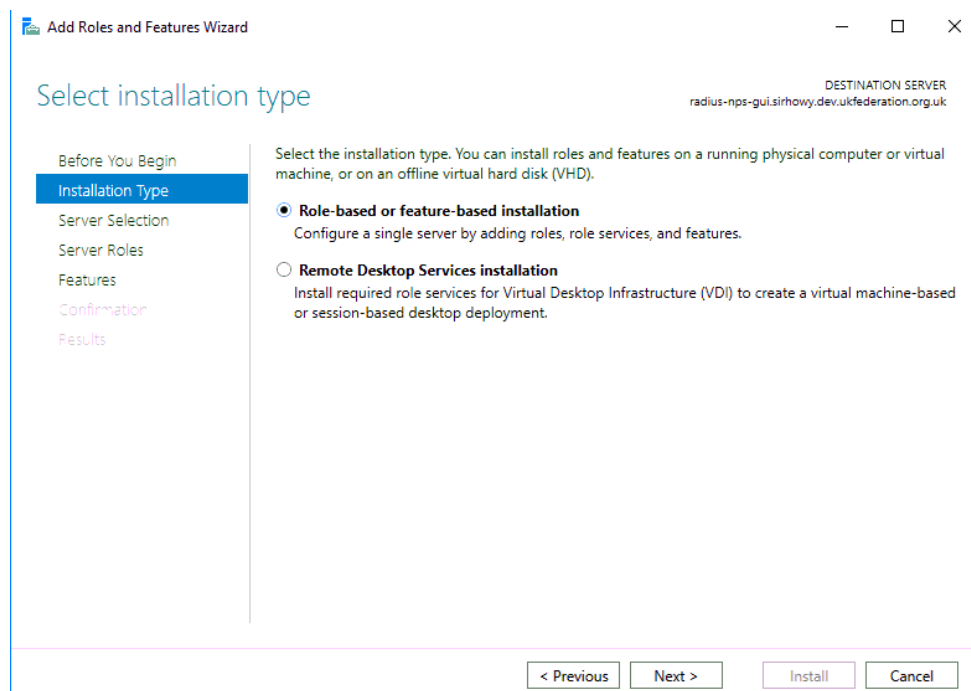
You should also tweak the default validity of the certificates issued by your CA as the default one year is too short, you could align this to the lifetime of the CA or slightly greater. See Section 8. Change the Certificate Authority - Validity period

## 5. Install and configure a Standalone Certificate Authority

From **Server Manager**, Choose **Add and Remove Roles**.



On the following screen you should choose **Role-based or feature-based installation**



Select a server from the server pool you wish to install this on. This is likely to be the server that you are currently using.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. On the right, it says 'DESTINATION SERVER radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area has the instruction 'Select a server or a virtual hard disk on which to install roles and features.' and two radio buttons: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Below this is a 'Server Pool' section with a 'Filter:' text box. A table lists the server pool members:

Name	IP Address	Operating System
radius-nps-gui.sirhowy.d...	172.16.196.24	Microsoft Windows Server 2016 Standard

Below the table, it says '1 Computer(s) found'. A note states: 'This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

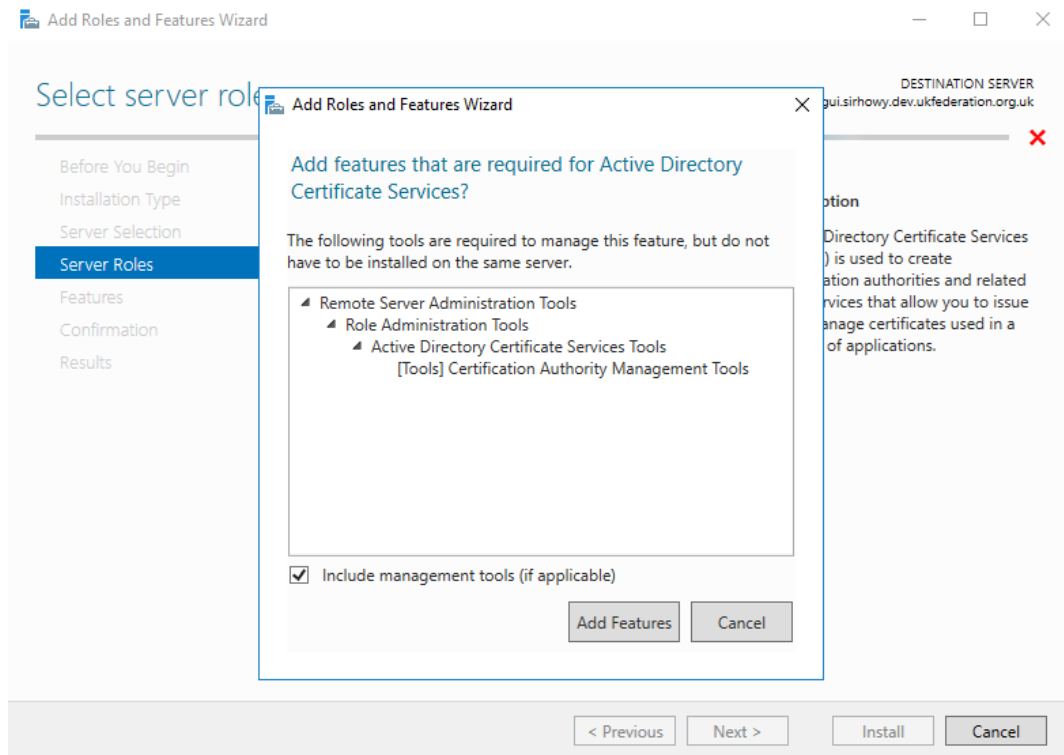
Select the **Active Directory Certificate Services** role

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select server roles'. On the right, it says 'DESTINATION SERVER radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles' (highlighted), 'Features', 'Confirmation', and 'Results'. The main content area has the instruction 'Select one or more roles to install on the selected server.' and a list of roles under the heading 'Roles'. The roles are:

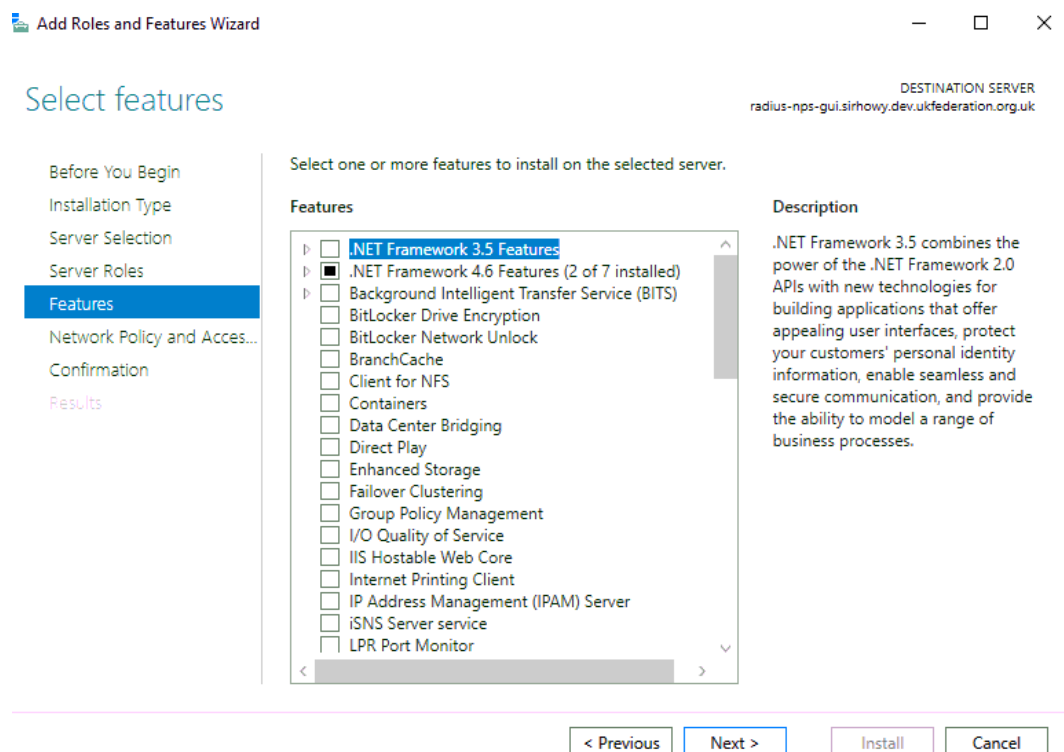
- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☒ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☒ Network Policy and Access Services (Installed)
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

On the right, under the heading 'Description', it says: '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.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

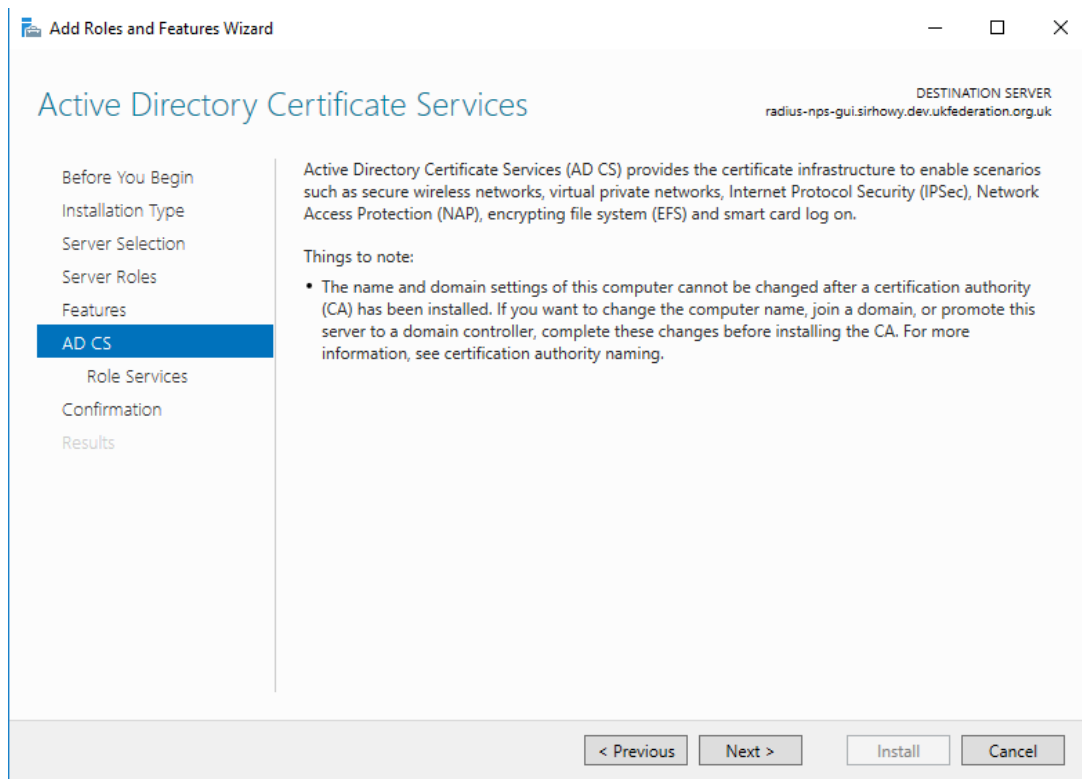
The following dialogue will appear, click **Add Features**. When you return to the **Add Roles and Features Wizard** click **Next**



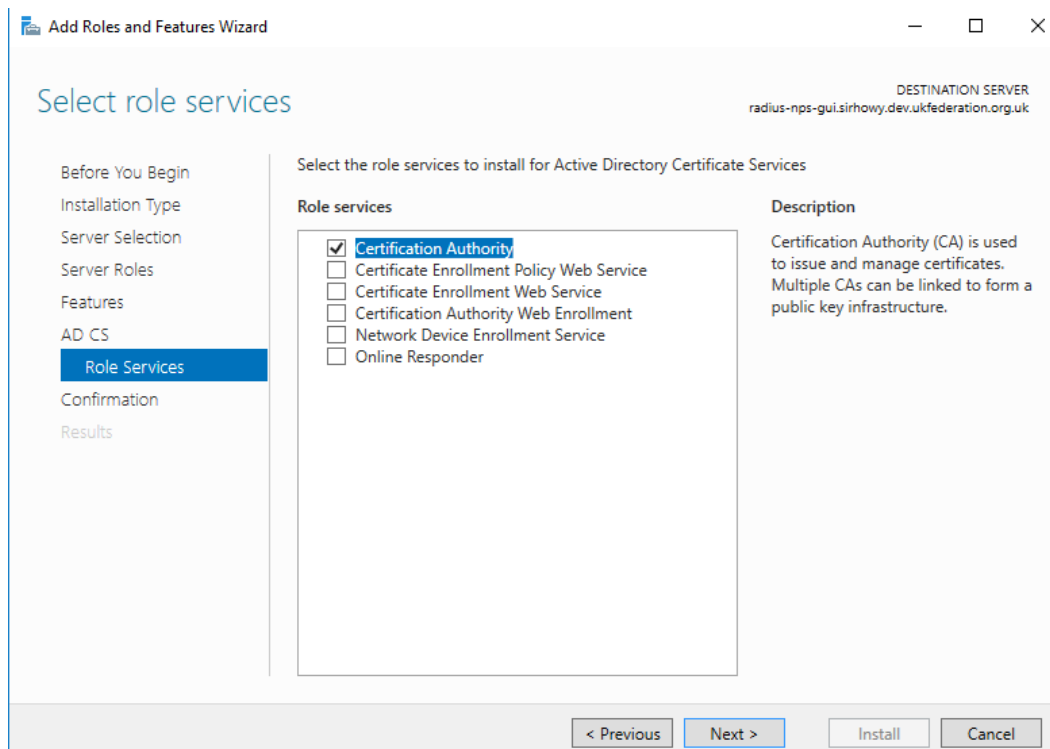
Click **Next**.



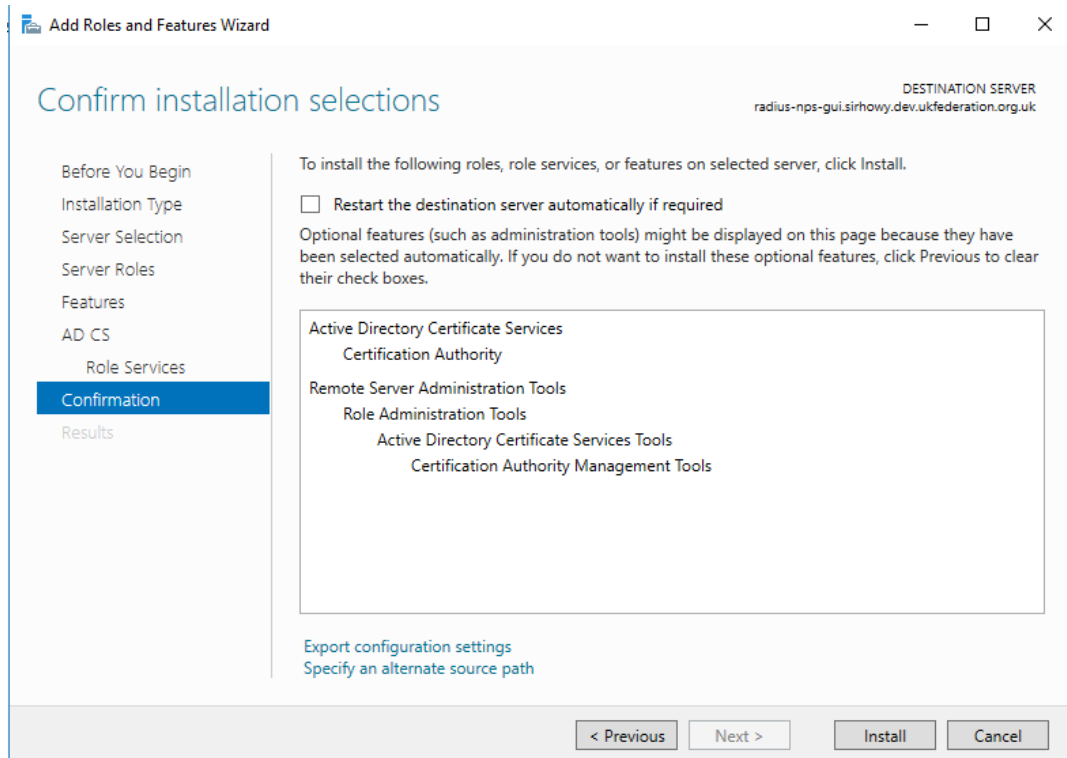
Take note of this dialogue in relation to DNS/Hostname of the server and then click **Next**



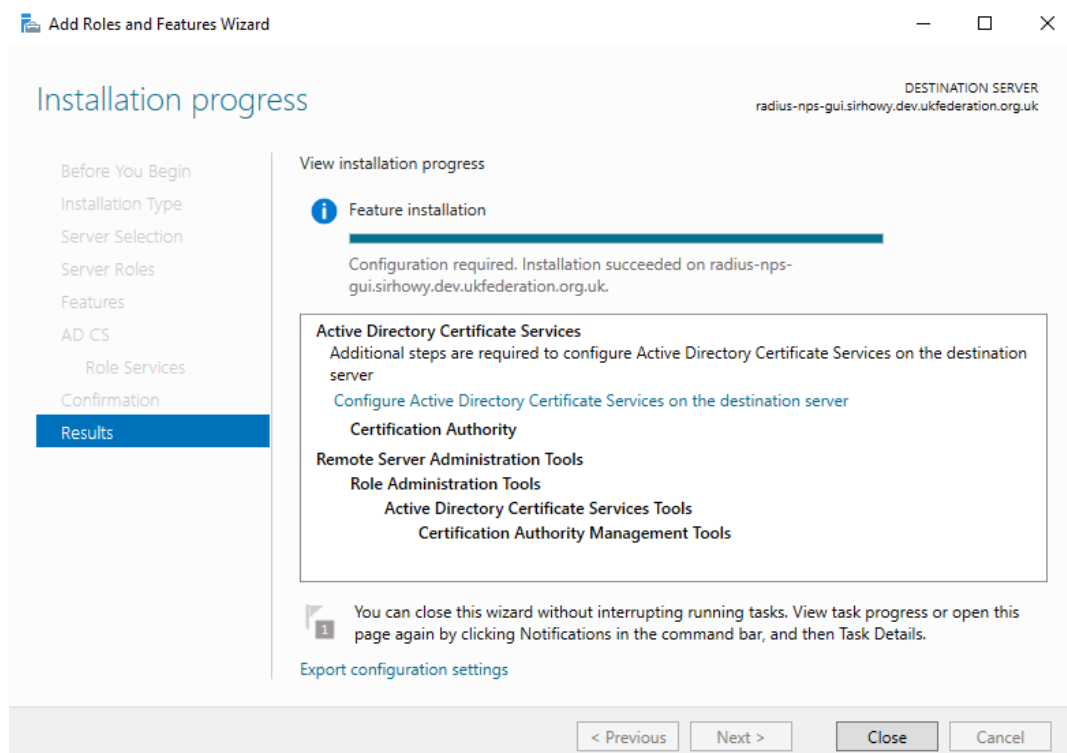
There is no need to select any additional **Role Services** and keep it as below



Hit **Install** on the confirmation dialogue, there is no need to tick the Restart



Once installed, click on **Configure Active Directory Certificate Services on the destination server**





You can now configure your Standalone CA. Here you will select the **credentials of the appropriate administrative account**, this can usually be left as default

The screenshot shows the 'AD CS Configuration' window with the 'Credentials' tab selected. The window title is 'AD CS Configuration'. The 'DESTINATION SERVER' is 'radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. The left sidebar has 'Credentials' selected, with other options: 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Specify credentials to configure role services'. It contains two lists of role services and their required group memberships:

- 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

Below these lists is a 'Credentials' field with the text 'SIRHOWY\jagland' and a 'Change...' button. At the bottom right are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. A link 'More about AD CS Server Roles' is at the bottom left.

