

# Microsoft NPS Configuration Guide eduroam (UK)

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

## Contents

1.	Introduction
2.	Limitations of Network Policy Server5
3.	Installing NPS6
4.	Certificates and Certificate Authority 10
5.	Install and configure a Standalone Certificate Authority12
6.	Change the Certificate Authority - Validity period
7.	Change the Certificate Authority - CRL Distribution Points
8.	Creating the Server Certificate 25
9.	Signing your certificate requests with your CA
10.	Import the Server Certificate
11.	Configure NRPS Shared Secrets Template 41
12.	Add NRPS as RADIUS Clients 42
13.	Add local Access Points / Wireless Infrastructure RADIUS Clients
14.	Add NRPS as RADIUS Proxy Servers45
15.	Add a Connection Request Policy for your roaming users
16.	Add a Connection Request Policy for local users
17.	Add a Connection Request Policy for eduroam visitors57
18.	Reorder Connection Request Policies60
19.	Create Network Policy
20.	Register server in Active Directory68



### 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
o.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-servicesdocumentation/implementing-eduroam-roadmap
- ii) the eduroam(UK) Technical Specification https://community.ja.net/library/janet-servicesdocumentation/eduroamuk-technical-specification
- iii) Attribute Filtering for Microsoft IAS and NPS: https://community.ja.net/library/janet-servicesdocumentation/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 .

📥 Add Roles and Features Wizard	— C	×
Before you begin	DESTINATION radius-nps-gui.sirhowy.dev.ukfederatio	SERVER 1.org.uk
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	<ul> <li>This wizard helps you install roles, role services, or features. You determine which roles, role services to install based on the computing needs of your organization, such as sharing document hosting a website.</li> <li>To remove roles, role services, or features:</li> <li>Start the Remove Roles and Features Wizard</li> <li>Before you continue, verify that the following tasks have been completed: <ul> <li>The Administrator account has a strong password</li> <li>Network settings, such as static IP addresses, are configured</li> <li>The most current security updates from Windows Update are installed</li> </ul> </li> <li>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.</li> <li>To continue, click Next.</li> </ul> <li>Skip this page by default</li>	ces, or its, or
	< Previous Next > Install Ca	incel

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

	- ·
Before You Begin	machine, or on an offline virtual hard disk (VHD).
Server Selection	Role-based or feature-based installation
Server Roles	Configure a single server by adding roles, role services, and features.
Features	Remote Desktop Services installation
Confirmation	or session-based desktop deployment.
Results	

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

Before You Begin	Select a server or a virtual hard disk on which to install roles and features.
Installation Type	<ul> <li>Select a server from the server pool</li> </ul>
Server Selection	<ul> <li>Select a virtual hard disk</li> </ul>
Server Roles	Server Pool
Features	
	Filter:
	Name IP Address Operating System
	radius-nps-gui.sirhowy.d 172.16.196.24 Microsoft Windows Server 2016 Standard
	1 Computer(s) found

**Jisc** 



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

elect server ro	Add Roles and Features Wizard	X gui.sirhowy.dev.ukfederation.org.u
Before You Begin Installation Type	Add features that are required for Network Policy and Access Services?	otion
Server Selection         The following tools are required to manage this feature, but do n have to be installed on the same server.		rk Policy and Access Services es Network Policy Server
Features Confirmation Results	<ul> <li>Remote Server Administration Tools</li> <li>Role Administration Tools         [Tools] Network Policy and Access Services Tools     </li> </ul>	y of your network.
	✓ Include management tools (if applicable)          Add Features       Cancel	

No additional features are required, click Next

Jisc



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

Jisc

To install the following roles, role services, or features on selected server, click Install.				
Kestart 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 hoves				
Network Policy and Access Services				
Remote Server Administration Tools				
Role Administration Tools				
Network Folicy and Access Services Tools				
Export configuration settings				

#### 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.

🔁 Add Roles and Features Wizard		-		×
Before you begin	radius-nps-gui.sirhow	DESTIN/ y.dev.ukfed	ATION SER\ leration.org	/ER J.uk
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	<ul> <li>This wizard helps you install roles, role services, or features. You determine which features to install based on the computing needs of your organization, such as shorting a website.</li> <li>To remove roles, role services, or features: Start the Remove Roles and Features Wizard</li> <li>Before you continue, verify that the following tasks have been completed: <ul> <li>The Administrator account has a strong password</li> <li>Network settings, such as static IP addresses, are configured</li> <li>The most current security updates from Windows Update are installed</li> <li>If you must verify that any of the preceding prerequisites have been completed, or complete the steps, and then run the wizard again.</li> </ul> </li> <li>To continue, click Next.</li> </ul>	roles, role aring doc	e services, uments, «	or 3r

< Previous Next >

Install

Cancel

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 like to be the server that you are currently using.

📥 Add Roles and Features Wizard		_		×
Select destination	Server radius-nps-gui.sir	DESTIN/ howy.dev.ukfed	ATION SERV eration.org	VER J.uk
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features.    Select a server from the server pool  Select a virtual hard disk Server Pool  Filter:  Name IP Address Operating System radius-nps-gui.sirhowy.d 172.16.196.24 Microsoft Windows Server 20	16 Standard		
Select the <b>Active Directory Certif</b>	1 Computer(s) found This page shows servers that are running Windows Server 2012 or a newer reli and that have been added by using the Add Servers command in Server Mana newly-added servers from which data collection is still incomplete are not sho < Previous Next >	ease of Wind ager. Offline s wn. Install	ows Serve ervers an Cance	er, Id
🚵 Add Roles and Features Wizard		-		×
Select server roles	radius-nps-gui.sirt	DESTINA nowy.dev.ukfede	TION SERVE ration.org.u	:R Jk
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Roles       Description         Active Directory Certificate Services       Active Directory Domain Services         Active Directory Federation Services       Active Directory Lightweight Directory Services         Active Directory Rights Management Services       and manage         Device Health Attestation       DHCP Server         Fax Server       File and Storage Services (1 of 12 installed)         Host Guardian Services       WultiPoint Services         Network Policy and Access Services (Installed)       Print and Document Services         Remote Desktop Services       Volume Activation Services         Volume Activation Services       Web Server (IIS)	tory Certificat sed to create authorities ar that allow yc e certificates u pplications.	e Services nd related nu to issue ised in a	5 ] e

< Previous

Next >

Install

Cancel



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

Select server ro	Add Roles and Features Wizard	X gui.sirhowy.dev.ukfederation.org
Before You Begin Installation Type	Add features that are required for Active Directory Certificate Services?	ption
Server Selection Server Roles	The following tools are required to manage this feature, but do not have to be installed on the same server.	Directory Certificate Service ) is used to create
Features Confirmation Results	<ul> <li>Remote Server Administration Tools</li> <li>Role Administration Tools</li> <li>Active Directory Certificate Services Tools         [Tools] Certification Authority Management Tools</li> </ul>	vices that allow you to issu anage certificates used in a of applications.
	✓       Include management tools (if applicable)         Add Features       Cancel	

#### Click Next.

Select features		DESTINATION SER radius-nps-gui.sirhowy.dev.ukfederation.org
Before You Begin	Select one or more features to install on the selected server.	Description
Server Selection Server Roles Features Network Policy and Acces Confirmation Results	NET Framework 3.5 Features         Image: State Sta	.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 provi the ability to model a range of business processes.

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

📥 Add Roles and Features Wizard		-		×
Active Directory	Certificate Services radius-nps-gui.sirhowy.	DESTINA dev.ukfede	TION SERVI eration.org.(	ER uk
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Active Directory Certificate Services (AD CS) provides the certificate infrastructure t such as secure wireless networks, virtual private networks, Internet Protocol Securit 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 certi (CA) has been installed. If you want to change the computer name, join a domain server to a domain controller, complete these changes before installing the CA. I information, see certification authority naming.	o enable y (IPSec), fication a n, or pror For more	scenarios Network uthority note this	:
	Destant No. 1		(	_
	< Previous Next > Inst		Cancel	

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

📥 Add Roles and Features Wizard		- 🗆 X
Select role service Before You Begin	Select the role services to install for Active Directory Certificat	DESTINATION SERVER radius-nps-gui.sirhowy.dev.ukfederation.org.uk e Services
Installation Type Server Selection Server Roles Features AD CS <b>Role Services</b> Confirmation Results	Kole 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.
	< Previous Nex	t > Install Cancel



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

🚡 Add Roles and Features Wizard		-		×
Confirm installation	ON Selections radius-nps-gui.sirho	DESTIN/ wy.dev.ukfed	ATION SER\ deration.org	/ER J.uk
Before You Begin	To install the following roles, role services, or features on selected server, click In	istall.		
Installation Type	Restart the destination server automatically if required			
Server Selection Server Roles	Optional features (such as administration tools) might be displayed on this page been selected automatically. If you do not want to install these optional features their check boxes.	e because t s, click Prev	hey have vious to cl	ear
AD CS Role Services	Active Directory Certificate Services Certification Authority			
Confirmation	Remote Server Administration Tools Role Administration Tools			
Results	Active Directory Certificate Services Tools Certification Authority Management Tools			
	Export configuration settings Specify an alternate source path			
	< Previous Next > In	nstall	Cance	:I

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

📥 Add Roles and Features Wizard		_		$\times$
Installation progres	S radius-nps-gui.sirhow	DESTINA y.dev.ukfede	TION SERV eration.org	/ER .uk
Before You Begin	View installation progress			
Installation Type	1 Feature installation			
	· · · · · · · · · · · · · · · · · · ·			
Server Roles	Configuration required. Installation succeeded on radius-nps-			
	gui.sirnowy.dev.uktederation.org.uk.			
AD CS	Active Directory Certificate Services			
Role Services	Additional steps are required to configure Active Directory Certificate Services server	s on the d	estinatio	n
Confirmation	Configure Active Directory Certificate Services on the destination server			
Results	Certification Authority			
	Remote Server Administration Tools			
	Active Directory Certificate Services Tools			
	Certification Authority Management Tools			
	You can close this wizard without interrupting running tasks. View task pro	gress or o	open this	
	<ul> <li>page again by clicking rotuncations in the command bar, and then lask b</li> <li>Event configuration settings</li> </ul>	cidiis.		
	export configuration settings			
	< Previous Next > Clo	ose	Cance	



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



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

📥 AD CS Configuration			-		$\times$
Role Services		radius-nps-gui.sir	DESTINAT howy.dev.ukfede	ION SER	VER g.uk
Credentials	Select Role Services to configure				
Role Services	_				
Setup Type	<ul> <li>Certification Authority</li> </ul>				
СА Туре	Certification Authority Web Enrollment				
Private Key	Network Device Enrollment Service				
Cryptography	Certificate Enrollment Web Service				
CA Name	Certificate Enrollment Policy Web Service				
Certificate Request					
Certificate Database					
Confirmation					
Progress					
Results					
	More about AD CS Server Roles				
	< Previous	Next >	Configure	Cance	el



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.



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



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



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

#### Nb.Do not use SHA1 or MD5.

📥 AD CS Configuration			-		×
Cryptography for	CA	radius-nps-gui.sirh	DESTINAT nowy.dev.ukfeder	ION SERV ation.org	/ER .uk
Credentials Role Services	Specify the cryptographic options	5			
Setup Type	Select a cryptographic provider:		Key length:		
СА Туре	RSA#Microsoft Software Key Storage Provider	~	2048		۲
Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select the hash algorithm for signing certificates SHA256 SHA384 SHA512 SHA1 MD5 Allow administrator interaction when the priv	issued by this CA:	by the CA.		
	More about Cryptography				
	< Previous	Next >	Configure	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



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



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



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.

📥 AD CS Configuration			-		$\times$
Confirmation		DES radius-nps-gui.sirhowy.dev.u	TINATIO	ON SERV tion.org.	'ER .uk
Credentials Role Services	To configure the following roles, <ul> <li>Active Directory Certificat</li> </ul>	role services, or features, click Configure. e Services			
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authority CA Type: Cryptographic provider: Hash Algorithm: Key Length: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location: Certificate Database Log Location:	Standalone Root RSA#Microsoft Software Key Storage Provider SHA256 2048 Disabled 08/03/2068 15:45:00 CN=Sirhowy NPS guide eduroam service,DC=sirhowy,DC=dev,DC=ukfederation, C:\Windows\system32\CertLog C:\Windows\system32\CertLog	DC=org	,DC=uk	
		< Previous Next > Configu	re	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;





### 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

onsole Root	Issued To	Add or Permove Span-inc		Emination Data Internalized Derma	Friendle Manaa
Certificates (Local Computer)        Personal     Certificates      Certificates     Enterprise Trust     Enterprise Trust     Compared at a Certification Authorities	E <sub>p</sub> l Sirhowy	You can select snap-ins for this consol extensible snap-ins, you can configure Available snap-ins:	e from those available on yo which extensions are enab	Selected snap-ins:	set of snap-ins. For
Intermediate Certification Authonities Intrusted Volishers Intrusted Certificates Intrusted People Client Authentication Issuers Preview Build Roots Remote Desktop Smart Card Trusted Roots Intrusted Devices Windows Live ID Token Issuer		Snap-in Vender Active X Control Microsoft Cartholize Anthonization Manager Microsoft Carthicate Templates Microsoft Carthicates Microsoft Component Services Microsoft Computer Managem Microsoft Device Manager Microsoft Enterprise PKI Microsoft Enterprise PKI Microsoft Enterprise PKI Microsoft Enterprise PKI Microsoft Component PKI	Cor Cor Cor Cor Cor Cor Cor Cor Cor Cor Cor Cor Cor Cor Cor Add >	Console Koot	Eat Extensions Remove Move Up Move Down
		Group Policy Object Microsoft Bescription: Allows you to configure certification a	t cor v	manage certificates issued by this CA.	Advanced OK Cancel