Select role services to configure, as there is only one **Certification Authority** then just hit **Next**

The screenshot shows the 'AD CS Configuration' window with the 'Role Services' tab selected. The window title is 'AD CS Configuration'. The 'DESTINATION SERVER' is 'radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. The left sidebar has 'Role Services' selected, with other options: 'Credentials', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Certificate Request', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Select Role Services to configure'. It contains a list of role services with checkboxes:

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

At the bottom right are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. A link 'More about AD CS Server Roles' is at the bottom left.

We recommend the use of a **Standalone CA**, as this should be more portable than an Enterprise CA, which is heavily integrated with Active Directory. Select **Standalone CA** and click **Next**

**Tip:** if you want to setup an Enterprise CA there are some instructions in the GÉANT guide.

AD CS Configuration

DESTINATION SERVER  
radius-nps-gui.sirhowy.dev.ukfederation.org.uk

### Setup Type

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

[More about Setup Type](#)

< Previous   Next >   Configure   Cancel

Select **Root CA** and then hit **Next**.

AD CS Configuration

DESTINATION SERVER  
radius-nps-gui.sirhowy.dev.ukfederation.org.uk

### CA Type

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.

[More about CA Type](#)

< Previous   Next >   Configure   Cancel

Select **Create a new private key** and hit **Next**

The screenshot shows the 'Private Key' step of the AD CS Configuration wizard. The left-hand navigation pane lists steps: Credentials, Role Services, Setup Type, CA Type, Private Key (highlighted), Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the type of the private key'. It includes a sub-header 'To generate and issue certificates to clients, a certification authority (CA) must have a private key.' and two radio button options: 'Create a new private key' (selected) and 'Use existing private key'. Below the 'Create a new private key' option, there is explanatory text: 'Use this option if you do not have a private key or want to create a new private key.' Below the 'Use existing private key' option, there are two sub-options: 'Select a certificate and use its associated private key' and 'Select an existing private key on this computer', each with explanatory text. At the bottom right, there is a 'More about Private Key' link. The bottom of the window features navigation buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

Set a minimum Key length of **2048**, and at least **SHA256** for your hash algorithm.

Nb. Do not use SHA1 or MD5.

The screenshot shows the 'Cryptography for CA' step of the AD CS Configuration wizard. The left-hand navigation pane lists steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography (highlighted), CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the cryptographic options'. It includes two dropdown menus: 'Select a cryptographic provider:' (set to 'RSA#Microsoft Software Key Storage Provider') and 'Key length:' (set to '2048'). Below these is a list box for 'Select the hash algorithm for signing certificates issued by this CA:' with options: SHA256 (selected), SHA384, SHA512, SHA1, and MD5. At the bottom, there is an unchecked checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' and a 'More about Cryptography' link. The bottom of the window features navigation buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

The **Common Name for this CA** can be modified, and should be something friendly for users, as they may see this whilst configuring their device. E.g. `Camford University eduroam service`

The screenshot shows the 'AD CS Configuration' wizard window. The left-hand navigation pane lists several steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name (which is highlighted in blue), Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'CA Name' and contains the following text: '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:' followed by a text box containing 'Sirhowy NPS guide eduroam service', 'Distinguished name suffix:' followed by a text box containing 'DC=sirhowy,DC=dev,DC=ukfederation,DC=org,DC=uk', and 'Preview of distinguished name:' followed by a text box containing 'CN=Sirhowy NPS guide eduroam service,DC=sirhowy,DC=dev,DC=u'. At the bottom right, there is a link 'More about CA Name'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

Please give the **Certificate Authority** a long-life, we recommendation **20 years or more**.

The screenshot shows the 'AD CS Configuration' wizard window at the 'Validity Period' step. The left-hand navigation pane is the same as in the previous screenshot, but 'Validity Period' is now highlighted in blue. The main area is titled 'Validity Period' and contains the following text: 'Specify the validity period', 'Select the validity period for the certificate generated for this certification authority (CA):', a text box with '50' and a dropdown menu set to 'Years', 'CA expiration Date: 08/03/2068 15:45:00', and 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom right, there is a link 'More about Validity Period'. The bottom of the window has four buttons: '< Previous', 'Next >' (which is highlighted in blue), 'Configure', and 'Cancel'.

Your CA will be stored at the **Certificate database location**, ensure that it is backed up regularly to a secure location.

The screenshot shows the 'AD CS Configuration' wizard window. The left-hand navigation pane lists several steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, **Certificate Database** (which is highlighted in blue), Confirmation, Progress, and Results. The main area of the wizard is titled 'Specify the database locations'. It contains two text input fields: 'Certificate database location:' with the value 'C:\Windows\system32\CertLog' and 'Certificate database log location:' with the value 'C:\Windows\system32\CertLog'. In the top right corner, it says 'DESTINATION SERVER radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

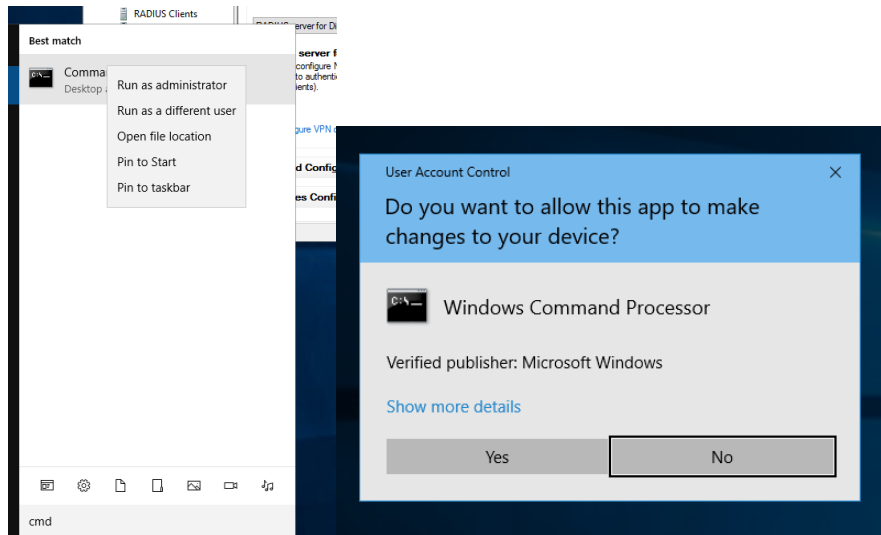
This is the final page of the wizard, click **Configure**, the next dialogue will advise that the “Configuration Succeeded” click **Close**. You should complete the additional tasks mentioned in **Sections 6 and 7** of this guide.

The screenshot shows the 'AD CS Configuration' wizard window at the 'Confirmation' step. The left-hand navigation pane is the same as in the previous screenshot, but 'Confirmation' is now highlighted in blue. The main area is titled 'Confirmation' and contains the text 'To configure the following roles, role services, or features, click Configure.' Below this is a section header 'Active Directory Certificate Services' with a small upward arrow icon. Underneath, there is a list of configuration details for the 'Certification Authority':  
CA Type: Standalone Root  
Cryptographic provider: RSA#Microsoft Software Key Storage Provider  
Hash Algorithm: SHA256  
Key Length: 2048  
Allow Administrator Interaction: Disabled  
Certificate Validity Period: 08/03/2068 15:45:00  
Distinguished Name: CN=Sirhowy NPS guide eduroam service,DC=sirhowy,DC=dev,DC=ukfederation,DC=org,DC=uk  
Certificate Database Location: C:\Windows\system32\CertLog  
Certificate Database Log Location: C:\Windows\system32\CertLog  
In the top right corner, it says 'DESTINATION SERVER radius-nps-gui.sirhowy.dev.ukfederation.org.uk'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

## 6. Change the Certificate Authority - Validity period

This means that the CA will issue certificates that are valid for a long period, align this with the validity period of the CA i.e. 20 years+.

Search for the command prompt `cmd` in Start, and then right click choose **Run as Administrator**, following this you will need to choose **Yes** in the User Account Control dialogue.



On the command prompt enter the following commands;

(the number 20 here is the number of years, so adjust this as required)

```
certutil -setreg CA\ValidityPeriodUnits 20
certutil -setreg CA\ValidityPeriod Years
net stop certsvc && net start certsvc
```

You can see the successful output of this below;

```
Administrator: Command Prompt
Old Value:
  ValidityPeriodUnits REG_DWORD = 1
New Value:
  ValidityPeriodUnits REG_DWORD = 32 (50)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>certutil -setreg CA\ValidityPeriod Years
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Sirhowy NPS guide eduroam service\ValidityPer
iod:
Old Value:
  ValidityPeriod REG_SZ = Years
New Value:
  ValidityPeriod REG_SZ = Years
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>net stop certsvc && net start certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.

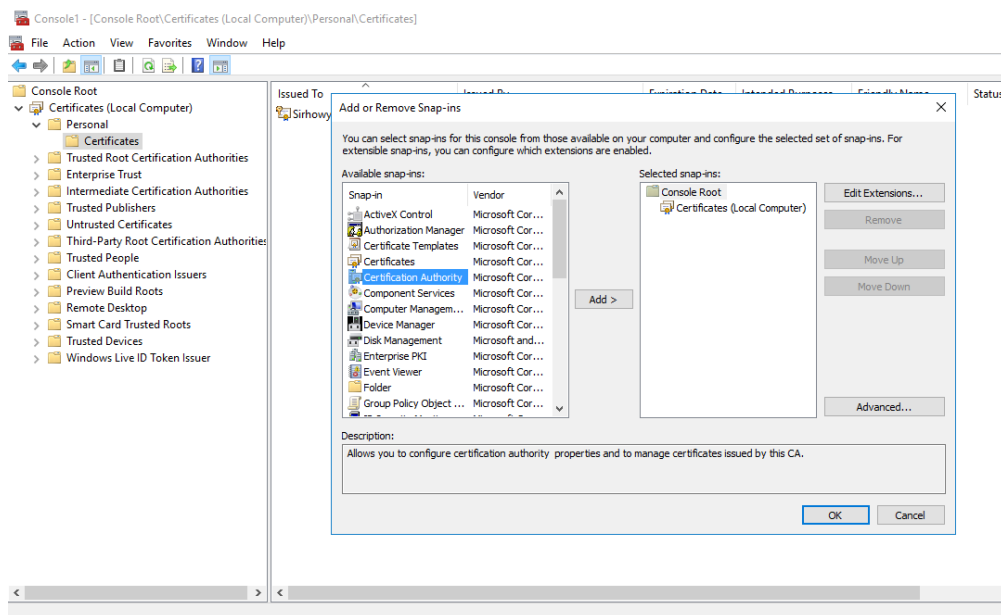
The Active Directory Certificate Services service is starting.
The Active Directory Certificate Services service was started successfully.

C:\Windows\system32>
```

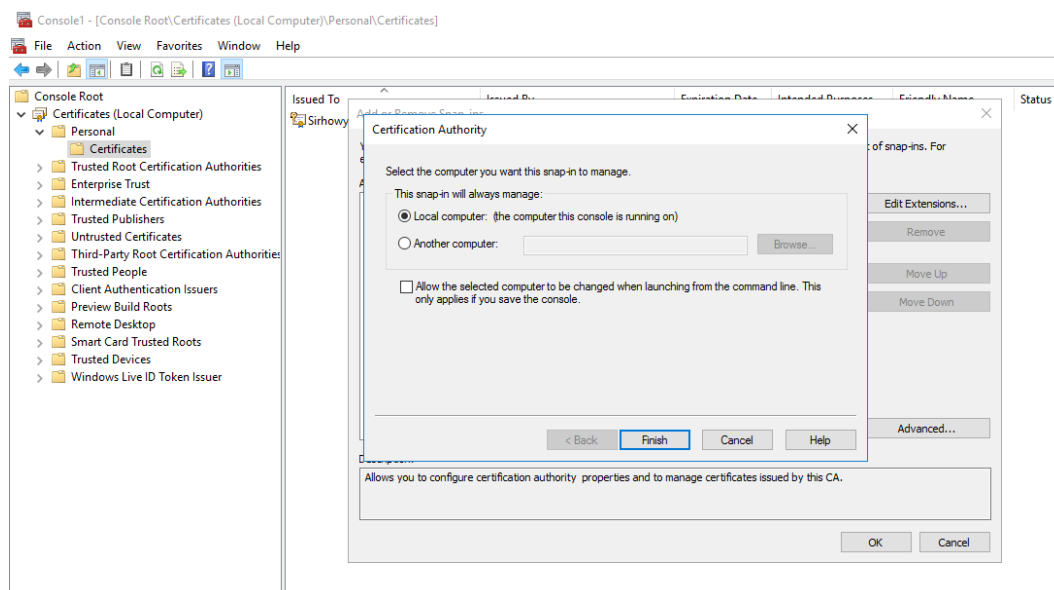
## 7. Change the Certificate Authority - CRL Distribution Points

The CRL Distribution points created by the CA in Windows may not be compatible with devices looking for a URL starting `http://`, as a result we would recommend the following steps.

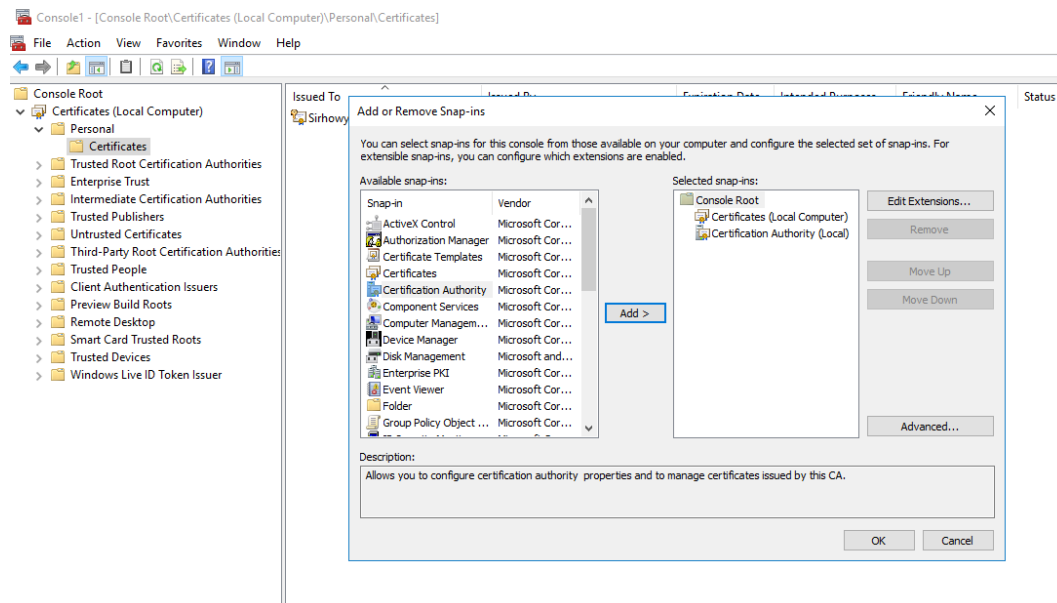
Add the **Certification Authority** Snap-in to MMC



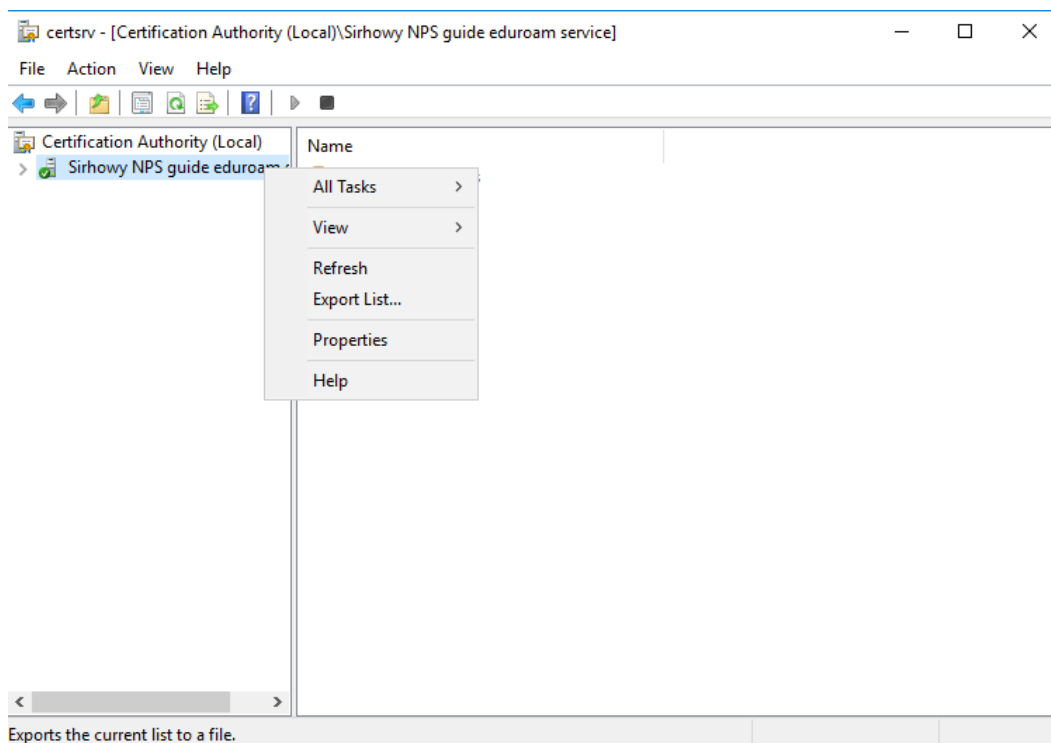
Choose **Local Computer**



You should see **Certification Authority** on the right hand side under **Selected Snap-ins**



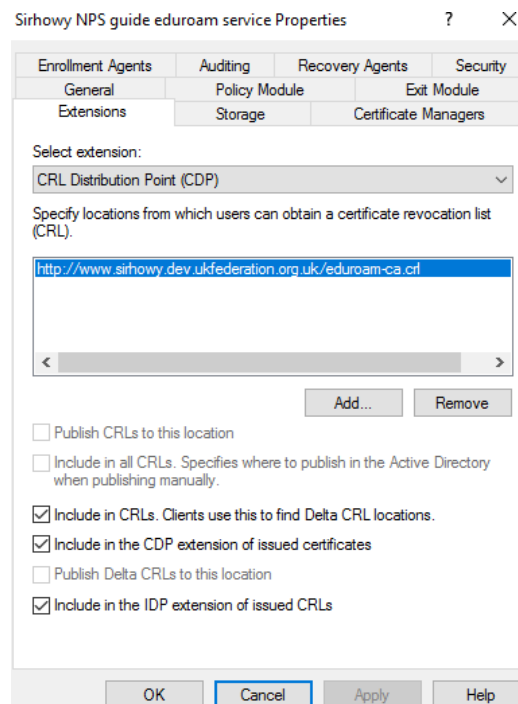
In MMC with certificate authority snap-in selected, right click and choose **Properties**.





In the **Extensions** tab, **Add a CRL Distribution Point (CDP)** location, this should be somewhere you could feasibly place a CRL distribution file, for our example `http://www.camford.ac.uk/eduroam-ca.crl`

Choose **Include in the CDP extension of issued certificates** for the above CRL, make sure to untick this from any of the other CRLs or remove all other CRLs. There is no requirement for **Include in CRLs. Client us this to find Delta CRL locations** and, **Include in the IDP extension of issued CRLs** to be ticked or unticked.