#### Choose Local Computer

Console Root	Issued To	A Issued Dy	Evolution Data Intended Durne	cos Eriandhy Mamo
Certificates (Local Computer)  Certificates Certificates  Certificates	Sirhowy 4		n) Browse	Edit Extensions  Edit Extensions  Remove  Move Up  Move Down
		< Back Finish Allows you to configure certification authority properties and to m	Cancel Help	Advanced



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

onsole Root	leaved Te	^	and Div		Emination Data Intended Burns	Friendly Name	-
Certificates (Local Computer)     Certificates (Local Computer)     Certificates     Trusted Root Certification Authorities     Intermediate Certification Authorities     Intrusted Publishers     Untrusted Certificates     Thrid-Party Root Certification Authorities     Trusted People     Client Authentication Issuers     Preview Build Roots     Remote Desktop     Smart Card Trusted Roots     Trusted Devices     Windows Live ID Token Issuer	Issued Io Sinformy AA	dd or Remove Snap-ins ou can select snap-ins for t xtensible snap-ins; Snap-in Active X Control Authorization Manager Certificate Templates Certificates Certificates Computer Managem Component Services Computer Managem Dek Management Enterprise PKI Enterprise PKI Enterprise PKI Coro Policy Object Folder	tis console from the configure which ex Wendor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	se available on yo tensions are enab	ur computer and configure the selected : led. Selected snap-ins: Console Root Console Root Console Root Console Computer)	Edit Extensions Edit Extensions Remove Move Up Move Down Advanced	×
	Ĺ	Allows you to configure cer	tification authority	properties and to r	manage certificates issued by this CA.	0%	

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

🐻 certsrv - [Certification Authority (Local)\Sirhowy NPS guide eduroam service]	_	×
File Action View Help		
Certification Authority (Local) Name		 
All Tasks		
View >		
Refresh		
Export List		
Properties		
Help		
Exports the current list to a file.		



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.

nowy NPS guide edu					
Enrollment Agents	Auditing	Recover	y Agents	Seci	urity
General	Policy Mod	lule	E	xit Module	
Extensions	Storage		Certificate	e Managers	
Select extension:					
CRL Distribution Point	(CDP)				~
http://www.sirhowy.d	ev.uktederation.o	org.uk/edu	roam-ca.c	đ	
<					>
<		Ad	d	Remove	>
Publish CRLs to this	s location	Ad	d	Remove	> *
Publish CRLs to this     Include in all CRLs.     when publishing ma	s location Specifies where anually.	Ad to publish i	<b>d</b>	Remove	> >
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. Cl</li> </ul>	s location . Specifies where anually. ients use this to fi	Ad to publish i ind Delta C	d in the Acti RL locatio	Remove ive Director	<b>&gt;</b>
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. CI</li> <li>Include in the CDP</li> </ul>	s location Specifies where anually. ients use this to fi extension of issu	Ad to publish i ind Delta C ed certifica	d in the Acti RL locatio tes	Remove ive Director	> y
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. CI</li> <li>Include in the CDP</li> <li>Publish Delta CRLs</li> </ul>	s location Specifies where anually. ients use this to f extension of issu	Ad to publish i ind Delta C ed certifica	d in the Acti RL locatio tes	Remove ve Director	> > y
Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs Include in the IDP /	s location Specifies where anually. ients use this to fi extension of issue to this location	Ad to publish i ind Delta C ed cettifica	d in the Acti RL locatio tes	Remove ve Director	> y
Publish CRLs to thi Include in all CRLs, when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs Include in the IDP el Include in the In	s location Specifies where anually. ients use this to fi extension of issue to this location extension of issue	Ad to publish i ind Delta C ed certifica ed CRLs	d in the Acti RL locatio tes	Remove ve Director	> > y
Publish CRLs to thii Include in all CRLs. When publishing ma Include in CRLs. CI Include in the CDP Publish Delta CRLs Include in the IDP of Include In the Include In	s location . Specifies where anually. ients use this to fi extension of issue to this location extension of issue	Ad to publish i ind Delta C ed certifica ed CRLs	d in the Acti RL locatio tes	Remove ve Director	> y

### 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 use 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 you own private CA and generate self-signed certificates you should see the instructions provided in the GÉANT guide GN<sub>3</sub>-NA<sub>3</sub>-T<sub>4</sub>-UFS1<sub>4</sub>o.

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**.

less is	Vondor	^		Console Root	Edit Extensions	
	venuor				Eur Extensions	
ActiveX Control	Microsoft Cor				Remove	
Authorization Manager	Microsoft Cor					
Certificate Templates	Microsoft Cor					
P Certificates	Microsoft Cor				Môve Up	
Certification Authority	Microsoft Cor				Move Down	
Component Services	Microsoft Cor		Add >		Libre bown	
Computer Managem	Microsoft Cor					
Device Manager	Microsoft Cor					
Disk Management	Microsoft and					
Enterprise PKI	Microsoft Cor					
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor				Advanced	

Choose Computer account and click Next.

Certificates span-in	× ۲
	: of snap-ins. For
This snap-in will always manage certificates for:	
O My user account	Edit Extensions
◯ Service account	Eur Extensions
Computer account	Remove
	Move Up
	Move Down
	Advanced
< Back Next > Cancel	r a computer.
	OK Cancel



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

Add as Pamaus Sana inc	× ا
Select the computer you want this snap-in to manage.	: of snap-ins. For
This snap-in will always manage:	Edit Extensions
O Another computer: Browse	Remove
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	Move Up
Cancel	Advanced r a computer.
	OK Cancel

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...**.

All	l Tasks	>	Request New Certificate				
Re	fresh		Import				
Exp	port List		Advanced Operations	>	Create Cust	tom Request	
Vie	ew	>			Manage En	rollment Policies	
Ar Lir	range Icons ne up Icons	>					
He	elp						
						>	

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

		—		>
Certificate Enrollment				
Select Certificate Enrollment Policy				
Certificate enrollment policy enables enrollment for certificates Certificate enrollment policy may already be configured for you	based on predefin	ned certificat	e templat	es.
Configured by your administrator				
Active Directory Enrollment Policy				٠
Configured by you			Add N	lew
Custom Request				
Proceed without enrollment policy				
		Next	Can	ncel

Choose Request format: PKCS #10 and click Next.

		_		×
🔄 Certificate Enrollment				
Custom request				
Chose an option from	the list below and configure the certificate options as required.			
Template:	(No template) CNG key		~	
	Suppress default extensions			-
Request format:	PKCS #10			
	Осмс			
Note: Key archival is	not available for certificates based on a custom certificate reques	t, even v	hen this	
option is specified in	the centricate template.			
	1	Vext	Cano	cel

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

Jisc

			_		×
🔄 Ce	rtificate Enrollment				
(	Certificate Information				
	Click Next to use the options already selected for this request, and then click Next.	template, or click Details to	customize	the certific	ate
	Custom request	STATUS: Available		Details	5 🔺
	The following options describe the uses and val Key usage: Application policies:	idity period that apply to th	is type of c	ertificate:	
	Validity period (days):			Properties	;
			Next	Ca	ncel

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

Certificat	e Propert	ties					×
General	Subject	Extensions	Private Key				
A friend	lly name	and descript	ion will mak	e it easier	to identify	and use a cert	tificate.
Friendly	/ name:						
Sirhow	y eduroa	m service					
Descrip	tion:						
eduroa	im servic	es for users a	t Sirhowy				
					ОК	Cancel	Apply



•

•

•

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 -C (country) i.e. GB
- -E(acontacte-mailaddress)e.g. it@camford.ac.uk
- Email • Locality

State

- -L(town/city)e.g. Camford
- Organization

Country

-O(Organisation Name) e.g. Camford University -S(County)e.g. Camfordshire

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

Certificate Properties		×
General Subject Extensions	Private Key	
The subject of a certificate is can enter information about can be used in a certificate.	the user or computer to wh the types of subject name a	nich the certificate is issued. You and alternative name values that
Subject of certificate		
The user or computer that is	receiving the certificate	
Subject name:		
Туре:		CN=radius.camford.ac.uk C=GB
Organization	Add >	E=it@camford.ac.uk
Value:	< Remove	L=Camford O=Camford University
		O=Camfordshire
Alternative name:		
Туре:		DNS
DNS ×	/	Tadius.camioru.ac.uk
Value:	Adds	
	Add >	
	< Remove	
	ОК	Cancel Apply



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

Certificate Properties	$\times$
General Subject Extensions Private Key	
The following are the certificate extensions for this certificate type.	^
Key usage 🗸 🗸	
Extended Key Usage (application policies)	
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.	
Available options: Selected options:	
Client Authentication Code Signing Secure Email Time Stamping Microsoft Trust List Signin Microsoft Time Stamping IP security end system IP security unnel termine IP security user C Make the Extended Key Usage critical	<pre></pre>
· · ·	*
OK Cancel Appl	1

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

Certificate Properties	×
General Subject Extensions Private Key	
Make the Extended Key Usage critical	^
Basic constraints	~
The basic constraints extension is used to indicate whether the certificate is a certificate or an end entity certificate.	a CA
Enable this extension	
Allow subject to issue certificates	
Path length:	
Make the basic constraints extension critical	
Include Symmetric algorithm	<b>*</b>
Custom extension definition	^
Custom extensions can be defined by specifying object identifiers (OIDs).	
Add the following custom extensions:	
Object ID:	¥
OK Cancel	Apply

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**.



Certificate Properties	×
General Subject Extensions Private Key	
ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider	^
Show all CSPs	
Key options	
Set the key length and export options for the private key.	
Key size: 2048 V	
Make private key exportable	
Allow private key to be archived	
Strong private key protection	
Select Hash Algorithm	
Select Hash Algorithm to be used for this request	
Hash Algorithm: sha256 🗸 🗸	
Select Signature Format	
	~
OK Cancel Apple	/

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**.

	_		×
📮 Certificate Enrollment			
Where do you want to save the offline request?			
If you want to save a copy of your certificate request or want to process the request later to your hard disk or removable media. Enter the location and name of your certificate re click Finish.	r, save t quest, a	he reques and then	,t
File Name: C:\Users\jagland\Documents\sirhowy-nps-guide.req	Br	owse	]
File format: Base 64 Binary			-
Fin	ish	Cano	:el

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

onsole Root  Certificates (Local Computer)  Certificates (Local Computer)  Conference	Issued To	Add or Remove Snap-ins	Furnisation Data Internet Duran	set of spaning. For	
Trusted Root Certification Authorities		extensible snap-ins, you can configure which extension Available snap-ins:	ns are enabled.		
Interprise must Intermediate Certification Authorities Trusted Publishers		Snap-in Vendor ^	Console Root	Edit Extensions	
Untrusted Certificates Third-Party Root Certification Authorities		ActiveX Control Microsoft Cor	car sindities (cotal computer)	Remove	
Trusted People		Certificates Microsoft Cor		Move Up	
Control Adulter Induction Issues     Preview Build Roots     Preview Build Roots     Smart Card Trusted Roots     Trusted Devices     Windows Live ID Token Issuer		Component Services Microsoft Cor     Component Services Microsoft Cor     Computer Manager     Microsoft Cor     Device Manager     Microsoft Cor     Disk Managerent Microsoft Cor     Disk Managerent Microsoft Cor     Distreprise PKI Microsoft Cor     Distreprise PKI Microsoft Cor     Distreprise PKI Microsoft Cor     Distreprise PKI Microsoft Cor	Component Services Microsoft Cor	Add >	Move Down
		Group Policy Object Microsoft Cor		Advanced	
		Description: Allows you to configure certification authority proper	ties and to manage certificates issued by this CA.	OK Cancel	

#### Choose Local Computer

🚰 Console1 - [Console Root\Certificates (Local C	mputer)\Personal\Certificates]	
🚡 File Action View Favorites Window	elp	
🗢 🔿 🙍 🗊 📋 🙆 💀 😰 📷		
Console Reoot Console Certificates (Local Computer) Cartificates (Local Computer) Cartificates C	Issued To Add on Research Cases line Certification Authority Select the computer you want this snap-in to manage. This snap-in will always manage:  Ducal computer: the computer this console is running on) Another computer: the console is running on) Another computer: Browse. Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.  Reack Finish Cancel Help C	Ciendu Mana