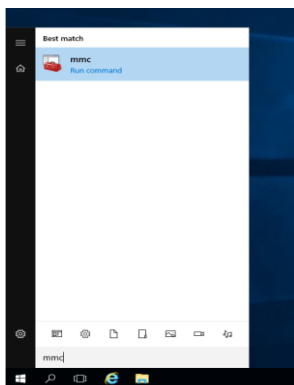


## 8. Creating the Server Certificate

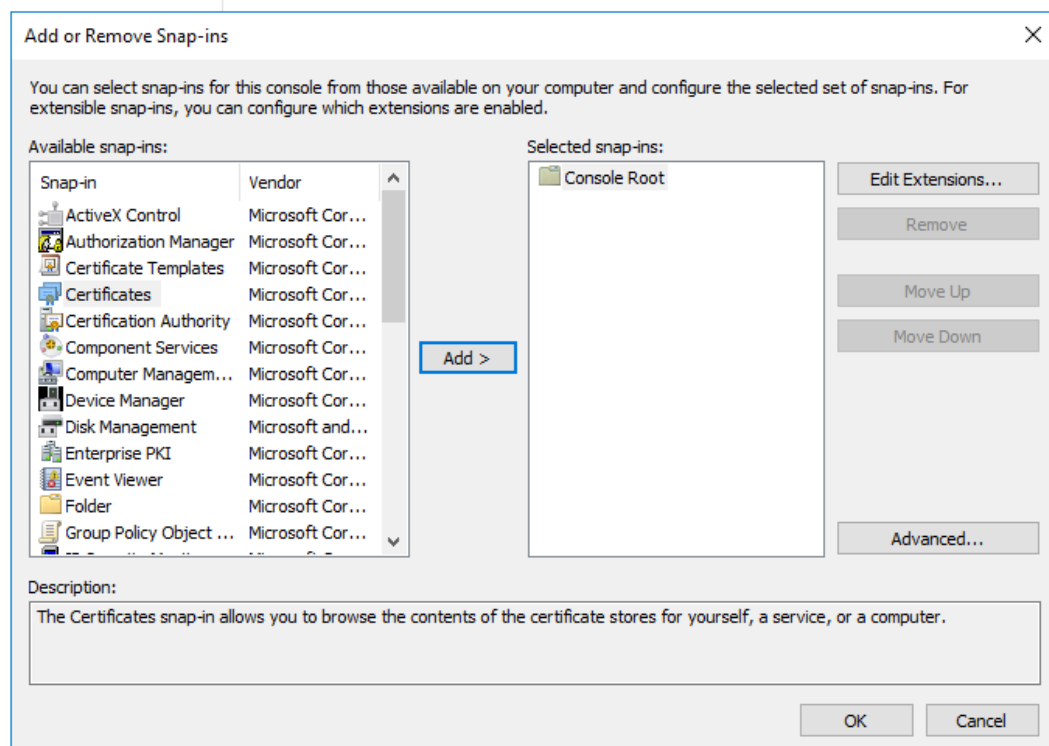
PEAP-MSCHAPv2 and EAP-TLS authentication methods, in common with all other EAP methods (with the exception of EAP-PWD - which is not supported in NPS) require an X.509 server certificate to be installed on the authenticating RADIUS server. The certificate is used to establish the secure authentication tunnel and is used by the RADIUS server to identify itself to the user's device.

To acquire a server certificate from your certificate provider you must generate a certificate signing request (CSR) on the NPS server that you want the certificate for. If deploying more than one ORPS, normally you acquire one certificate and then copy that and the private key to all ORPSs. The following describes how to generate your CSR for submission to your certificate provider (e.g. **Jisc Certificate Service**). If you operate your own private CA and generate self-signed certificates you should see the instructions provided in the GÉANT guide **GN3-NA3-T4-UFS140**.

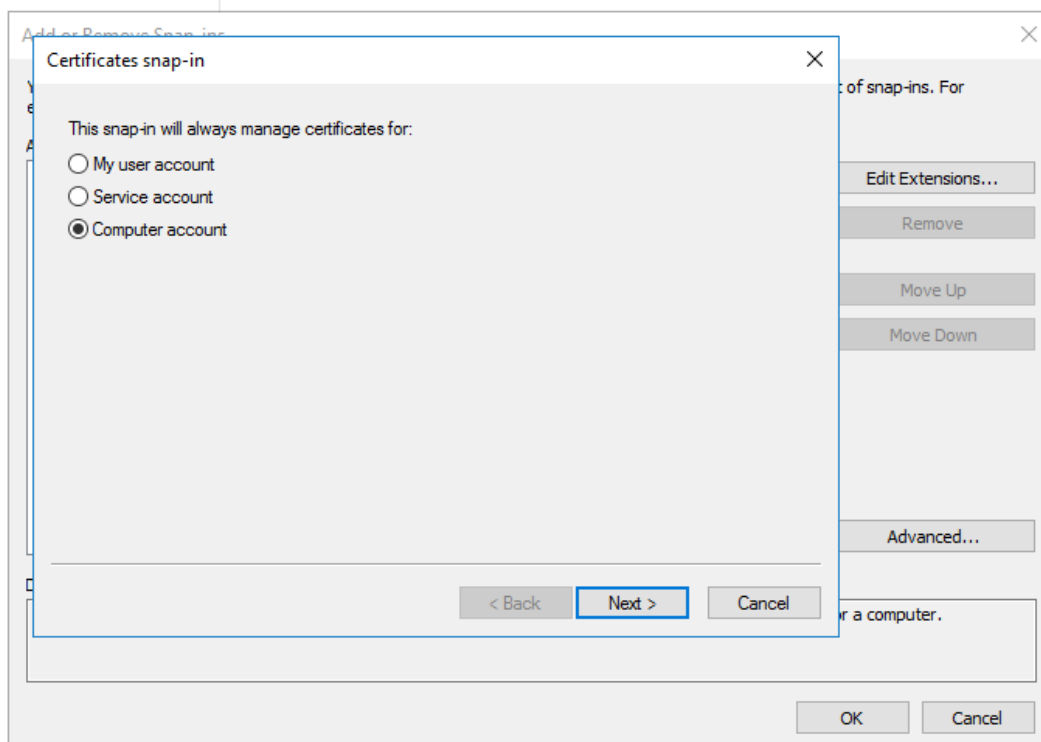
Go to **Start**, **run** and type **mmc** and click on it.



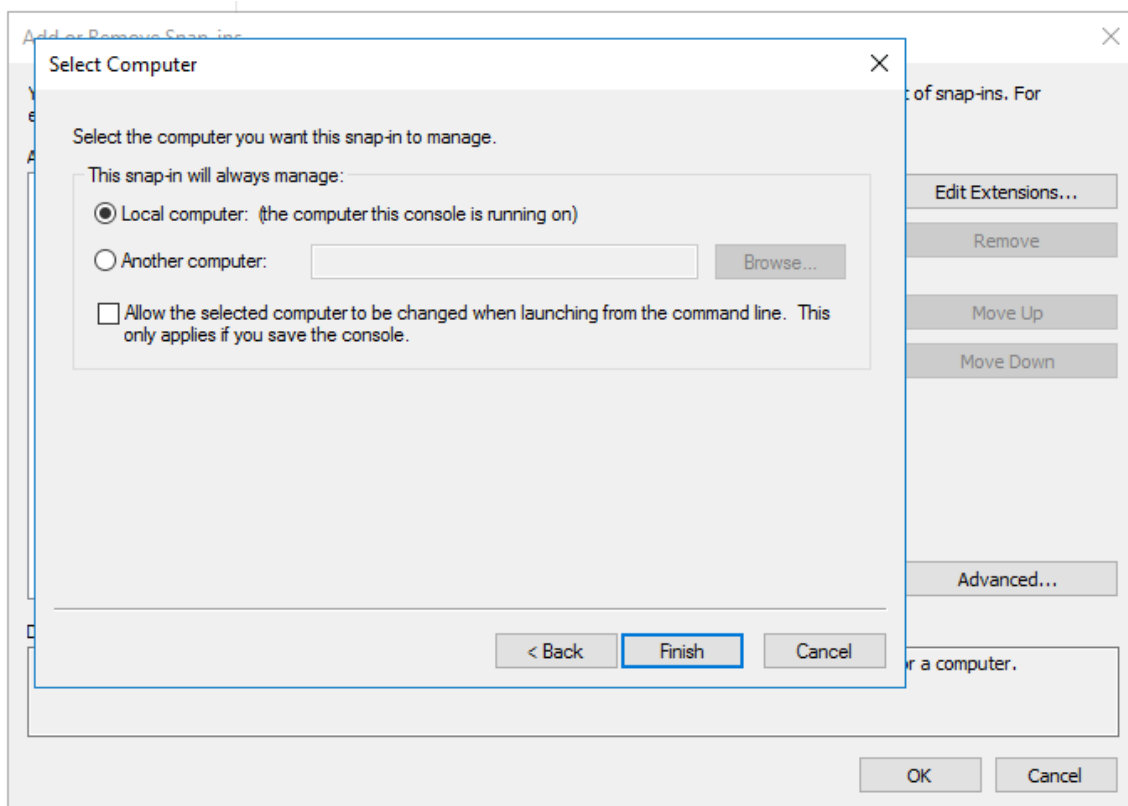
In the mmc console click **File, Add/Remove Snap-in...** Then from the list of **Available snap-ins** choose **Certificates** and click **Add**.



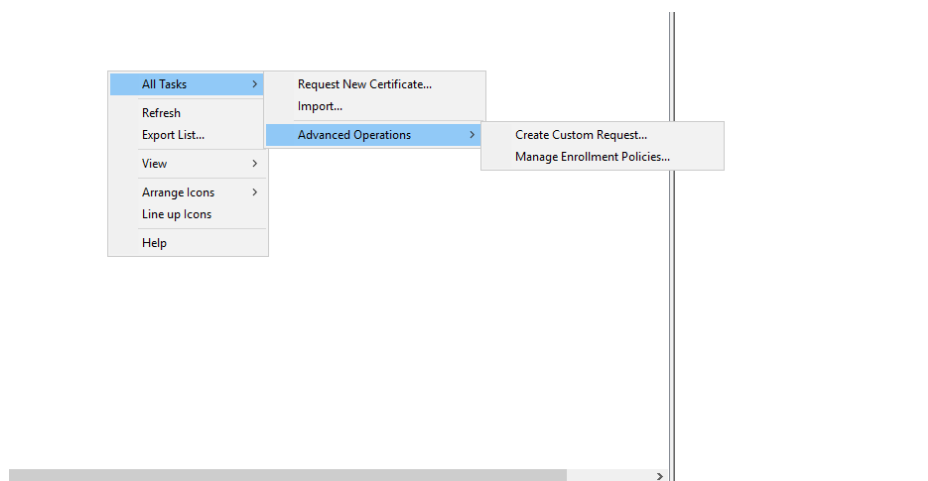
Choose **Computer account** and click **Next**.



Choose **Local Computer**: and then click **Finish**. Then click **OK**



In the menu on the left, under **Certificates (Local Computer)**, right click on **Certificates** under **Personal**. Then under **All Tasks, Advanced Operations**, click **Create Custom Request....**



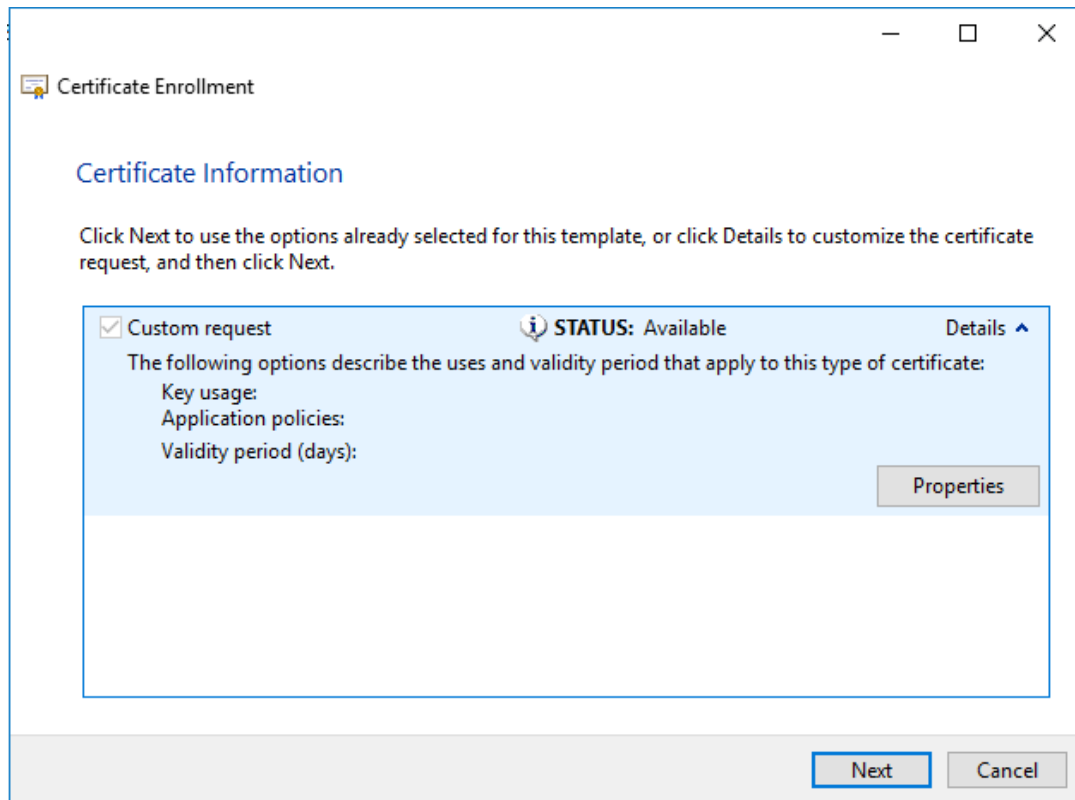
Click **Next** on the **Certificate Enrollment – Before you begin** page, on the **Select Certificate Enrollment Policy** page shown below choose 'Proceed without enrollment policy' under **Custom Request**. Then click **Next**.

The screenshot shows a window titled 'Certificate Enrollment' with a subtitle 'Select Certificate Enrollment Policy'. Below the subtitle, there is explanatory text: 'Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.' The main area contains two sections: 'Configured by your administrator' with a dropdown menu showing 'Active Directory Enrollment Policy', and 'Configured by you' with a sub-section 'Custom Request' containing the option 'Proceed without enrollment policy'. An 'Add New' link is visible next to the 'Configured by you' section. At the bottom right, there are 'Next' and 'Cancel' buttons.

Choose **Request format: PKCS #10** and click **Next**.

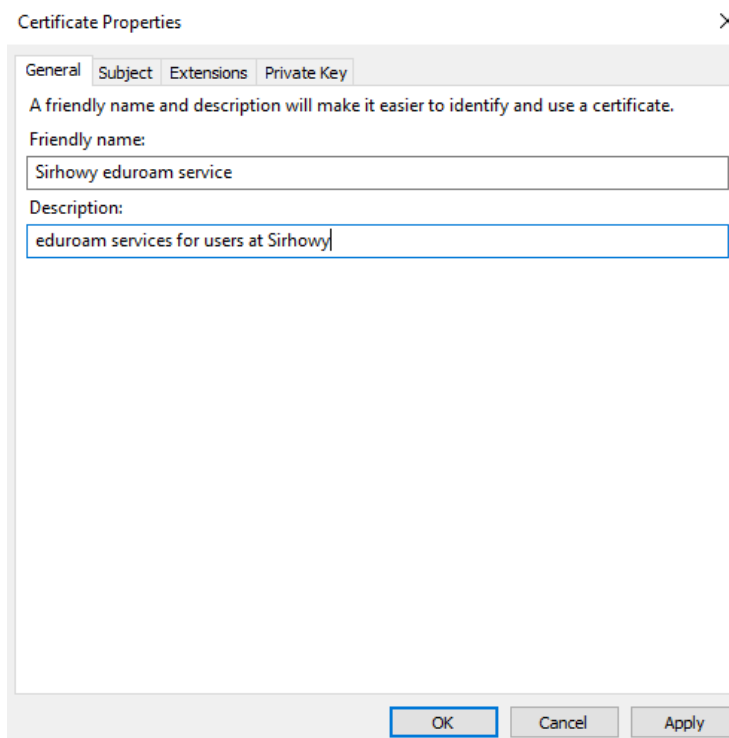
The screenshot shows a window titled 'Certificate Enrollment' with a subtitle 'Custom request'. Below the subtitle, there is explanatory text: 'Chose an option from the list below and configure the certificate options as required.' The main area contains two sections: 'Template:' with a dropdown menu showing '(No template) CNG key' and a checkbox for 'Suppress default extensions', and 'Request format:' with two radio buttons: 'PKCS #10' (selected) and 'CMC'. A note at the bottom states: 'Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.' At the bottom right, there are 'Next' and 'Cancel' buttons.

On the **Certificate Information** page click the **Details** button and click **Properties**.



The screenshot shows the 'Certificate Enrollment' window. The title bar says 'Certificate Enrollment'. Below the title bar, there's a section titled 'Certificate Information'. Below this, there's a message: 'Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.' Below this message, there's a light blue box containing a checked checkbox labeled 'Custom request', a status indicator 'STATUS: Available' with a lock icon, and a 'Details' link with an upward arrow. Below these, there's text: 'The following options describe the uses and validity period that apply to this type of certificate:' followed by three lines: 'Key usage:', 'Application policies:', and 'Validity period (days):'. To the right of this text is a 'Properties' button. At the bottom right of the window are 'Next' and 'Cancel' buttons.

Enter a **Friendly name**: for the certificate reflecting your organisation name e.g. `Camford University eduroam service`.



The screenshot shows the 'Certificate Properties' dialog box. It has four tabs: 'General', 'Subject', 'Extensions', and 'Private Key'. The 'General' tab is selected. Below the tabs, there's a message: 'A friendly name and description will make it easier to identify and use a certificate.' Below this, there's a 'Friendly name:' label followed by a text box containing 'Sirhowy eduroam service'. Below that, there's a 'Description:' label followed by a text box containing 'eduroam services for users at Sirhowy'. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Click on the **Subject** tab then enter relevant information for your server in the **Subject name**:

- Common name – CN (fully-qualified domain name - FQDN) e.g. `radius.camford.ac.uk`
- Country – C (country) i.e. GB
- Email – E (a contact e-mail address) e.g. `it@camford.ac.uk`
- Locality – L (town / city) e.g. Camford
- Organization – O (Organisation Name) e.g. Camford University
- State – S (County) e.g. Camfordshire

Under **Alternate Name** choose **DNS**, enter the fully-qualified domain name - FQDN e.g. `radius.camford.ac.uk`

The screenshot shows the 'Certificate Properties' dialog box with the 'Subject' tab selected. The dialog has four tabs: 'General', 'Subject', 'Extensions', and 'Private Key'. The 'Subject' tab contains the following information:

**Subject of certificate**  
The user or computer that is receiving the certificate

**Subject name:**

Type: **Organization** (dropdown menu)  
Value: (empty text box)

**Alternate name:**

Type: **DNS** (dropdown menu)  
Value: (empty text box)

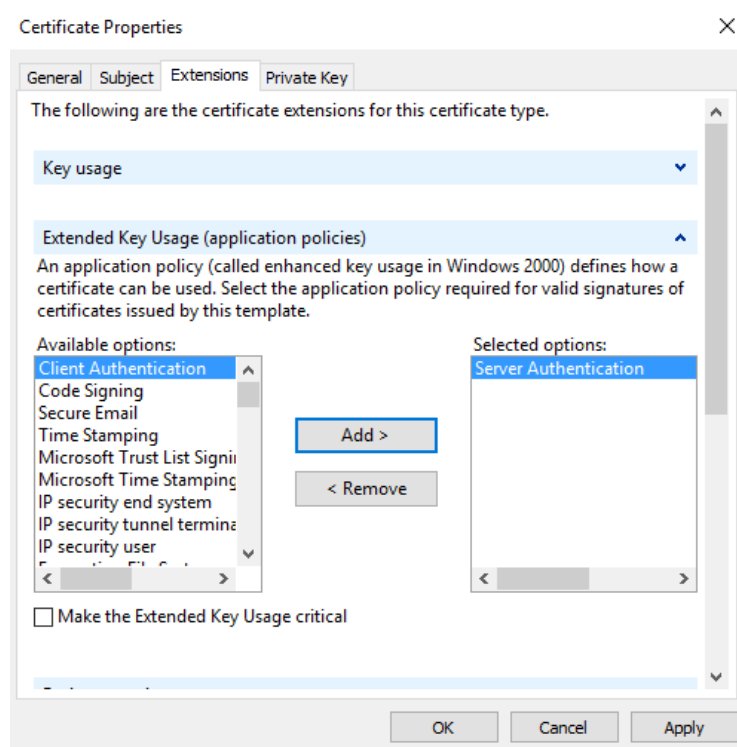
Buttons: 'Add >' and '< Remove' are present for both the Subject name and Alternate name sections.