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

console Root       Issued To       Issued To       Finish Land A.       Finish Data       Finish Data	🔶 📶 📋 🖸 🔂 🖬		
Q Certificates (Local Computer)       Add or Remove Snap-ins       ×         Personal       Certificates       ×         Certificates (Local Computer)       Voi can select anap-ins for this concole from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins; you can configure which extensions are enabled.       ×         Trusted Root Certification Authorities       Selected snap-ins:       Selected snap-ins:         Selected Certificates       Snap-in       Vendor       Enterprise Reveal         Windows Live ID Token Issuer       Certificate Templates       Microsoft Cor       Certificates         Solution       Selected snap-ins:       Certificates       More Up         Move Down       Certificates       More Down         Move Down       Certificate Remose Tor       Microsoft Cor         Certificate Remote Desktop       Computer Managem       Microsoft Cor         Solution       Computer Managem       Microsoft Cor       Microsoft Cor         Solution       Certificate Remote Desktop       Computer Managem       Add >         Windows Live ID Token Issuer       Perview Recosoft Cor       Fielder       Microsoft Cor       Advanced to manufactor         Vindows Live ID Token Issuer       Description:       Certificate Reveere       Microsoft Cor       <	Console Root	Issued To	institute Data Internalizat Durana Criteriallu Manua
Group Policy Object Microsoft Cor  Advanced Description:	Certificates (Local Computer)  Personal  Certificates  Trusted Root Certification Authorities  Trusted Publishers  Trusted Publishers  Trusted Certificates  Trusted Certification Authorities  Trusted People  Cirent Authentication Issuers  Preview Build Roots  Remote Desktop  Smart Card Trusted Roots  Trusted Devices  Windows Live ID Token Issuer	Add or Remove Snap-ins You can select snap-ins for this console from those available on your comp extensible snap-ins, you can configure which extensions are enabled. Available snap-ins: Snap-in Vendor ActiveX Control Microsoft Cor Computer Managem. Microsoft Cor	× puter and configure the selected set of snap-ins. For ed anap-ins: onsole Root ↓ Certificates (Jocal Computer) ↓ Certificates (Jocal Computer) ↓ Certification Authority (Local) ↓ Move Up ↓ Move Down
Allows you to configure certification authority properties and to manage certificates issued by this CA.		Project Territory Policy Object Microsoft Cor      Description:     Alows you to configure certification authority properties and to manage	Advanced

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

🚡 Console1 - [Console Root\Certification Autho	rity (Local)]		
🔚 File Action View Favorites Window	Help		
🗢 🔿 🙋 🖬 🔒 🛛 🖬 🕨 🔳			
Console Root  Certificates (Local Computer)  Personal  Certificates  Cer	Name	Description Certification Authority	
<ul> <li>Certification Authority (Local)</li> </ul>			
Sirhowy NPS guide eduroan All T	ïasks → S	tart Service	
Ssued Certificates New	Window from Here S	top Service	
Pending Requests Failed Requests	esh S	ubmit new request	
Prop	perties B	lack up CA lestore CA	
Help	R	lenew CA Certificate	
<	>		



Select your existing certificate request file (.req file)

Open Request File							×
← → · ↑	] → This	PC > Documents			✓ Ö Search Doo	uments	P
Organize 🔻 🛛 N	ew folder					== -	?
1 Outstanson		Name	Date modified	Туре	Size		
Desktop	*	sirhowy-nps-guide.req	08/03/2018 17:11	REQ File	2 KB		
Downloads	*						
Documents	*						
Pictures	*						
💻 This PC							
💣 Network							
	File nam	ne: sirhowy-nps-guide.reg			✓ Request F	les (*.req; *.txt; *.cr	nc 🗸
					Open	Cance	el
15	suea Certi	ricates					
🚞 P.	ending Rec	quests					
	illeu Kequ	50					

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

Console1 - [Console Root\Certification Author	ty (Local)\Sirho	wy NPS guide edure	oam service\Pending Requ	iests]				
File Action View Favorites Window	Help							
🗢 🔿 📶 🖻 🗟 🗾								
Console Root	Request ID	Binary Request	Request Status Code	Request Dispositio	n Message	Request Submission Date	Requester Name	Requ
<ul> <li>Certificates (Local Computer)</li> </ul>	2	BEGIN NE	The operation compl	Taken Under Subr	nission	08/03/2018 17:12	SIRHOW/Viagland	
V Personal					All Tasks	S > View Attribu	utes/Extensions	
Certificates Trusted Root Certification Authorities					Refresh	Export Bina	y Data	
> Contempose Trust						Issue		
> Intermediate Certification Authorities					Help	Depy		
> iii Trusted Publishers						beny		
> iii Untrusted Certificates								
> Third-Party Root Certification Authoritie	5							
> 📔 Trusted People								
Client Authentication Issuers								
Preview Build Roots     Preview Decktop								
Smart Card Trusted Roots								
> Trusted Devices								
> iii Windows Live ID Token Issuer								
<ul> <li>Certification Authority (Local)</li> </ul>								
🗸 🚽 Sirhowy NPS guide eduroam service								
Revoked Certificates								
Ssued Certificates								
Pending Requests								
Palled Requests								



The certificate will now appear under Issued Certificates

Console Root     Console Root     Console Root     Console Root     Personal     Certificates (Local Computer)     Personal     Certificates (Local Computer)     Trusted Root Certification Authorities     Trusted Publishers     Simant Card Trusted Roots     Trusted Devices     Windows Live ID Token Issuer     Windows Live ID Token Issuer     Sinhowy NPS guide eduroam service     Bevoked Certificates     Sishowy NPS guide eduroam service     Beud Certificates     Failed Requests     Failed Requests	Request ID	Requester Name SIRHOW/Yjagland	Binary Certificate	Certificate Template	Serial Number 1c00000020a1	Certificate Effective Date 08/03/2018 17:03	Certificate Expirat 08/03/2019 17:13

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

🚰 Console1 - [Console Root\Certification Author	ty (Local)\Sirhowy	NPS guide eduroar	n service\lssued Certi	icates]			
蘠 File Action View Favorites Window	Help						
🔶 🔿 🔁 🖬 🍳 📾							
<ul> <li>Console Root</li> <li>Console Root</li> <li>Console Root</li> <li>Certificates (Local Computer)</li> <li>Certificates (Context Computer)</li> <li>Trusted Root Certification Authorities</li> <li>Trusted Root Certification Authorities</li> <li>Trusted Publishers</li> <li>Untrusted Certification Authorities</li> <li>Trusted People</li> <li>Cleint Authenitication Issuers</li> <li>Preview Build Roots</li> <li>Remote Desktop</li> <li>Sinowy NPS guide eduroam service</li> <li>Sinowy NPS guide eduroam service</li> <li>Sinowy NPS guide eduroam service</li> <li>Pending Requests</li> <li>Failed Requests</li> </ul>	Request ID	Requester Name SIRHOWNjagland Certificat General Del This cer • Er Iss Iss Val	Binary Certificate BEGIN CERTI e c certificate Informati tificate is intended f sures the identity of a r guide.sirbowy ued to: radius-noc- guide.sirbowy ued by: sirbowy NPS id from 08/03/2018	Certificate Template	Serial Number 1c0000020a1 × e(s):	Certificate Effective Date 08/03/2018 17:03	Certificate Expiratic 08/03/2019 17:13
< >	<				ОК		>



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



This will launch the Certificate Export Wizard

🔚 Console1 - [Console Root\Certification Authorit	y (Local)\Si	rhowy NPS guide eduroan	n service\lssued Certi	ficates]			
🖀 File Action View Favorites Window H	lelp						
Console Root	Request I	D Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiratic
Certificates (Local Computer)	2	SIRH <u>OWY</u> jagland	BEGIN CERTI		1c00000020a1	08/03/2018 17:03	08/03/2019 17:13
Certificates						×	
Trusted Root Certification Authorities		<ul> <li>— — — — — — — — — — — — — — — — — — —</li></ul>					
> Enterprise Trust		Certificate Expor	t Wizard				
Intermediate Certification Authorities							
> Trusted Publishers							
> Intrusted Certificates		Welcome t	o the Certificat	e Export Wizard			
> iii Third-Party Root Certification Authorities							
> 🛄 Trusted People							
> Client Authentication Issuers		This wizard helps	you copy certificates,	ertificate trust lists and cer	tificate revocation		
> Preview Build Roots		lists from a certifi	cate store to your disk.				
> Remote Desktop							
Smart Card Trusted Roots		A certificate, white and contains info	ch is issued by a certific rmation used to protect	ation authority, is a confirm t data or to establish secure	ation of your identity		
Windows Live ID Token Issuer		connections. A ce	ertificate store is the sy	stem area where certificate	s are kept.		
Certification Authority (Local)							
Sirhowy NPS guide edurgam service		To contract date	N				
Revoked Certificates		To continue, click	next.				
Issued Certificates							
Pending Requests							
🧮 Failed Requests							
< >	<				Next Car	ncel	>
	· ·						,



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



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

Console1 - [Console Root\Certification Author File Action View Favorites Window	ty (Local)\Sirhowy NPS <b>Help</b>	guide eduroam service\lssued Certif	icates]					
Console Root	Request ID Requ	ester Name Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	e Certificate Expiratio	Actions	
<ul> <li>✓ Certificates (Local Computer)</li> <li>✓ Personal</li> <li>✓ Certificates</li> <li>&gt; Trusted Root Certification Authorities</li> <li>&gt; Enterprise Trust</li> <li>&gt; Intermediate Certification Authorities</li> <li>&gt; Untrusted Publishers</li> <li>&gt; Untrusted Publishers</li> <li>&gt; Trusted Pople</li> <li>&gt; Certificates</li> <li>&gt; Trusted Pople</li> <li>&gt; Client Authentication Issuers</li> <li>&gt; Preview Build Roots</li> <li>&gt; Preview Build Roots</li> <li>&gt; Preview Build Roots</li> <li>&gt; Smart Card Trusted Roots</li> <li>&gt; © Trusted Devices</li> <li>&gt; Windows Live ID Token Issuer</li> <li>✓ Gisthowy NPS guide eduroam service</li> <li>≅ Revoked Certificates</li> <li>&gt; Praing Requests</li> <li>⇒ Failed Requests</li> </ul>	2 SIRH	OWY\jaqlandBEGIN CERTI		1c00000020a1	08/03/2018 17:03	08/03/2019 17:13	Issued Certificates	
	🚡 Save As						× <sup>15</sup>	
	$\leftrightarrow \rightarrow \cdot \uparrow$	> This PC > Documents			~ Ū	Search Documents	م	
	Organize 🔻 Ne	w folder						
	<ul> <li>Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Pictures</li> <li>This PC</li> <li>Network</li> </ul>	Name * *		Date modified	Type 5	ize		
	File name:	sirhowy-nps-guide.cer					~	
	Save as type:	DER Encoded Binary X.509 (*.cer)					~	
	∧ Hide Folders					Save	Cancel	
x >	<			Next Can	cel	>		

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

🚰 Console1 - [Console Root\Certification Authorit	ty (Local)\	Sirhov	y NPS guide eduroar	n service\lssued Certi	ficates]				
File Action View Favorites Window F	Help								
🗢 🔿 🔁 🖬 🙆 🖬									
Console Root	Request	t ID	Requester Name	Binary Certificate	Certificate Templat	e Serial Number	Certificate Effective Date	Certificate Expiratio	Actions
Certificates (Local Computer)     Personal	2	-	SIRHOWY\jagland	BEGIN CERTI		1c00000020a1	08/03/2018 17:03	08/03/2019 17:13	Issued Certificates
Certificates							×		More Actions
> Trusted Root Certification Authorities		←	F Certificate Expor	t Wizard					2
> Interprise rust > Intermediate Certification Authorities									More Actions
> 🧰 Trusted Publishers									
> Untrusted Certificates > Third-Party Root Certification Authorities			Completin	g the Certificat	e Export Wizar	d			
> 📔 Trusted People									
Client Authentication Issuers     Preview Build Boots			You have success	sfully completed the Cer	tificate Export wizard.				
> 🧰 Remote Desktop			You have specifie	d the Certificate Exp	ort Wizard 🛛 🗙				
Smart Card Trusted Roots			File Name		r	nd\Documents\sirhowy-			
<ul> <li>Windows Live ID Token Issuer</li> </ul>			Export Keys Include all certif	The export wa	as successful.				
Certification Authority (Local)			File Format		E	Binary X.509 (*.cer)			
<ul> <li>Revoked Certificates</li> </ul>					ОК				
Issued Certificates									
Failed Requests			<			>			
						Finish Can	cel		
< >>	<					Cum		>	

#### 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**....

• 🖤   📶 🔲   🖬 🔛 🔛						
Console Root  Console Root  Certificates (Local Computer)  Personal  Certificates  Certificates  Certificates  Certification Authorities  Intermediate Certification Authorities	Issued To ^ Call Sirhowy NPS guide eduroam se	Issued By Sirhowy NPS guide eduroam servi	Expiration Date 08/03/2068	Intended Purposes <all></all>	Friendly Name <none></none>	Statu
Induced Publishes     Induced Certificates     Third-Party Root Certification Authorities     Trusted People     Client Authentication Issuers     Preview Build Roots     Remote Desktop     Remote Desktop		All Tasks Refresh Export List View	Requ     Impo     Adva	est New Certificate rt nced Operations	>	
Sinar Carlo Rocker Rocker     Sinar Carlo Rocker     Windows Live ID Token Issuer     Certification Authority (Loca)     Sindow INPS guide eduroam service     Revoked Certificates     Issued Certificates     Issued Certificates     Sinar Carlo Requests     Failed Requests		Arrange Icons Line up Icons Help	>			

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.

A Network Policy Server		
File Antine View Hole		
File Action View Help		
🗢 🔿 🞽 🔟 🖬		
<ul> <li>NPS (Local)</li> <li>ADDUS Clients and Sen</li> <li>Policies</li> <li>Accounting</li> <li>Templates Management</li> <li>Shared Secrets</li> <li>RADIUS Clients</li> <li>RADIUS Clients</li> </ul>	New RADIUS Shared Secret Template         X           Shared Secret         Template name: [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	reuse whe
IP Filters	Secret entered here. Shared secrets are case-sensitive.     Manual      Generate     Shared secret:     Confirm shared secret:	
	Confirm shared secret:	
	OK Cancel	

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

🥪 Network Policy Server



### 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'



w RADIUS Client			×
ettings Advanced			
Enable this RADIUS cli	ent		
Select an existing temp	late:		
			$\sim$
Name and Address			
Friendly name:			
roaming0			
Address (IP or DNS):			
roaming0.ja.net			Verify
Shared Secret			
Select an existing Shared	Secrets template:		
froaming0			~
To manually type a share secret, click Generate. Y secret entered here. Sha Manual Shared secret:	d secret, click Manual, ou must configure the R red secrets are case-ser Generate	Fo automatically ger ADIUS client with th Isitive.	ierate a shared ie same shared
•••••			
Confirm shared secret:			
•••••			
		04	Capaci
		UK	Cancel

Nb.Repeat this procedure to add roaming1 and roaming2.