On the right side, there are two lists of values:

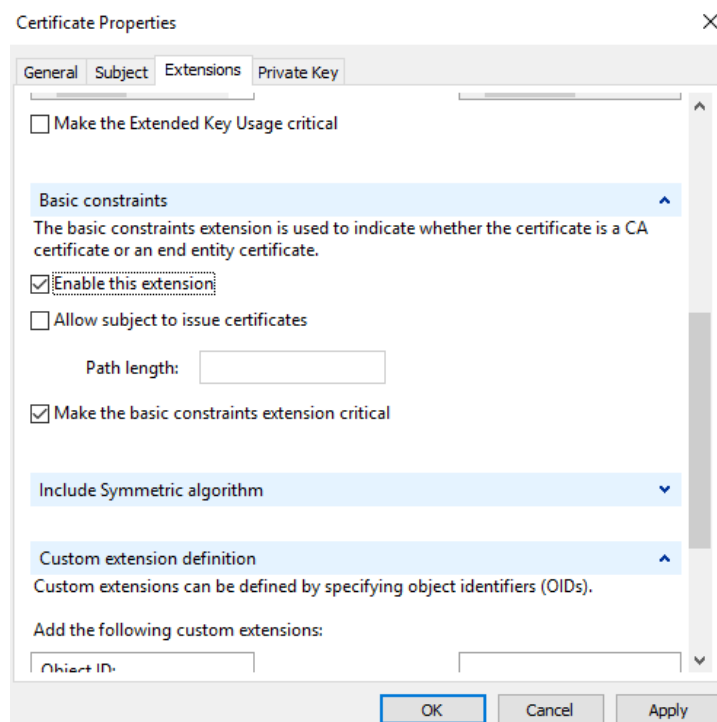
- Subject name values:** CN=radius.camford.ac.uk, C=GB, E=it@camford.ac.uk, L=Camford, O=Camford University, O=Camfordshire
- Alternate name values:** DNS, radius.camford.ac.uk

At the bottom of the dialog are buttons for 'OK', 'Cancel', and 'Apply'.

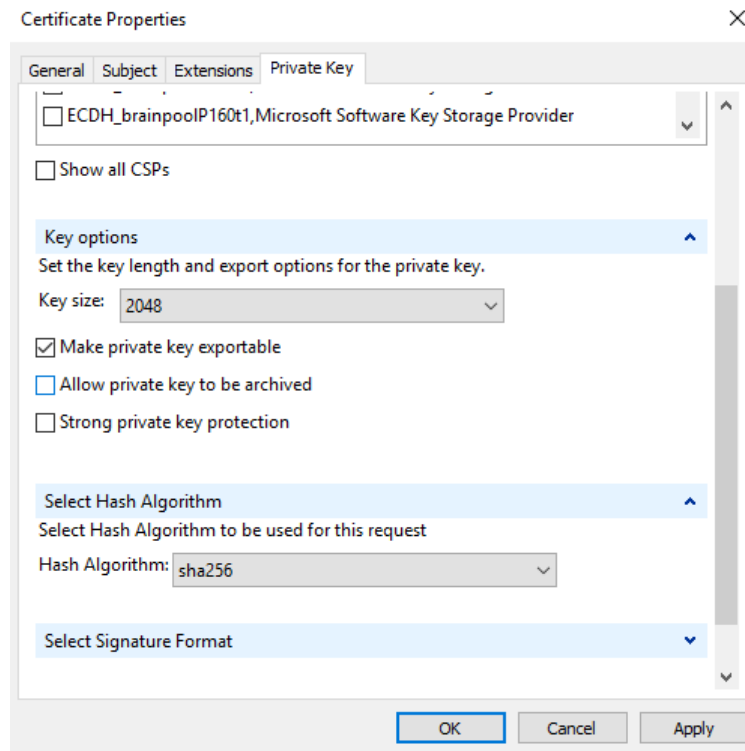
Click on the **Extensions** tab and then under **Extended Key Usage (application policies)** from the available options add **Server Authentication**.



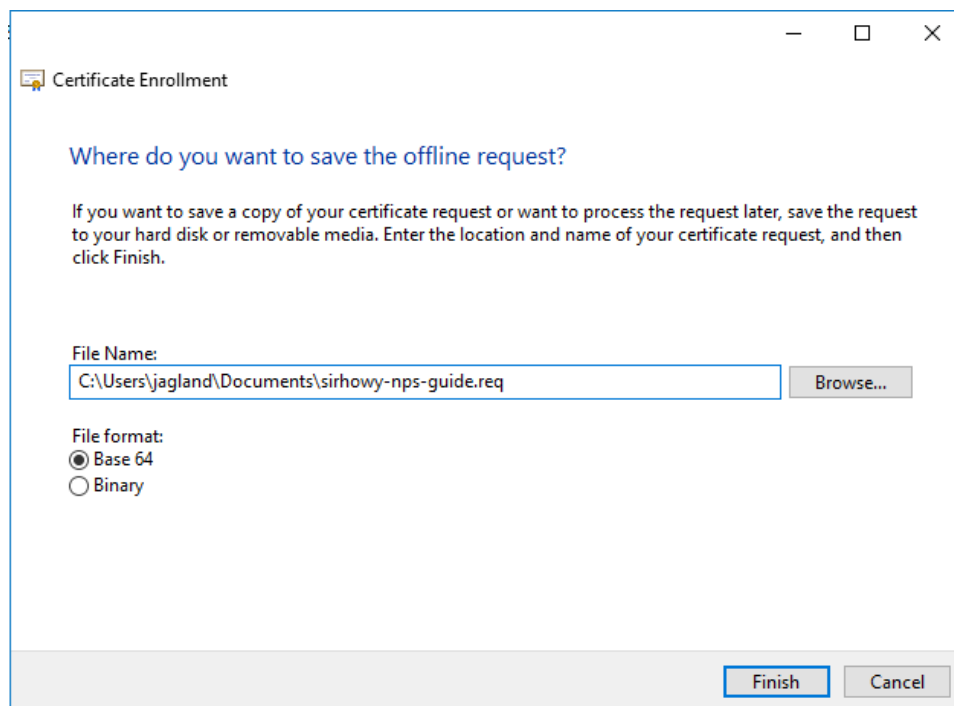
Under **Basic Constraints**, choose **Enable this extension** and **Make the basic constraints extension critical**



Click on the **Private Key** tab, under **Key options** choose a **Key size** of **2048**, tick **Make private key exportable**. Then under **Select Hash Algorithm** choose **sha256**.



Then click **OK** and click **Next**. Browse to a location e.g. Desktop and save the certificate signing request in base 64 format, e.g. as **server.req**, then click **Finish**.



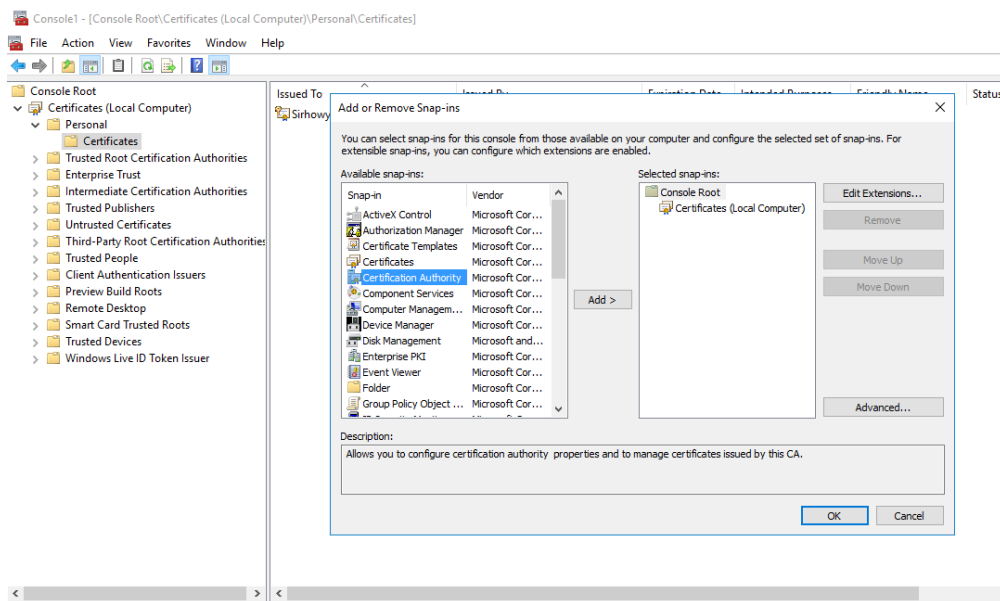
Send the CSR file to your **Certificate Authority**, if using your own CA then follow Section 9. If sending to an external CA for signing e.g. **Jisc Certificate Service**, then skip to Section 10.



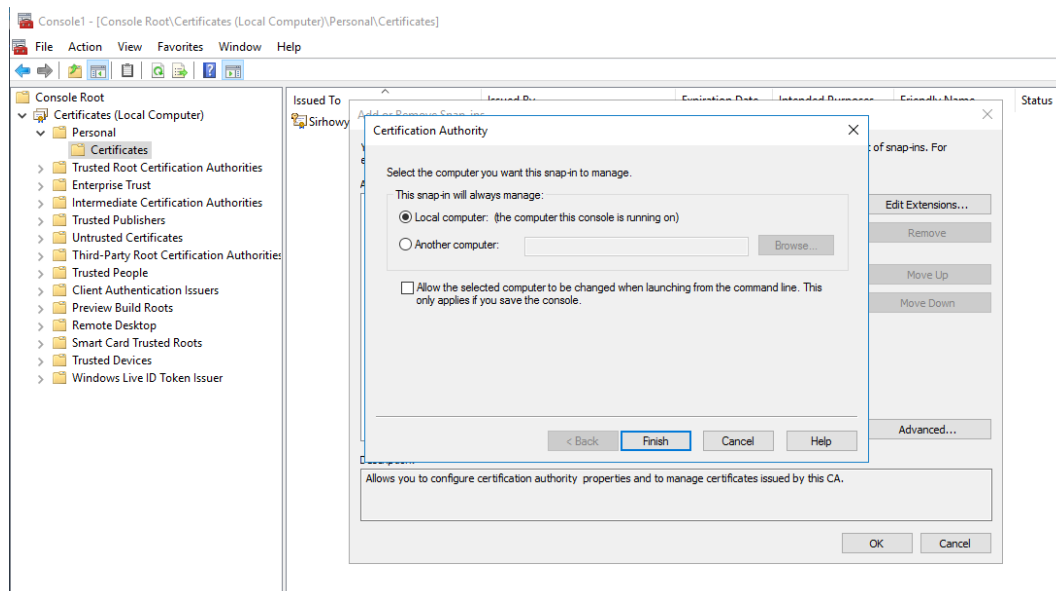
## 9. Signing your certificate requests with your CA

If you've completed Section 7 you will already have the **Certification Authority** Snap-in added to MMC and can skip the next three steps.

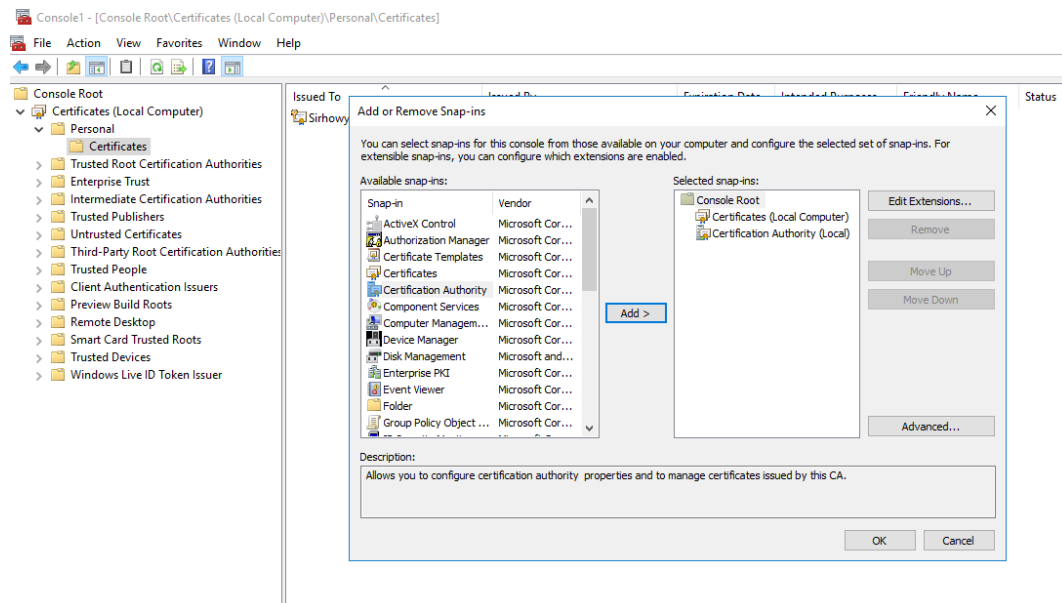
Add the **Certification Authority** Snap-in to MMC



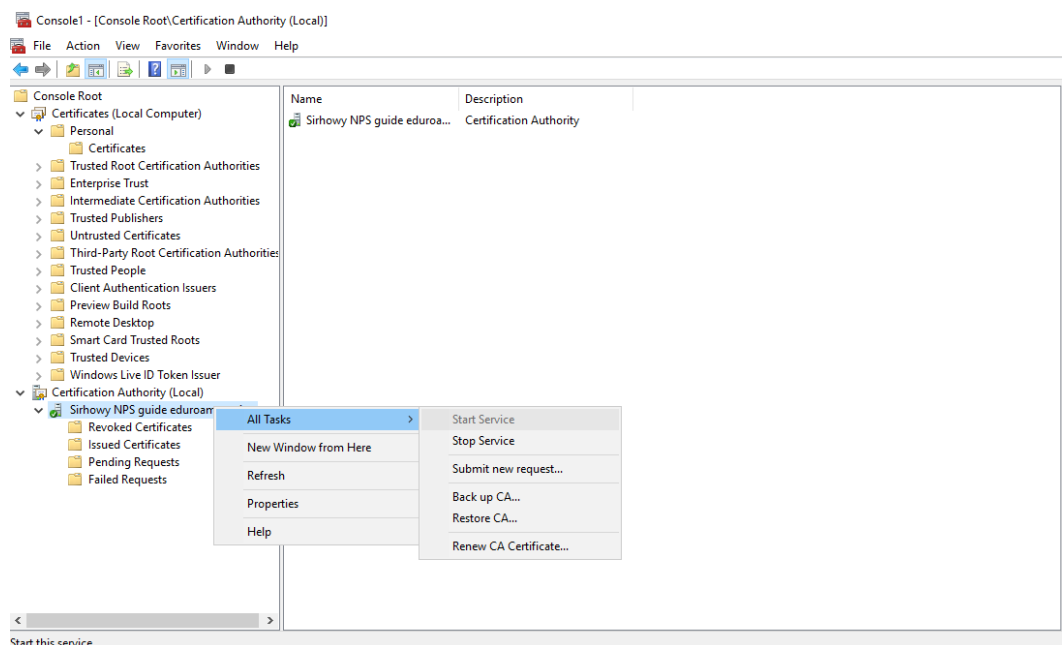
Choose **Local Computer**



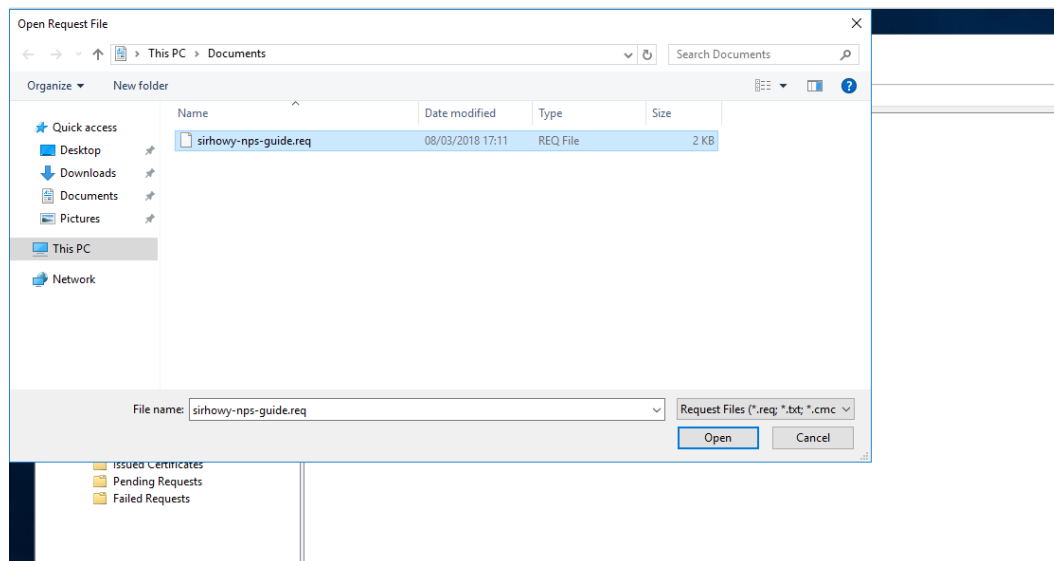
You should see **Certification Authority** on the right hand side under **Selected Snap-ins**



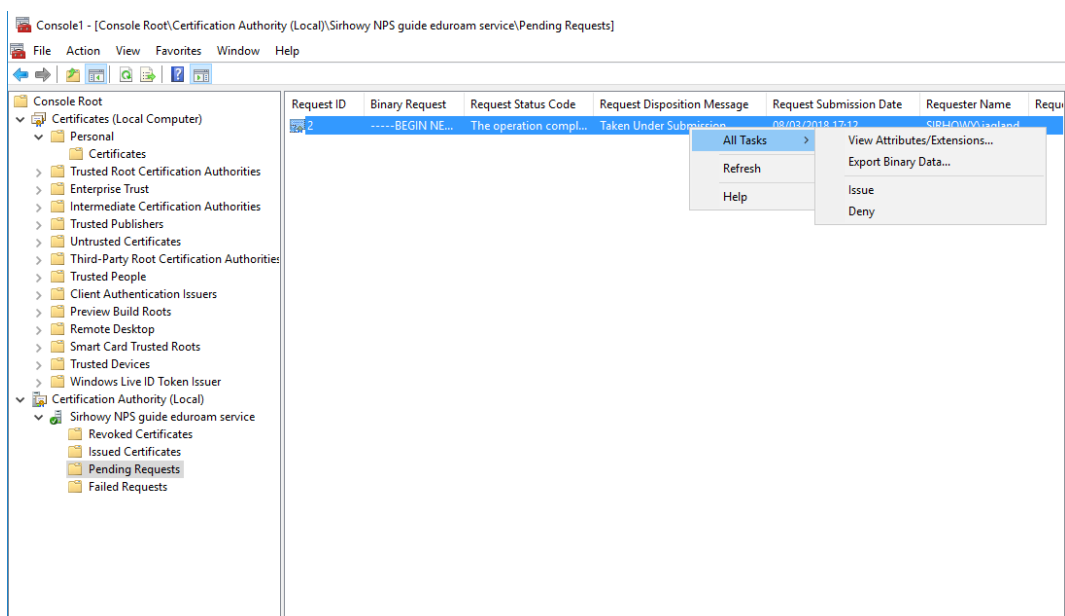
Right click on the **Certificate Authority (Local)**, and choose under **All Tasks**, **Submit new Request**