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

📔 RADIUS Cli	ents and Servers
🚪 RADIUS	Clients
🗄 Rem	New
Policies	Defearb
Necount 📲	Kerresn
🜉 Templat	Help
Charles Charles	•

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

ireless controller Properties	×
Settings Advanced	
Enable this RADIUS client	
Select an existing template:	
$\sim$	
Name and Address	
Friendly name:	
wreless 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.	
•••••	
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**.

New Remote RADIUS Serv	er Group		×
Group name: NRPS RADIUS Servers:			
RADIUS Server	Priority	Weight	Add Edit Remove
		0	K Cancel

In Server enter roaming0.ja.net then click on the Authentication/Accounting tab.



Address       Authentication/Accounting       Load Balancing         Select an existing Remote RADIUS Servers template:       None       ✓         None       ✓         Type the name or IP address of the RADIUS server you want to add.	Add RAD	IUS Server				>
Select an existing Remote RADIUS Servers template: None V Type the name or IP address of the RADIUS server you want to add.	Address	Authentication/Accounting	Load Balancing			
None $$\checkmark$$ Type the name or IP address of the RADIUS server you want to add.	Select	an existing Remote RADIUS S	Servers template:			
Type the name or IP address of the RADIUS server you want to add.	None					$\sim$
Server:	Type th Server	he name or IP address of the F	ADIUS server you	u want to add.		
roaming0.ja.net Verify	roamin	ng0.ja.net			Verify	

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

Add RAD	IUS Server		×
Address	Authentication/Accounting	Load Balanci	ng
Authent	tication port:		1812
Select a	an existing Shared Secrets terr	nplate:	
roaming	g0	-	~
Shared	secret:		*******
Confirm	shared secret:		*******
	uest must contain the messag	e authenticator	attribute
Accou	unting		
Acco	unting port:		1813
V	se the same shared secret for	authentication	and accounting.
s	elect an existing Shared Secre	ets template:	
r	roaming0		$\sim$
s	hared secret:		*******
C	onfirm shared secret:		******
M	orward network access server	start and stop	notifications to this server
			OK Cancel



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 •

Add RAD	IUS Server					×
Address	Authentication/Acc	ounting	Load Balancing			
The prio 1.	rity of ranking indicate	es the stat	tus of a server. A	primary ser	ver has a priorit	y of
Weight i servers f	is used to calculate h that have the same p	ow often r riority.	request are sent to	o a specifio	server in a gro	up of
Pri	ority:	1	Weight:		33	
Advan	iced settings					
Numb	per of seconds withou dered dropped:	t respons	e before request is	5	30	
Maxir identi	num number of dropp fied as unavailable:	ed reques	ts before server is	;	5	
Numb as un	per of seconds betwe available:	en reques	ts when server is	identified	30	

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

New Remote RAI	New Remote RADIUS Server Group				×
Group name:					_
NRPS					
RADIUS Servers:					
RADIUS Server	Priority	Weight			Add
roaming0.ja.net	1	33			Edit
roaming1.ja.net	1	33			
roaming2.ja.net	1	33			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	ion Request Policy X
	<b>Specify Connection Request Policy Name and Connection Type</b> You can specify a name for your connection request policy and the type of connections to which the policy is applie
Policy name:	c.
authenticate re	equests from NRPS locally
Network conne Select the type type or Vendor select Unspeci	ection method e of network access server that sends the connection request to NPS. You can select either the network access server r specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, ified.
<ul> <li>Type of net</li> <li>Unspecifie</li> <li>Vendor spe</li> </ul>	twork access server: ed  v ecific:
10	

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

Select condition	×
Select a condition, and then click Add.	
RADIUS Client Properties	^
Calling Station ID The Calling Station ID condition specifies the network access server telephone number dialed by the access client.	
Client Friendly Name The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.	
Client IPv4 Address The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.	
Client IPv6 Address The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the connection request to NPS.	
Client Vendor The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connection requests	v
Add Cancel	

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

Select condition		×
Sciece condition		
Select a condition, and the	en click Add.	
RADIUS Client Propertie	35	^
Calling Station The Calling Stati	Client Friendly Name X access client.	
Client Friendly The Client Friend NPS.	Specify the friendly name of the RADIUS client. You can use pattern matching ection request to syntax.	
Client IPv4 Add The Client IP Add to NPS.	roaming.*	
Client IPv6 Add The Client IPv6 A request to NPS.	OK Cancel = connection	
Client Vendor The Client Vendor	or Condition specifies the name of the vendor of the RADIUS client that sends connection requests	~
	Add Canc	el



#### For Authentication select Authenticate requests on this server and click Next.

New Connectio	on 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 con Settings:	nditions match the conn	ection request, these settings are applied.				
Forwarding Request	Connection cation	Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.				
Account	ing	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 Connect	ion Request Policy				×
	Configure Set NPS applies settings matched.	ettings s to the connect	tion request if all of th	e connection request p	olicy conditions for the policy are
Configure the s If conditions m	settings for this network atch the connection rec	policy. quest and the po	licy grants access, set	ings are applied.	
Specify a I Attribut RADIUS A Standa Vendor	Realm Name e thributes rd Specific	Select the a the order the Attribute: Rules: Find	tributes to which the for ey appear in the list. Called-Station-Id	Nowing rules will be appli	ed. Rules are processed in Add Edit Remove Move Up Move Down
			Pre	evious 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 Connect	tion Request Policy	×
	<b>Specify Authentication Methods</b> Configure one or more authentication methods required for the connection request to match this policy. For E authentication, you must configure an EAP type.	ΑP
✓ Override r	network policy authentication settings	
These auther	intication settings are used rather than the constraints and authentication settings in network policy.	
EAP types a	are negotiated between NPS and the client in the order in which they are listed.	
EAP Type:	s:	
Microsoft:	Protected EAP (PEAP) Move Up Move Down	
Add	Edit Remove	
Less secu	rre authentication methods: 1t Encypted Authentication version 2 (MS-CHAP-v2)	
User	can change password after it has expired	
Microsoft	t Encrypted Authentication (MS-CHAP)	
User	can change password after it has expired	
Encrypte	ed authentication (CHAP)	
	pted authentication (PAP, SPAP)	
Allow clie	ents to connect without negotiating an authentication method.	
	Previous Next Finish Cancel	

#### Click **Finish** on the final screen.

iew Connection Request Policy				
<b>i</b> (1	ompleting Connection Request Policy Wizard			
You have successf authenticate req Policy conditions	ully created the following connection request policy: uests from NRPS locally s:			
Condition	Value			
Client Friendly Nan	ne roaming.*			
Policy settings:				
Condition	Value			
Authentication Pro	vider Local Computer			
To close this wizard	J, click Finish.			
	Previous Next Finish Cano	el		



### 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

 $\times$ 



#### 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 local	users
Network connection	on method
Select the type of type or Vendor spe select Unspecified	network access server that sends the connection request to NPS. You can select either the network access server ecific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point,
Type of network	k access server:
Unspecified	$\checkmark$
O Vendor specific	x
10 🜲	



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 <code>@realm\$</code>, where realm is your organization's realm e.g. camford.ac.uk, ensure to put a backslash before each full-stop <code>@camford.acl.uk\$</code> then click **OK**.