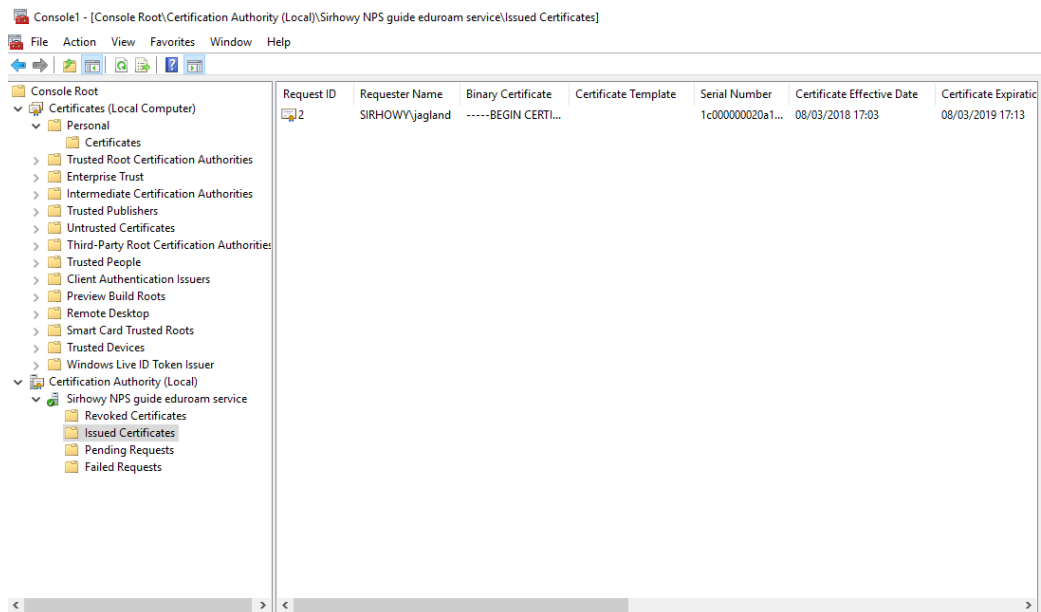
Select your existing certificate request file (.req file)



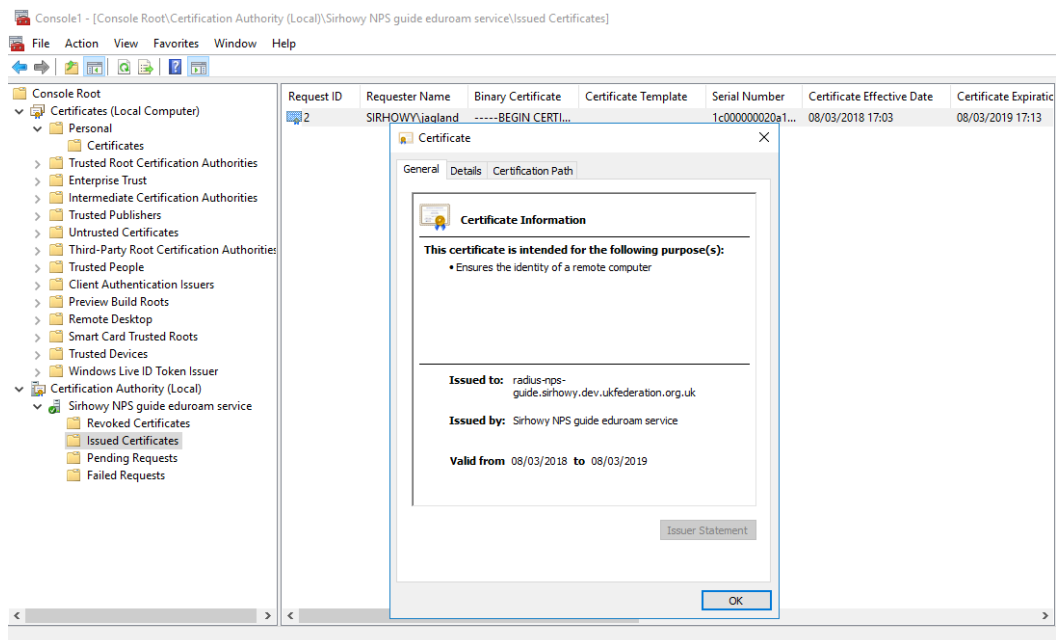
You will now see your request under **Pending Request**, right click and choose **Issue**



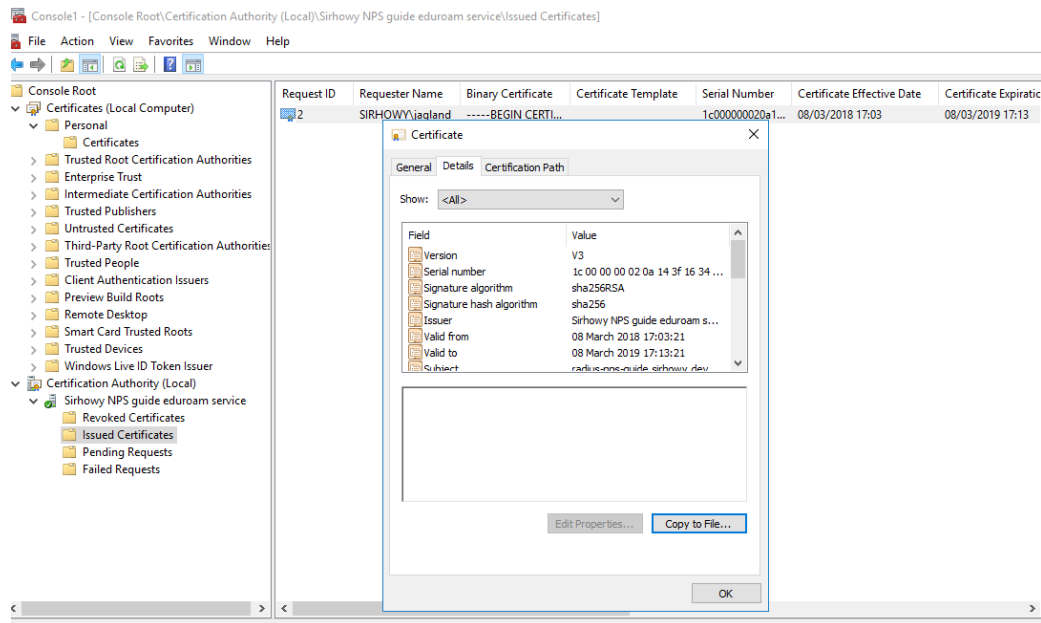
The certificate will now appear under **Issued Certificates**



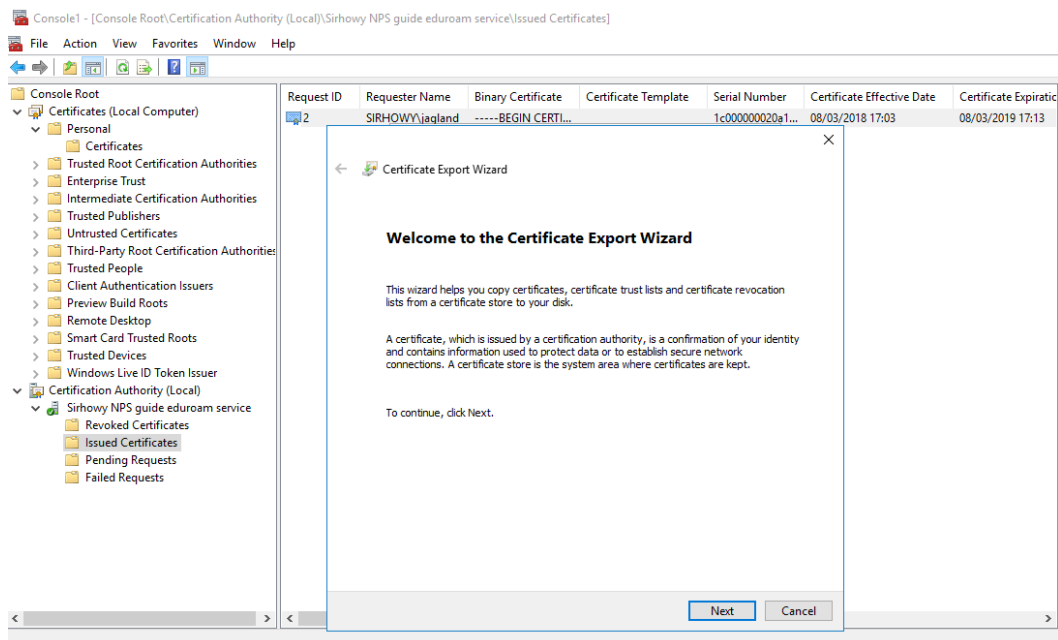
Double-click on the certificate to open the properties window.



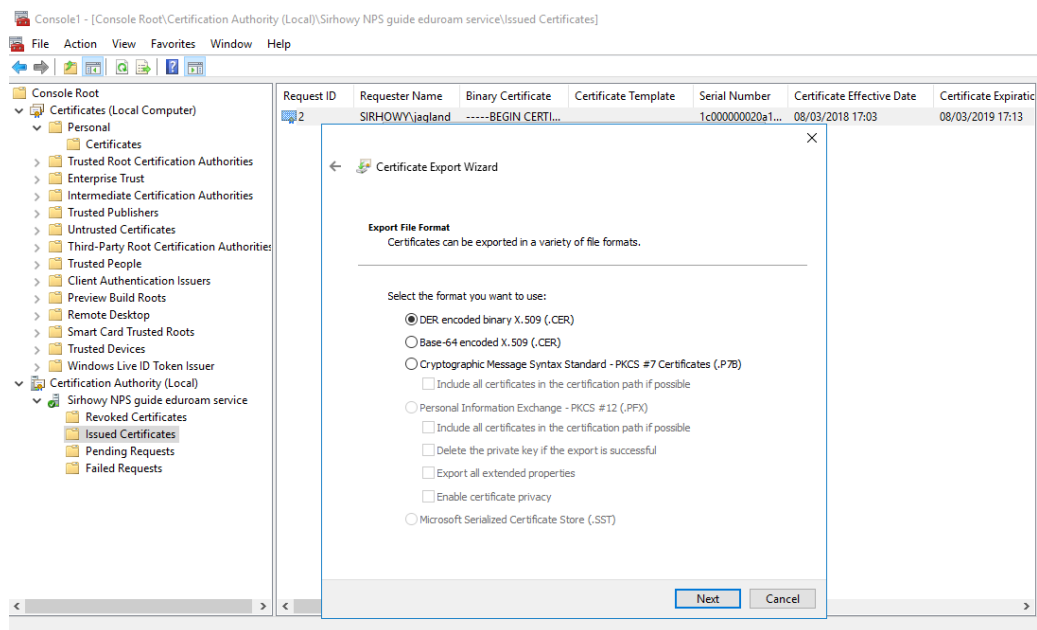
Move to the **details** tab and choose **Copy to File...**



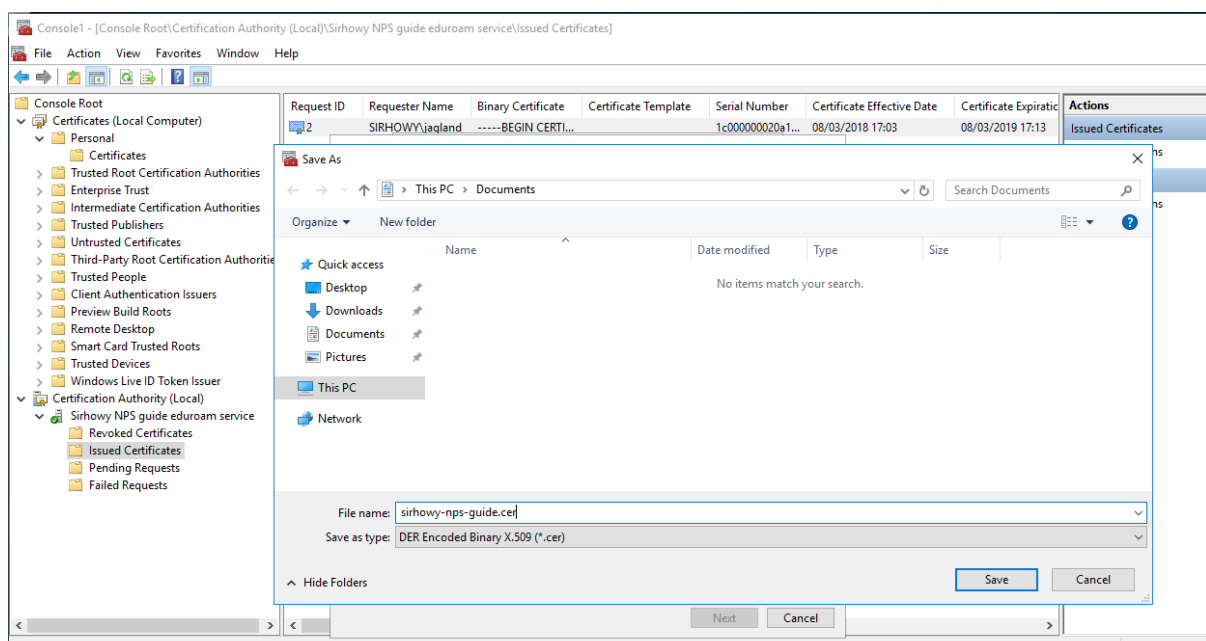
This will launch the **Certificate Export Wizard**



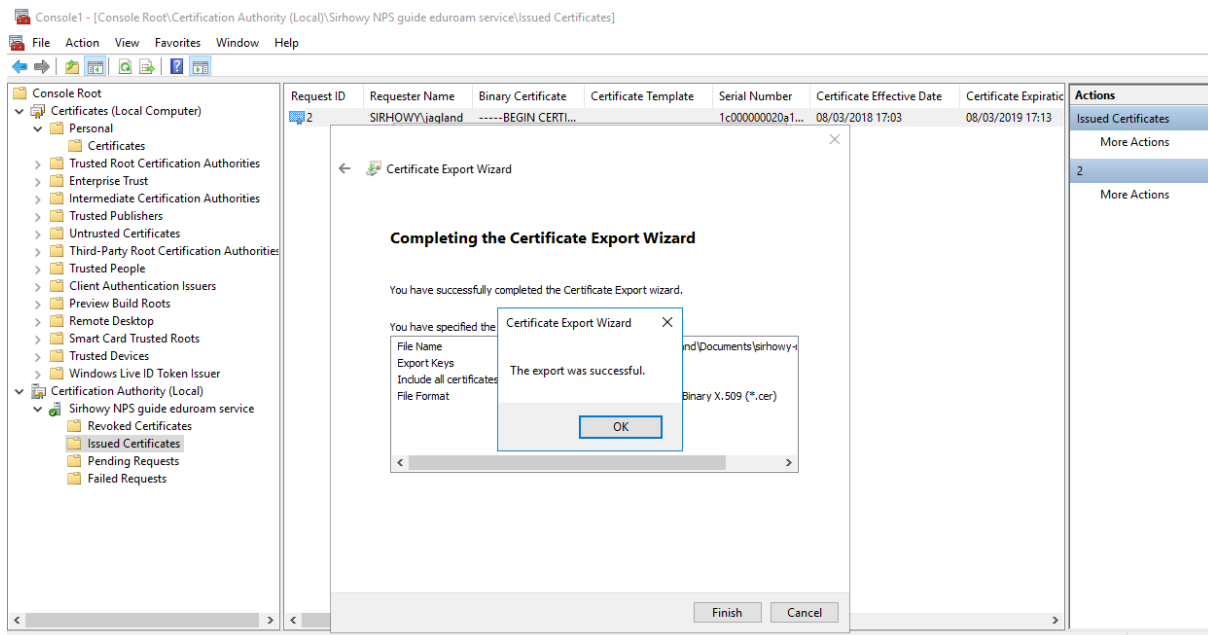
You can use the default format of **DER Encoded Binary x.509 (.cer)**



Specify a **.cer** filename e.g. **server.cer**



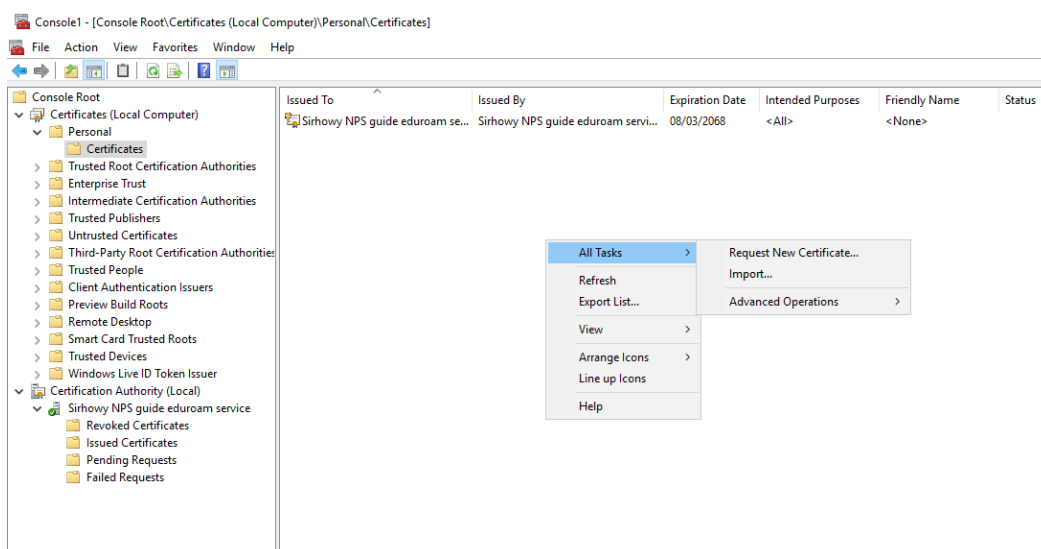
You can now complete the Certificate Export Wizard, click **Finish** and you should get a message to say "The export was successful", click **OK**



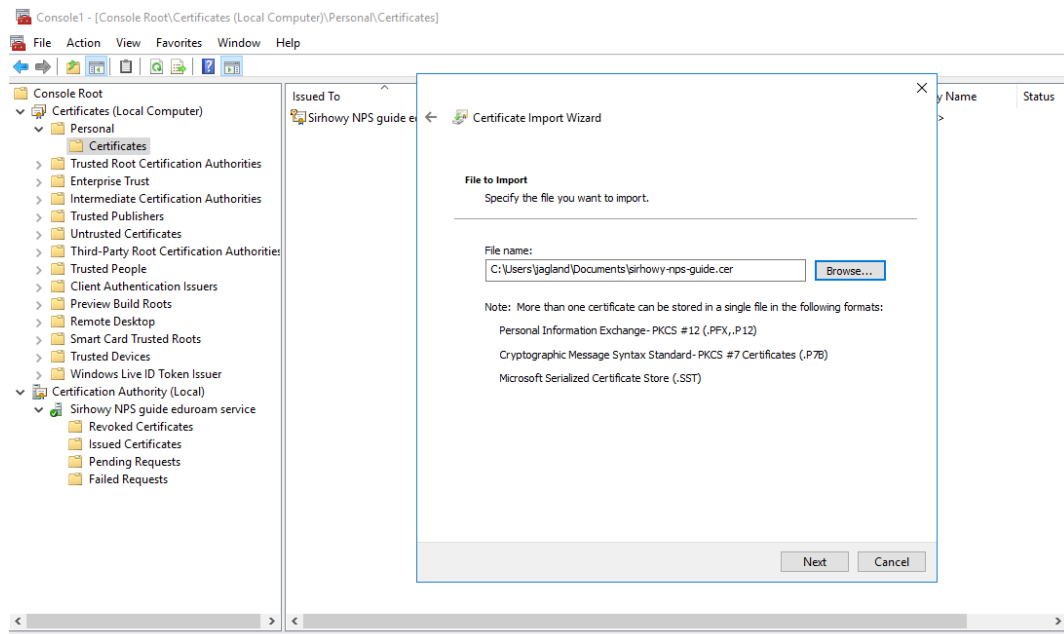
## 10. Import the Server Certificate

Once you receive your Certificate from the Certificate Authority you will need to install it together with any root Certificate Authority or Intermediate certificates.

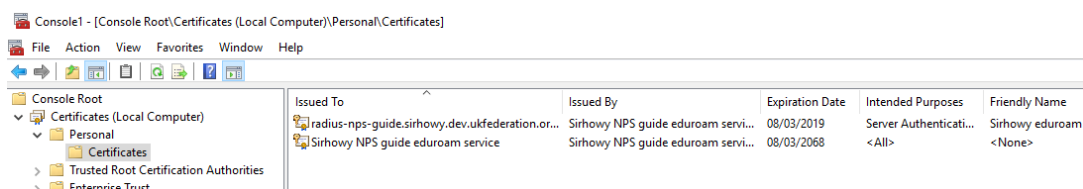
To install your new certificate, download it to your NPS server Desktop and go back to the MMC console. Under **Certificates (Local Computer)** and **Personal**, right click on **Certificates** and under **All Tasks** click **Import....**



In the Certificate Import Wizard window click **Browse...** and go to your server certificate file and click **Next**.



Click 'Next' and the certificate will be imported into the certificate store.



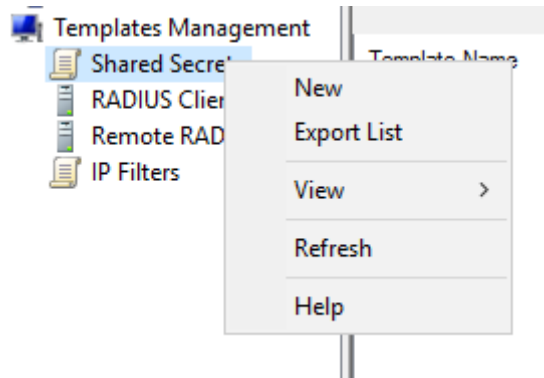
Nb. Repeat this procedure for any root or intermediate certificates.



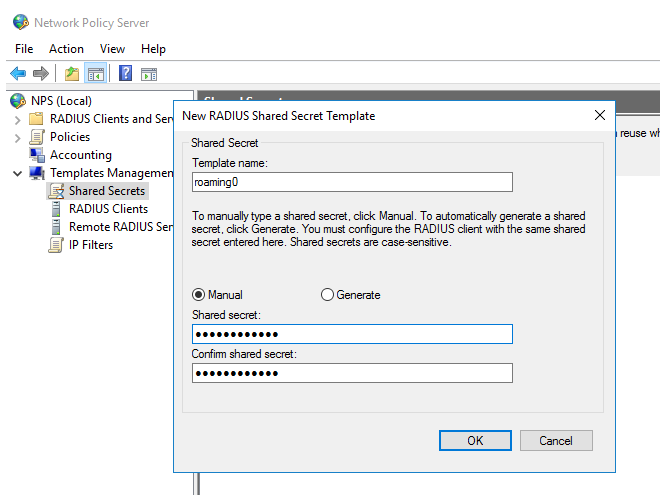
## 11. Configure NRPS Shared Secrets Template

Your NPS ORPS will need to configure each of the NRPS as both RADIUS Client and Remote RADIUS Server Group. Using a Shared Secret template will reduce duplication. You can obtain your Shared secrets from the [eduroam UK support site](#).

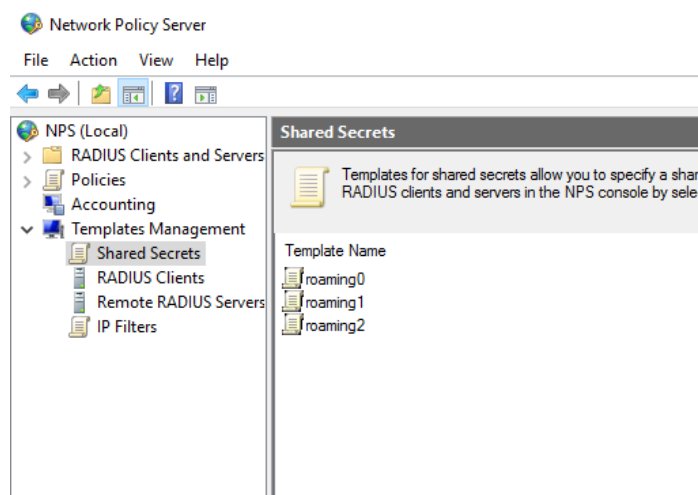
In **Network Policy Server**, choose **Templates Management**, then right click **Shared Secrets** and choose **New**



Enter a template name corresponding to the NRPS (`roaming0`) and enter the **Shared Secret** and repeat, clicking **OK**.



Nb. Repeat this for each NRPS (`roaming1` and `roaming2`)



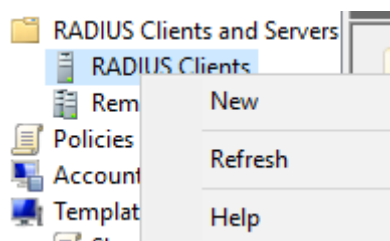
## 12. Add NRPS as RADIUS Clients

For your NPS ORPS to receive incoming RADIUS requests from the NRPS servers, these must be added to your NPS server as RADIUS clients. To do this, in **Network Policy Server** under **RADIUS Clients and Servers**, right click on **RADIUS Clients** and click **New**

Then in the New RADIUS Client box enter the following:

- Friendly name: roaming0
- Address: roaming0.ja.net
- Shared secret: Selected an existing Shared Secrets template: roaming0

And click 'OK'



New RADIUS Client

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:  
roaming0

Address (IP or DNS):  
roaming0.ja.net Verify...

Shared Secret

Select an existing Shared Secrets template:  
roaming0

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:  
.....

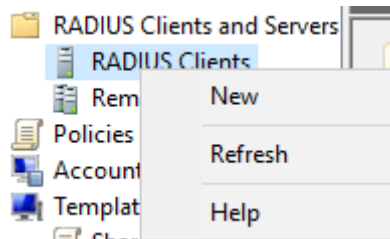
OK Cancel

Nb.Repeat this procedure to add `roaming1` and `roaming2`.

RADIUS Clients			
RADIUS clients allow you to specify the network access servers, that provide access to your network.			
Friendly Name	IP Address	Device Manufacturer	Status
roaming0	roaming0.ja.net	RADIUS Standard	Enabled
roaming1	roaming1.ja.net	RADIUS Standard	Enabled
roaming2	roaming2.ja.net	RADIUS Standard	Enabled

## 13. Add local Access Points / Wireless Infrastructure RADIUS Clients

To receive incoming RADIUS requests from the wireless infrastructure, access points / controllers must be added to the NPS server as RADIUS clients. To do this, in **Network Policy Server** under **RADIUS Clients and Servers**, right click on **RADIUS Clients** and click **New**



Then enter a **Friendly name**, **Address**, and **Shared secret** for your wireless device. Then click **OK**.

wireless controller Properties

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:  
wireless controller

Address (IP or DNS):  
10.1.2.3 Verify...

Shared Secret

Select an existing Shared Secrets template:  
None

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

☒ Manual ☐ Generate

Shared secret:  
.....

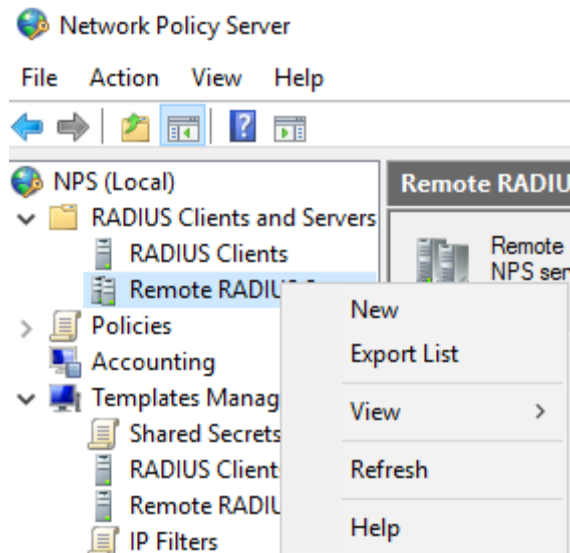
Confirm shared secret:  
.....

OK Cancel Apply

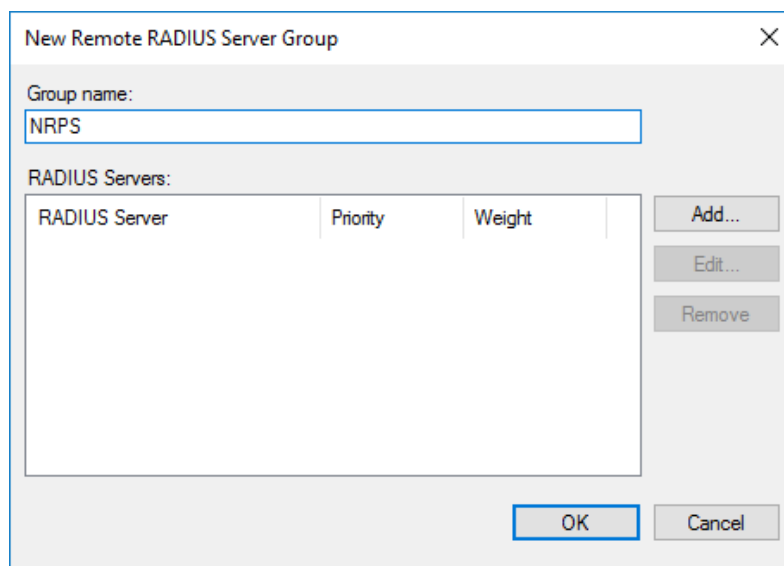
Repeat this step for any additional access points / controllers.

## 14. Add NRPS as RADIUS Proxy Servers

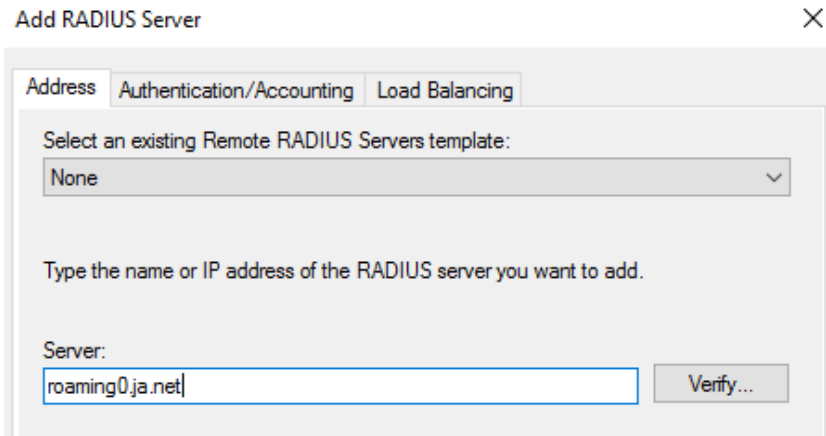
To be able to forward visitor authentications to the NRPS, Remote RADIUS servers need to be added to the configuration. To do this, in **Network Policy Server** under **RADIUS Clients and Servers**, right click on **Remote RADIUS Server Groups** and click **New**



For the **Group name** enter NRPS then click **Add**.



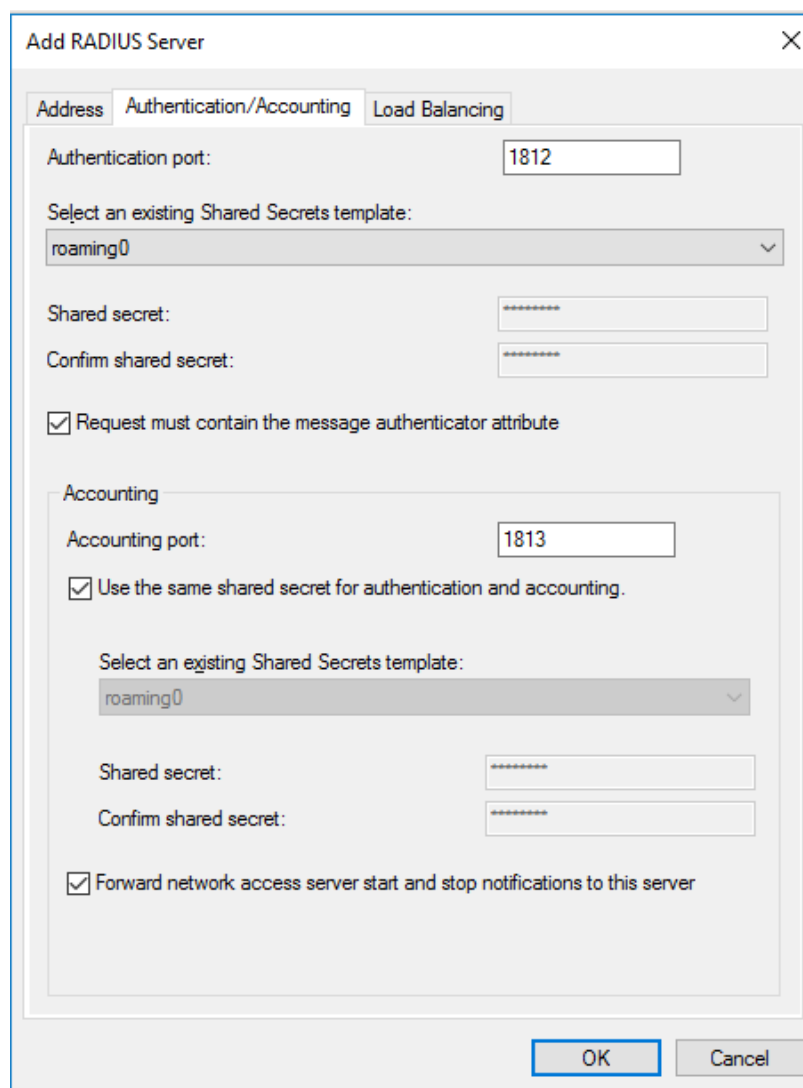
In **Server** enter `roaming0.jja.net` then click on the **Authentication/Accounting** tab.



The 'Add RADIUS Server' dialog box is shown with the 'Address' tab selected. It contains a dropdown menu for 'Select an existing Remote RADIUS Servers template:' with 'None' selected. Below this is a text field for 'Server:' containing 'roaming0.ja.net' and a 'Verify...' button.

Enter the following settings:

- Shared secret – Select an existing Shared Secrets template: `roaming0`
- Request must contain the message authenticator attribute – **Ticked**
- Forward network access server start and stop notifications to this server – **Unticked**



The 'Add RADIUS Server' dialog box is shown with the 'Authentication/Accounting' tab selected. It contains fields for 'Authentication port:' (1812) and 'Accounting port:' (1813). There are dropdown menus for 'Select an existing Shared Secrets template:' (roaming0) for both authentication and accounting. Checkboxes are present for 'Request must contain the message authenticator attribute' (checked), 'Use the same shared secret for authentication and accounting.' (checked), and 'Forward network access server start and stop notifications to this server' (checked). There are also fields for 'Shared secret:' and 'Confirm shared secret:' for both authentication and accounting, all masked with asterisks. 'OK' and 'Cancel' buttons are at the bottom.

Click on the 'Load Balancing' tab. Then enter the following settings:

- Priority – a number between 1 and 3 ( choose a random priority for the three NRPS )
- Weight – 33
- Number of seconds without a response before request is considered dropped – 30

The screenshot shows the 'Add RADIUS Server' dialog box with the 'Load Balancing' tab selected. The dialog has three tabs: 'Address', 'Authentication/Accounting', and 'Load Balancing'. The 'Load Balancing' tab contains the following settings:

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:  Weight:

Advanced settings

Number of seconds without response before request is considered dropped:

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

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

Click **OK** to add the server and then repeat the process for `roaming1` and `roaming2`.

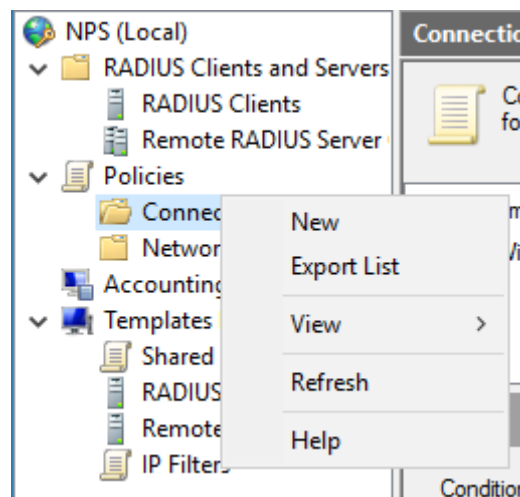
The screenshot shows the 'New Remote RADIUS Server Group' dialog box. The 'Group name' field is set to 'NRPS'. Below it, the 'RADIUS Servers' table lists three servers:

RADIUS Server	Priority	Weight
roaming0.ja.net	1	33
roaming1.ja.net	1	33
roaming2.ja.net	1	33

Buttons: Add..., Edit..., Remove, OK, Cancel.

## 15. Add a Connection Request Policy for your roaming users

This step adds a connection request policy for authentication requests incoming from NRPS from your roaming users. Authentication requests coming from the NRPS servers must always be responded to by the ORPS. Therefore a policy should be added to authenticate requests coming from the NRPS locally. To do this, in **Network Policy Server** under **Policies**, right click on **Connection Request Policies** and click **New**.



In **Policy name** enter "authenticate requests from NRPS locally", then click **Next**.

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:**  
authenticate requests from NRPS locally

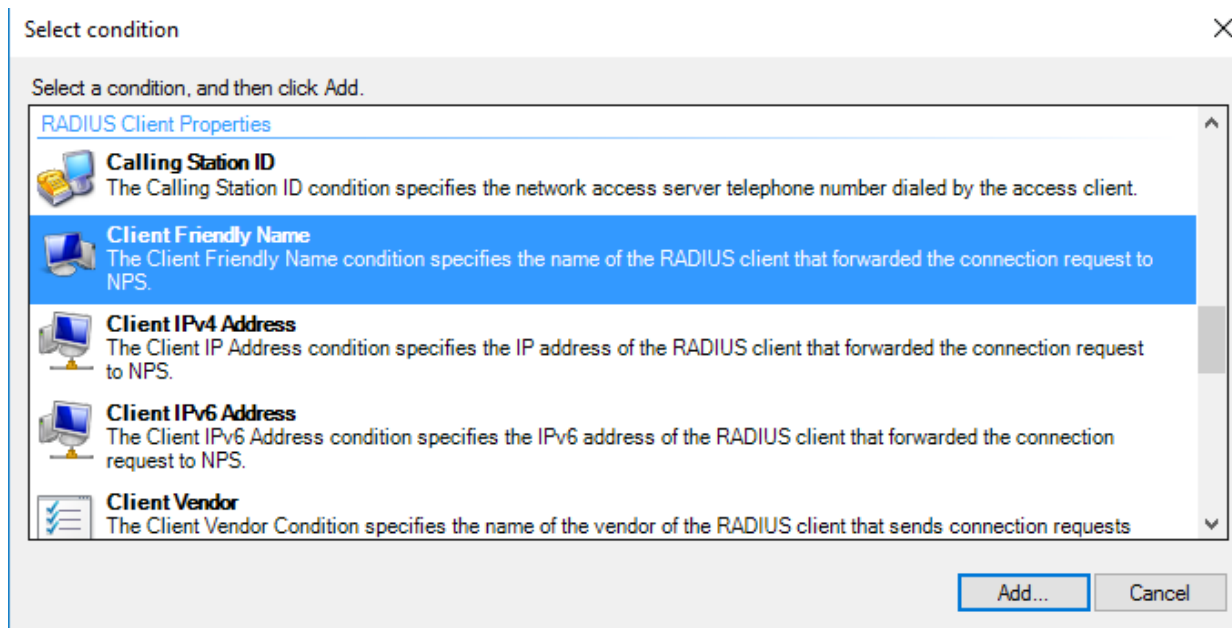
**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point,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

☒ Type of network access server:  
Unspecified

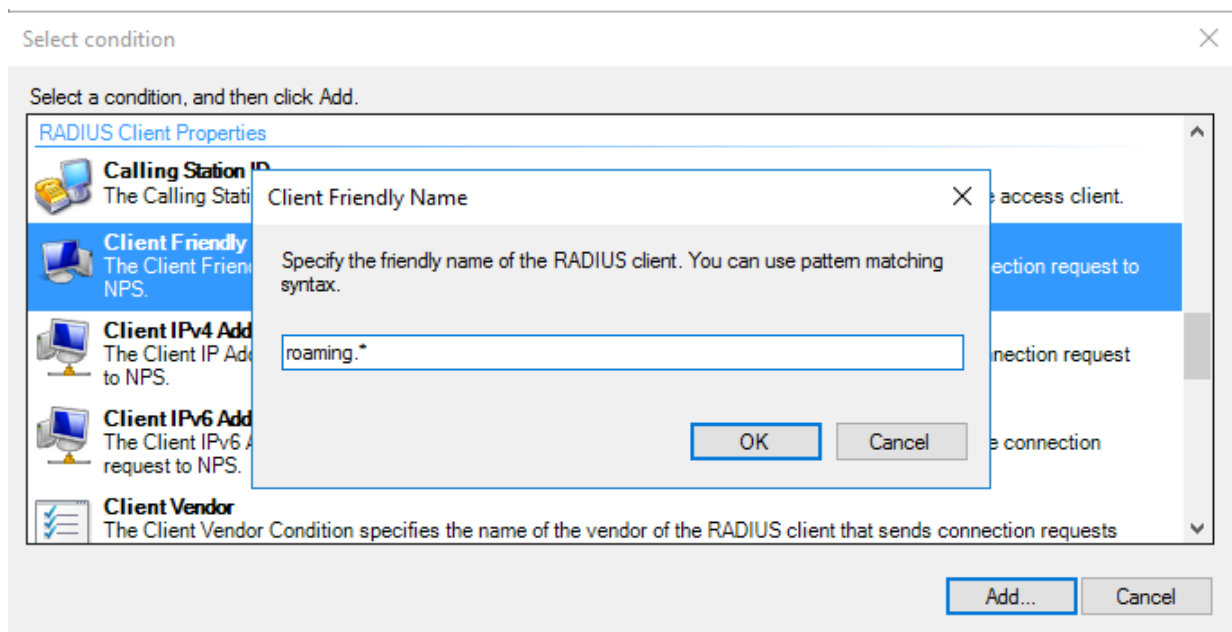
☐ Vendor specific:  
10



On the **Specify Conditions** page click **Add** then click on **Client Friendly Name** then click **Add**.




In the **Client Friendly Name** box enter `roaming.*` then click **OK** and the **Next** on the following screen.



For Authentication select **Authenticate requests on this server** and 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:**

**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:


NRPS ▼ New...

☐ Accept users without validating credentials

Previous Next Finish Cancel

Click **Next** on the **Configure Settings** screen.

New Connection Request Policy ✕

 **Configure Settings**

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

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

**Settings:**

**Specify a Realm Name**

- Attribute
- RADIUS Attributes**
- Standard
- ☒ Vendor Specific

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

Attribute: Called-Station-Id ▼

Rules:


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

Add Edit Remove Move Up Move Down

Previous Next Finish Cancel

We recommend you support anonymous outer identities, so choose **Override-network policy authentication setting'** and **Add EAP Type of Microsoft: Protected EAP (PEAP)**

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.

☒ **Override network policy authentication settings**  
These authentication settings are used rather than the constraints and authentication settings in network policy.

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

**EAP Types:**

Microsoft: Protected EAP (PEAP)	Move Up	Move Down
---------------------------------	---------	-----------

Add... Edit... Remove

**Less secure authentication methods:**

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)  
☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)  
☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)


☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

Previous Next Finish Cancel

Click **Finish** on the final screen.

New Connection Request Policy ×

 **Completing Connection Request Policy Wizard**

You have successfully created the following connection request policy:

**authenticate requests from NRPS locally**

**Policy conditions:**

Condition	Value
Client Friendly Name	roaming*

**Policy settings:**

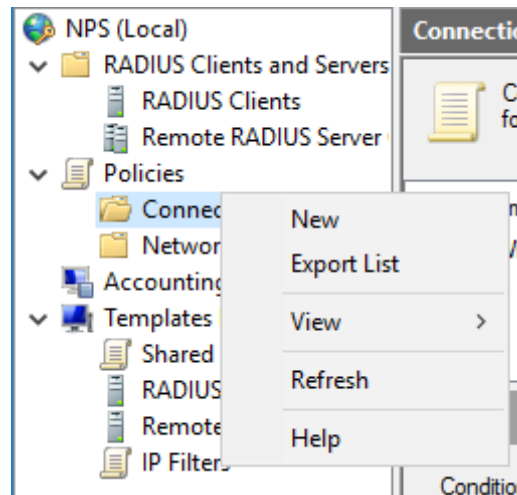
Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.

Previous Next Finish Cancel

## 16. Add a Connection Request Policy for local users

To authenticate local users a policy needs to be created. To do this, in **Network Policy Server** under **Policies**, right click on **Connection Request Policies** and click **New**.



In **Policy name** enter `authenticate local users`, and then click **Next**.

### 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

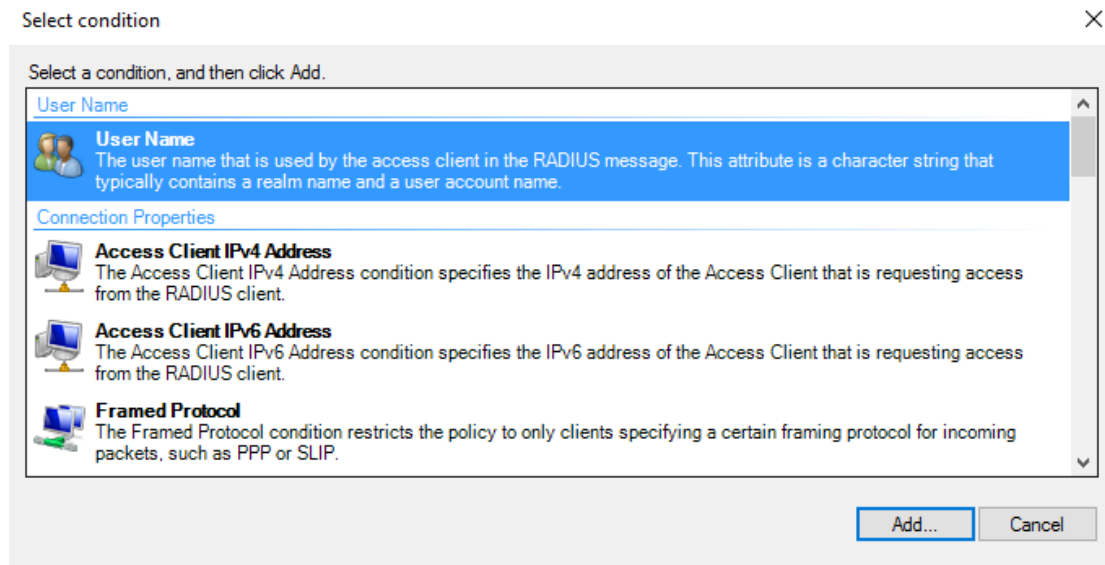
**Policy name:**

**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.

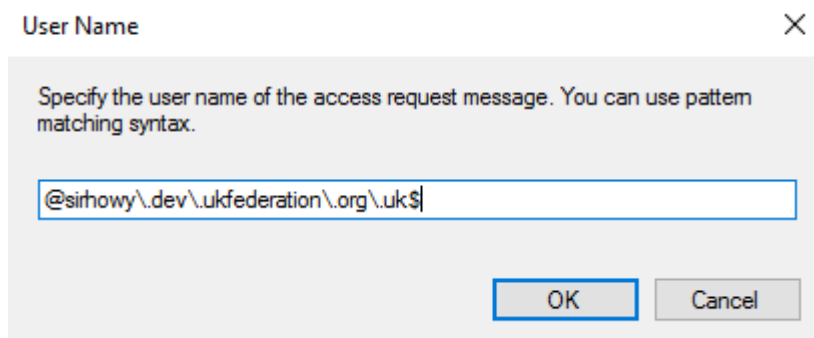
☒ Type of network access server:

☐ Vendor specific:

On the **Specify Conditions** page click **Add**, then click on **User Name**, then click **Add**.



In the '**User Name**' box enter a regularly expression formatted as `@realm$`, where realm is your organization's realm e.g. camford.ac.uk, ensure to put a backslash before each full-stop `@camford\.ac\.uk$` then click **OK**.



See [using the pattern matching syntax in NPS](#)

Click **Next** then for Authentication choose **Authenticate requests on this server** 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.

Condition	Value
User Name	@sirhowy\dev\ukfederation\org\uk\$

Condition description:

Add... Edit... Remove

Previous Next Finish Cancel

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:

NRPS New...

☐ Accept users without validating credentials

Previous Next Finish Cancel

We recommend you support anonymous outer identities, so choose **Override-network policy authentication setting'** and Add EAP Type of **Microsoft: Protected EAP (PEAP)**


The screenshot shows the 'New Connection Request Policy' dialog box with the 'Specify Authentication Methods' tab selected. The dialog has a title bar with 'New Connection Request Policy' and a close button. Below the title bar is a section with a computer icon and the title 'Specify Authentication Methods'. The text below the icon says: 'Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.' Below this is a checkbox labeled 'Override network policy authentication settings' which is checked. Below the checkbox is a text box containing 'Microsoft: Protected EAP (PEAP)'. To the right of the text box are 'Move Up' and 'Move Down' buttons. Below the text box are 'Add...', 'Edit...', and 'Remove' buttons. Below these buttons is a section titled 'Less secure authentication methods:' with several checkboxes: 'Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)', 'Microsoft Encrypted Authentication (MS-CHAP)', 'Encrypted authentication (CHAP)', 'Unencrypted authentication (PAP, SPAP)', and 'Allow clients to connect without negotiating an authentication method.' At the bottom of the dialog are 'Previous', 'Next', 'Finish', and 'Cancel' buttons.

In the list of **EAP Types**: select **Microsoft: Protected EAP (PEAP)** and click **Edit....** Then select the correct certificate in the **Certificate issued** list and ensure **Secured password (EAP-MSCHAP v2)** is in the list of **EAP Types**. Then click **OK**.

The screenshot shows the 'Edit Protected EAP Properties' dialog box. The title bar says 'Edit Protected EAP Properties'. The main text says: '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.' Below this is a 'Certificate issued to:' dropdown menu showing 'radius-nps-guide.sirhowy.dev.ukfederation.org.uk'. Below the dropdown are fields for 'Friendly name:', 'Issuer:', and 'Expiration date:'. Below these fields are checkboxes for 'Enable Fast Reconnect' (checked), 'Disconnect Clients without Cryptobinding', and 'Eap Types'. Below the 'Eap Types' section is a list box containing 'Secured password (EAP-MSCHAP v2)'. To the right of the list box are 'Move Up' and 'Move Down' buttons. At the bottom are 'Add', 'Edit', 'Remove', 'OK', and 'Cancel' buttons.

Click **Next** on the **Configure Settings** screen.

New Connection Request Policy ✕

 **Configure Settings**

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

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

**Settings:**

**Specify a Realm Name**

☐ Attribute

**RADIUS Attributes**

☐ Standard

☒ Vendor Specific

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


Attribute:

Rules:

Find	Replace With

Click **Finish** on the final screen.

New Connection Request Policy ✕

 **Completing Connection Request Policy Wizard**

You have successfully created the following connection request policy:

**authenticate local users**

**Policy conditions:**

Condition	Value
User Name	@sihowy\dev\ukfederation\org\uk\$

**Policy settings:**

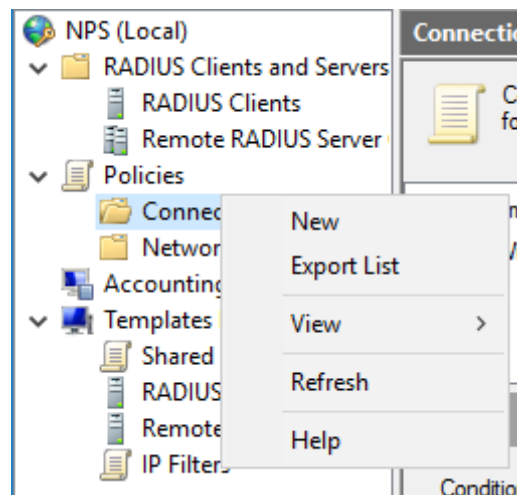
Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.



## 17. Add a Connection Request Policy for eduroam visitors

To proxy visitor authentications to the NRPS a policy needs to be created. To do this, in **Network Policy Server** under **Policies**, right click on **Connection Request Policies** and click **New**.



In **Policy name** enter proxy to eduroam, then click **Next**.

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:**  
proxy to eduroam

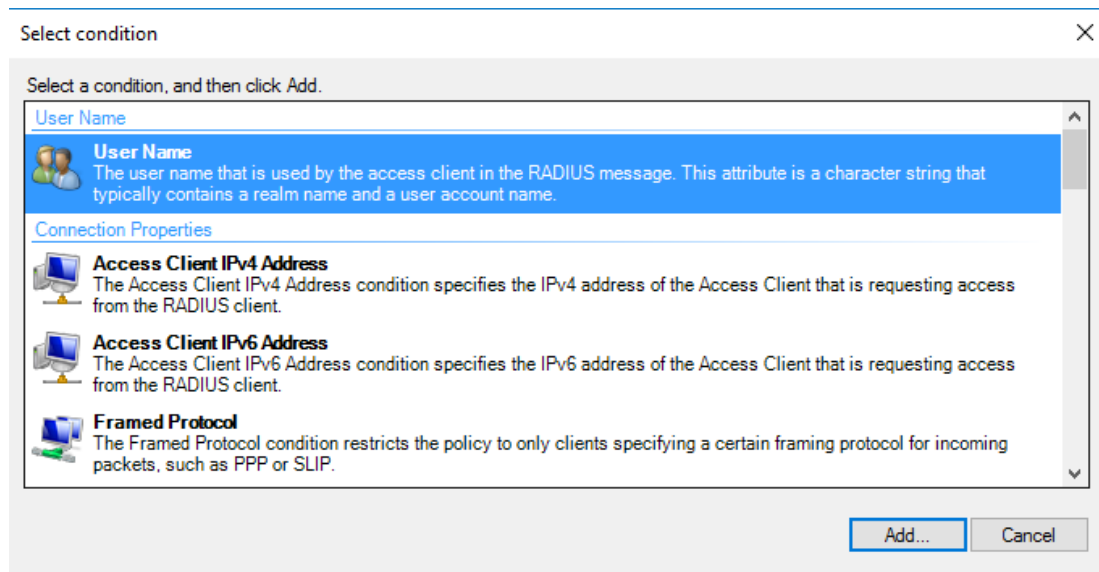
**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point,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

☒ Type of network access server:  
Unspecified

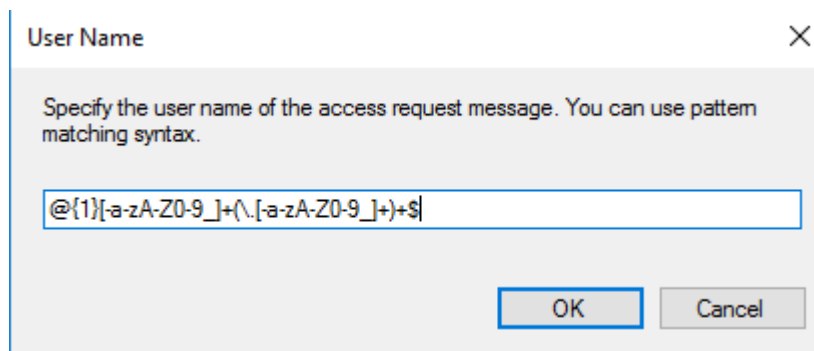
☐ Vendor specific:  
10

Previous Next Finish Cancel

On the **Specify Conditions** page click **Add** then click on **User Name** then click **Add**.



In the **User Name** box enter `@{1}[-a-zA-Z0-9_]+(\.[-a-zA-Z0-9_]+)+$` then click **OK**.



Click **Next** then for **Authenticate** tick **Forward requests to the following RADIUS server group for authentication:** and select **NRPS** from the dropdown list.

See [using the pattern matching syntax in NPS](#)

Click **Next** then click **Finish** on the final screen.

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:

NRPS New...

☐ Accept users without validating credentials

Previous Next Finish Cancel

New Connection Request Policy

### Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

**proxy to eduroam**

**Policy conditions:**

Condition	Value
User Name	@{1}[a-zA-Z0-9 ]+\.[a-zA-Z0-9 ]+.*

**Policy settings:**

Condition	Value
Authentication Provider	Forwarding Request
Authentication Provider Name	NRPS

To close this wizard, click Finish.





Previous Next Finish Cancel

## 18. Reorder Connection Request Policies

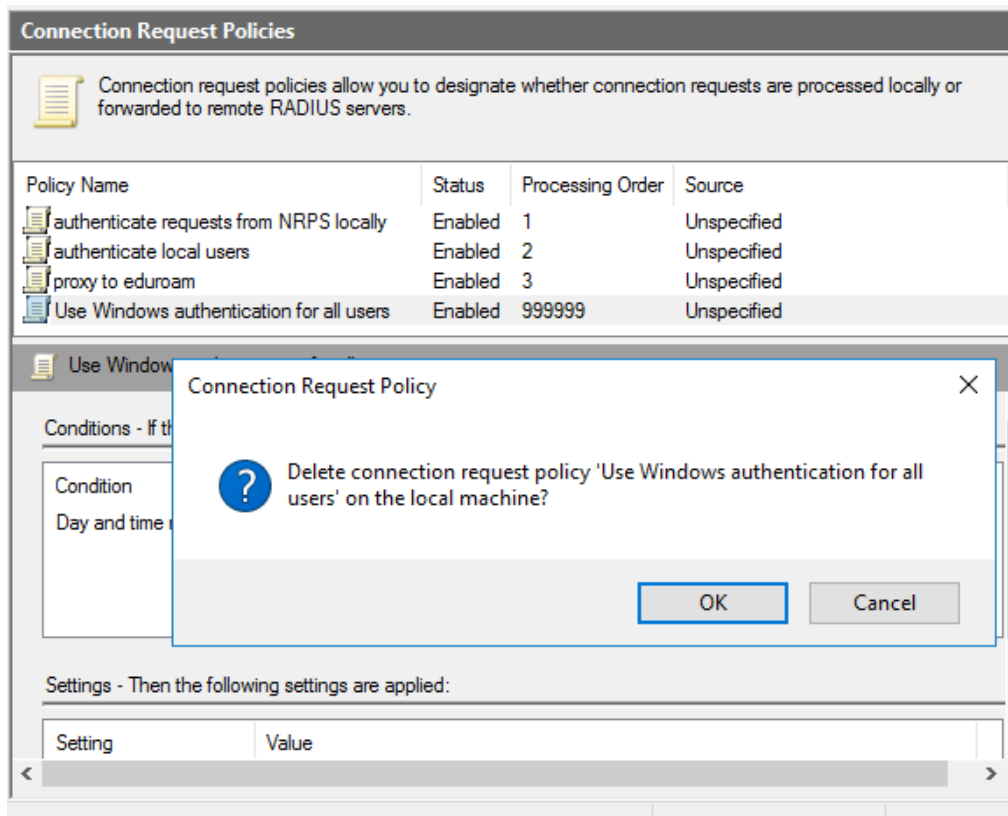
To ensure that local requests are processed first before proxying to eduroam, reorder the list into the following order:

1. authenticate requests from NRPS locally
2. authenticate local users
3. proxy to eduroam

To do this right click on a policy and then click **Move up** or **Move down** until it is in the correct position in the list.

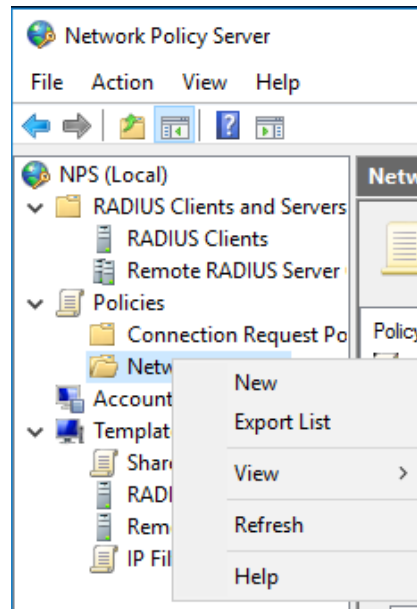
Connection Request Policies			
 Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.			
Policy Name	Status	Processing Order	Source
 authenticate requests from NRPS locally	Enabled	1	Unspecified
 authenticate local users	Enabled	2	Unspecified
 proxy to eduroam	Enabled	3	Unspecified

If the “Use Windows authentication for all users” policy exists, then delete it.



## 19. Create Network Policy

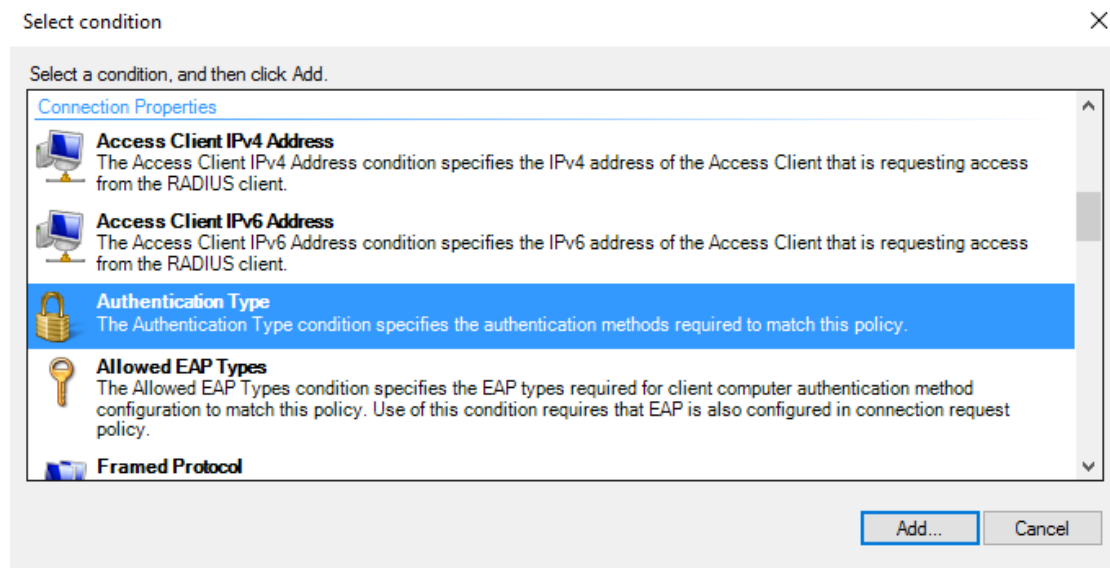
To authenticate users on the server a Network Policy needs to be created. To do this, in **Network Policy Server** under **Policies**, right click on **Network Policies** and click **New**.



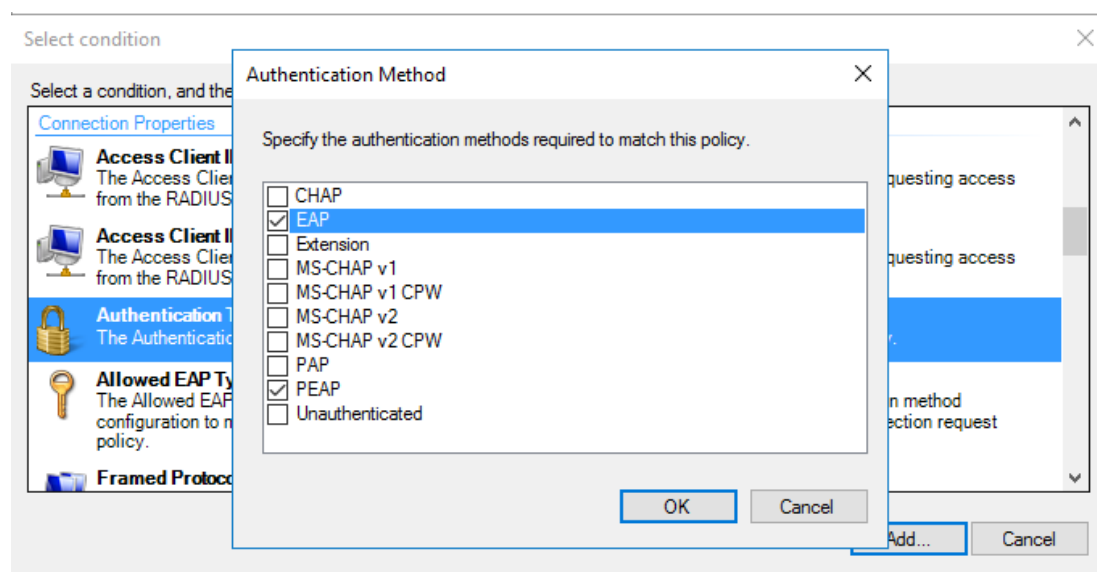
In the **Policy name:** box enter **local authentication** and then click **Next**.

A screenshot of the 'New Network Policy' wizard. The title bar says 'New Network Policy'. The main heading is 'Specify Network Policy Name and Connection Type'. Below this is a sub-heading: 'You can specify a name for your network policy and the type of connections to which the policy is applied.' The 'Policy name:' field contains 'local authentication'. Below this is the 'Network connection method' section. It has a description: '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.' There are two radio buttons: 'Type of network access server:' (selected) and 'Vendor specific:'. Under 'Type of network access server:', there is a dropdown menu showing 'Unspecified'. Under 'Vendor specific:', there is a dropdown menu showing '10'. At the bottom are buttons: 'Previous', 'Next' (highlighted), 'Finish', and 'Cancel'.

In the **Specify Conditions** window click **Add...** then from the list choose **Authentication Type** and click **Add...**




From the **Authentication Method** list choose **EAP** and **PEAP** then click **OK**.




Click **Next** then tick **Access granted** on the **Specify Access Permission** page, then click **Next** again.

New Network Policy ✕

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

**Conditions:**


Condition	Value
 Authentication Type	EAP OR PEAP

Condition description:  
The Authentication Type condition specifies the authentication methods required to match this policy.

Add... Edit... Remove

Previous Next Finish Cancel

New Network Policy ✕

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

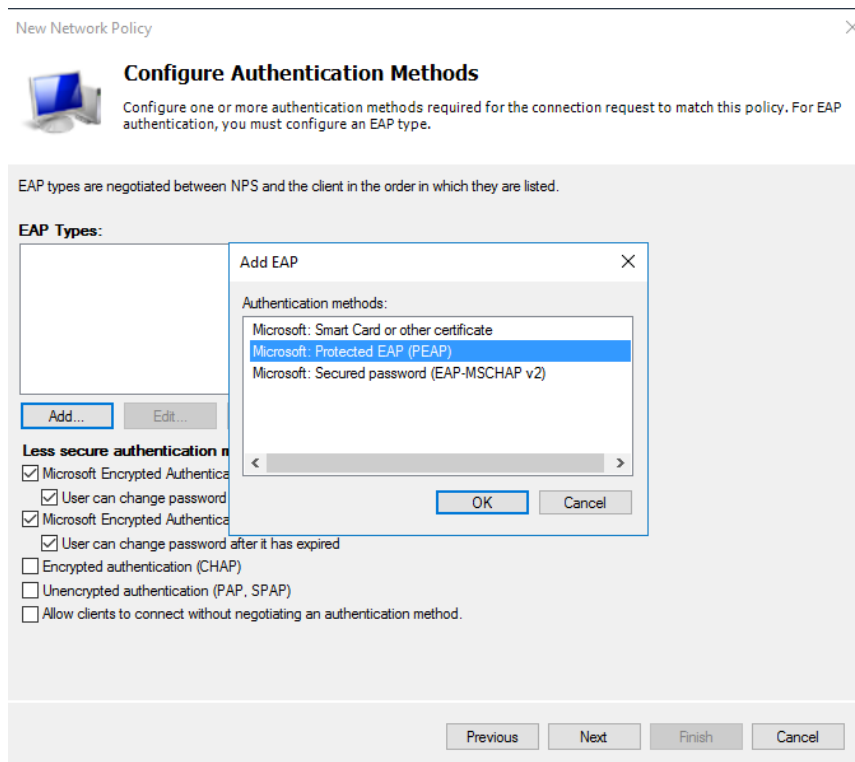
☒ **Access granted**  
Grant access if client connection attempts match the conditions of this policy.

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

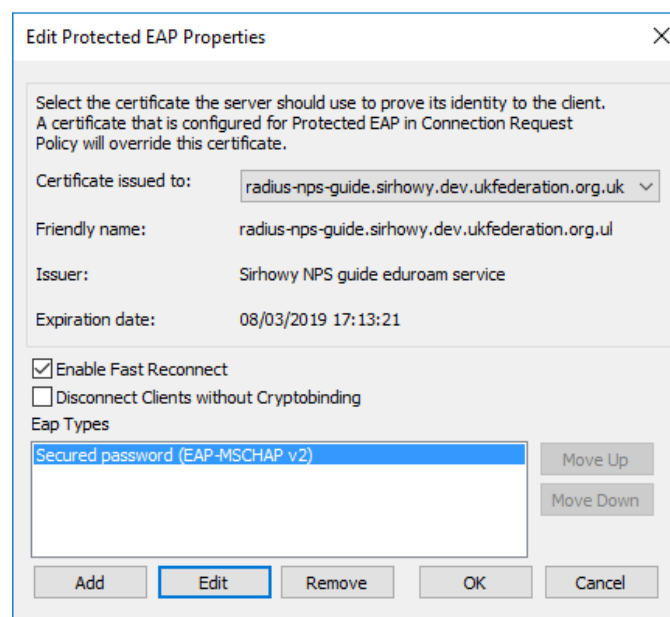
☐ **Access is determined by User Dial-in properties (which override NPS policy)**  
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

On the **Configure Authentication Methods** page click **Add...**



In the list of **EAP Types**: select **Microsoft: Protected EAP (PEAP)** and click '**Edit...**'. Then select the correct certificate in the **Certificate issued** list and ensure **Secured password (EAP-MSCHAP v2)** is in the list of **EAP Type**'. Then click **OK**.



On the **Configure Authentication Methods** page untick all **Less secure authentication methods**. Then 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.

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

**EAP Types:**

Microsoft: Protected EAP (PEAP)

Move Up

Move Down

Add...

Edit...

Remove

**Less secure authentication methods:**

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

Previous

Next

Finish

Cancel

On the **Configure Constraints** page click **Next**. Then on the **Configure Settings** page, under **RADIUS Attributes**, **Standard** remove both **Framed-Protocol PPP** and **Service-Type Framed** from the list.

## New Network Policy

**Configure Settings**

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

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

**Settings:****RADIUS Attributes**

- ☒ Standard
- ☒ Vendor Specific
- 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

Add...

Edit...

Remove

Previous


Next

Finish

Cancel

Under **Routing and Remote Access, Encryption** untick **No encryption**. Then 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:**

**RADIUS Attributes**

-  Standard
-  Vendor Specific

**Routing and Remote Access**

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

The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

If you use different network access servers for dial-up or VPN connections, ensure that the encryption settings you select are supported by your servers.


If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

☒ Basic encryption (MPPE 40-bit)  
☒ Strong encryption (MPPE 56-bit)  
☒ Strongest encryption (MPPE 128-bit)  
☐ No encryption

Previous **Next** Finish Cancel

Next, in the **Access Permission** area, choose **Access Granted**

New Network Policy ✕

 **Specify Access Permission**

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

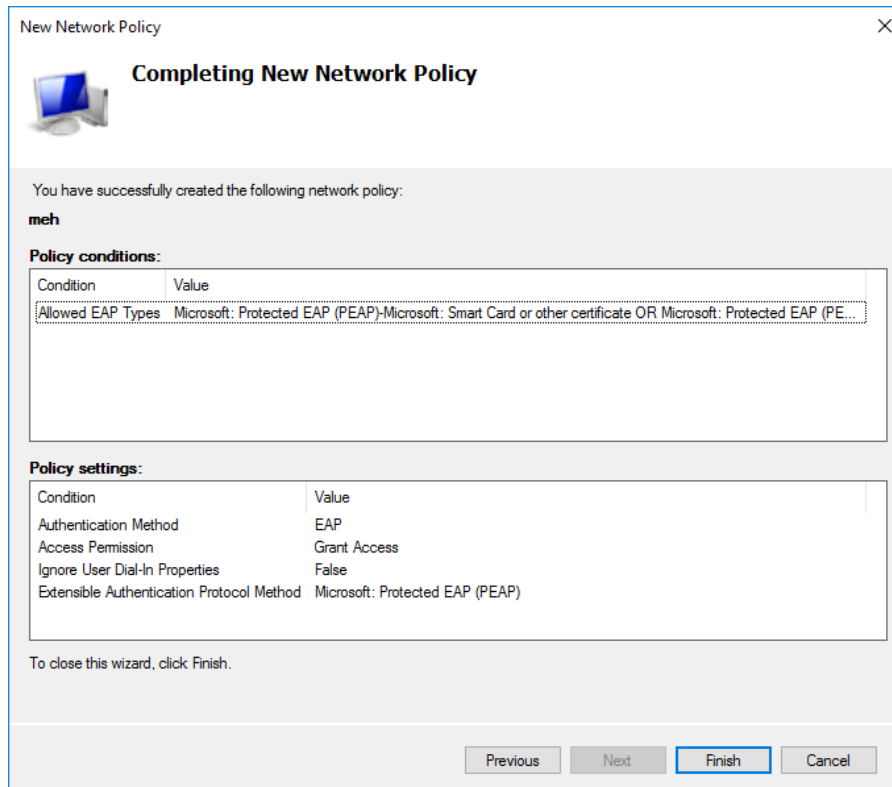
☒ **Access granted**  
Grant access if client connection attempts match the conditions of this policy.

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

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

Previous **Next** Finish Cancel

Then click **Finish** on the **Completing New Network Policy** page.



The screenshot shows the 'Completing New Network Policy' wizard. It displays the policy name 'meh' and its conditions. The policy settings table is as follows:

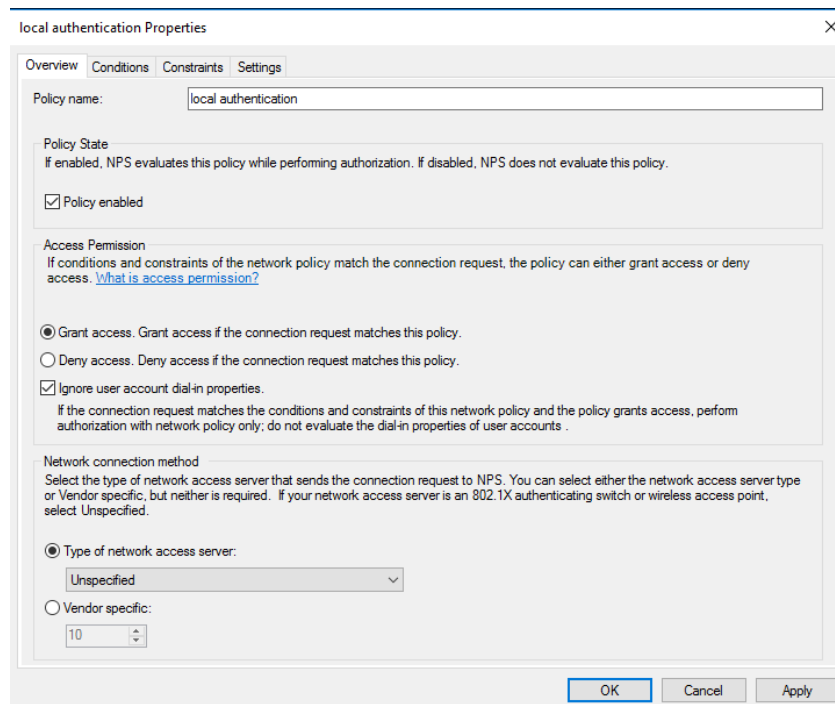
Condition	Value
Allowed EAP Types	Microsoft: Protected EAP (PEAP)-Microsoft: Smart Card or other certificate OR Microsoft: Protected EAP (PEAP)

Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Ignore User Dial-In Properties	False
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)

At the bottom, there are buttons for 'Previous', 'Next', 'Finish' (highlighted), and 'Cancel'.

**Optional:** This setting will depend on whether you would like to control access via the Dial-in Properties in Active Directory Users and Computers on a per user basis. If not, change the settings to **Ignore user account dial-in properties** from the Active Directory. To do this double click on the **local authentication** policy.



The screenshot shows the 'Local authentication Properties' dialog box. The 'Overview' tab is selected. The policy name is 'local authentication'. The 'Policy State' is 'Policy enabled'. The 'Access Permission' is 'Grant access'. The 'Ignore user account dial-in properties' checkbox is checked. The 'Network connection method' is 'Type of network access server' with a dropdown menu set to 'Unspecified'.

Policy name: local authentication

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

Buttons: OK, Cancel, Apply

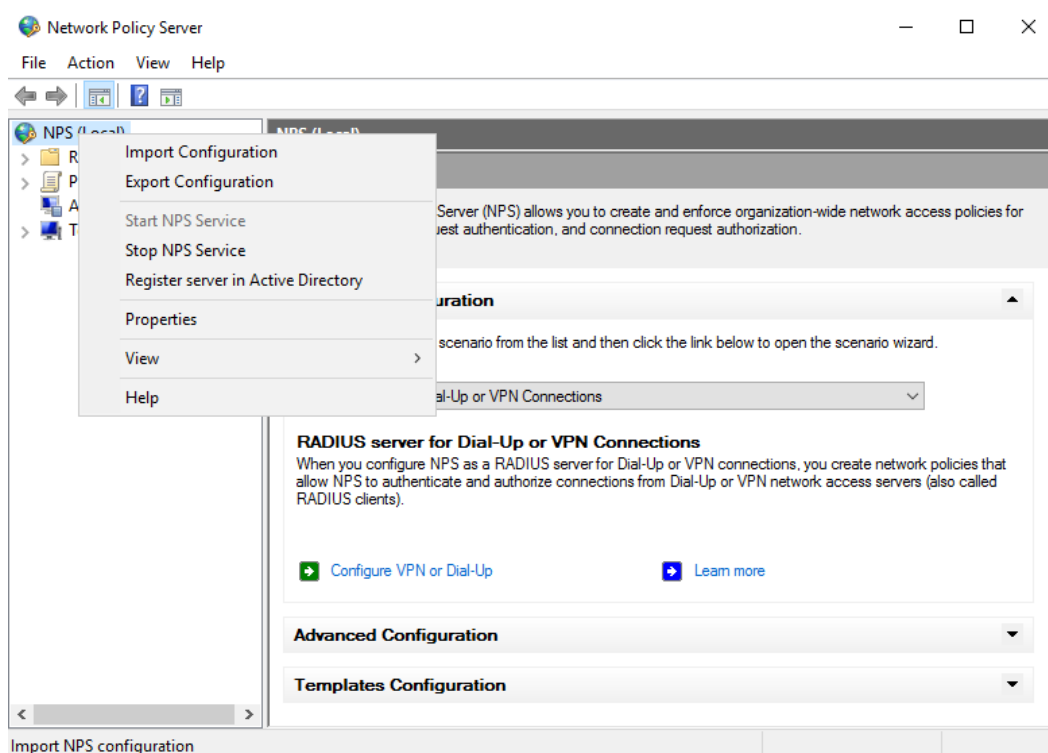
Network Policies				
 Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.				
Policy Name	Status	Processing Order	Access Type	S
 local authentication	Enabled	1	Grant Acce...	U
 Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	U
 Connections to other access servers	Enabled	999999	Deny Access	U

To ensure that local authentication is processed first, reorder the list so that local authentication is first. To do this right click on a policy and then click **Move up** or **Move down** until it is in the correct position in the list.

## 20. Register server in Active Directory

You should follow the process of registering the server in Active Directory.

Right click on **NPS (Local)**, choose **Register server in Active Directory**



Click **OK** on the next two dialogues.

## Network Policy Server



To enable NPS to authenticate users in the Active Directory, the computers running NPS must be authorized to read users' dial-in properties from the domain.

Do you wish to authorize this computer to read users' dial-in properties from the sirhowy.dev.ukfederation.org.uk domain?

OK

Cancel

## Network Policy Server



This computer is now authorized to read users' dial-in properties from domain sirhowy.dev.ukfederation.org.uk.

To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/NPS Servers Group in that domain.

OK