User Name	×
Specify the user name of the access request mess matching syntax.	age. You can use pattern
@sirhowy\.dev\.ukfederation\.org\.uk\$	
E	OK Cancel

#### See using the pattern matching syntax in NPS



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

New Connect	ion Request Pol	icy				×
	Specify C Specify the co minimum of or	Conditions nditions that determine who ne condition is required.	ether this connection re	quest policy is eval	uated for a co	nnection request. A
Conditions:						
Condition	ı	Value				
📇 User Na	me	@sirhowy\.dev\.ukfederat	tion\.org\.uk\$			
Condition de	escription:					
				Add	Edit	Remove
			Previous	Next	Finish	Cancel

New Connection	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 con	nditions match the conn	ection request, these settings are applied.				
Account	) Connection	Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication. <ul> <li>Authenticate requests on this server</li> <li>Forward requests to the following remote RADIUS server group for authentication:</li> <li>NRPS</li> <li>Accept users without validating credentials</li> </ul>				
		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 Connecti	on Request Policy	×
	Specify Authentication Methods	
	Configure one or more authentication methods required for the connection request to ma authentication, you must configure an EAP type.	atch this policy. For EAP
✓ Override n	network policy authentication settings	
These auther	tication settings are used rather than the constraints and authentication settings in network policy	y.
EAP types an	e negotiated between NPS and the client in the order in which they are listed.	
EAP Types	e	
Microsoft: F	Protected EAP (PEAP)	Move Up
		Move Down
Add	Edit Remove	
Less secur	e authentication methods:	
Microsoft	Encrypted Authentication version 2 (MS-CHAP-v2)	
User c	an change password after it has expired	
	Encrypted Autoentication (MS-CHAP)	
	an change password altern has expired	
	ted authentication (PAP, SPAP)	
Allow clier	nts to connect without negotiating an authentication method.	
	Previous Next Fi	nish Cancel

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.

Edit Protected EAP Prop	erties	×			
Select the certificate the server should use to prove its identity to the dient. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.					
Certificate issued to:	radius-nps-guide.sirhowy.dev.ukfedera	tion.org.uk \vee			
Friendly name:	radius-nps-guide.sirhowy.dev.ukfederat	ion.org.ul			
Issuer:	Sirhowy NPS guide eduroam service				
Expiration date:	on date: 08/03/2019 17:13:21				
Enable Fast Reconnect     Disconnect Cryptobinding     Eap Types					
Secured password (EAP-I	MSCHAP v2)	Move Up			
Move Down					
Add Edit	t Remove OK	Cancel			



#### ${\sf Click} \ {\bf Next} \ {\rm on} \ {\rm the} \ {\bf Configure} \ {\bf Settings} \ {\rm screen}.$

New Connection	on 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 s If conditions ma	ettings for this network p atch the connection requ	olicy. Jest and the po	olicy grants access, se	ttings are applied.		
Specify a R	Realm Name	Select the a the order the	attributes to which the ey appear in the list.	following rules will be ap	plied. Rules are	processed in
Standar	d	Attribute:	Called-Station-Id		$\sim$	
Vendor	Specific	Rules:				
		Find		Replace With		Add Edit Remove Move Up Move Down
			P	revious Next	Finish	Cancel

#### Click **Finish** on the final screen.

New Connection Reque	st Policy	$\times$
Comp	pleting Connection Request Policy Wizard	
You have successfully or authenticate local us Policy conditions:	eated the following connection request policy: <b>ers</b>	
Condition Value	.dev\ukfederation\org\uk\$	
Condition Authentication Provider	Value Local Computer	
To close this wizard, clic	c Finish.	

 $\times$ 

### Jisc

# 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  $\sim$ O Vendor specific: 10 \* Previous Next Finish Cancel

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

Jisc

>
^
,

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

User Name	$\times$
Specify the user name of the access request message. You can use pattem matching syntax.	
@{1}[-a-zA-Z0-9_]+(\.[-a-zA-Z0-9_]+)+\$	
OK Cancel	

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 Con The connection req remote RADIUS se	nection Request Forwarding uest can be authenticated by the local server or it can be forwarded to RADIUS servers in a rver group.	
If the policy conditions match the con	nnection 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         Accept users without validating credentials	
lew Connection Request Policy	Previous Next Finish Cancel	>
Completing (	Connection Request Policy Wizard	
You have successfully created the foll proxy to eduroam	owing connection request policy:	
Policy conditions: Condition Value User Name @{1]{-a-zA-Z0-9_]+(\_[-a	9-2A-Z0-9_]+)+\$	
Policy settings:		
Condition Value Authentication Provider Forw Authentication Provider Name NRP	e arding Request S	
To close this wizard, click Finish.		
	Previous Next Finish Can	cel



### 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			
suthenticate 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.

Connection Request Policies				
Connection request policies allow you to forwarded to remote RADIUS servers.	o designate	e whether connectio	on requests are processed locally or	
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	
Use Windows authentication for all users	Enabled	999999	Unspecified	
Conditions - If the Condition Day and time to Condition Condition	y tion reque ocal mach	est policy 'Use Win ine?	imes authentication for all	
			OK Cancel	
Settings - Then the following settings are appli	ed:			_
Setting Value				
<				>
1				

### 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.

New Network	Policy	×
	Specify Network Policy Name and Connection Type	
	You can specify a name for your network policy and the type of connections to which the policy is applied.	
Policy name	e:	
local authentio	ication	
select Unspec	in specific, but neutren is required. In your network access server is an ouz. IX authenticating switch of wireless access profiled.	JITIL,
Unspecifie	ied V	
O Vendor spe	eofic:	
10		
	Previous Next Finish Cancel	

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

Select o	condition	>
Select a	a condition, and then click Add.	
Conne	ection Properties	^
Ņ	Access Client IPv4 Address The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.	l
Ņ	Access Client IPv6 Address The Access Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access from the RADIUS client.	ł
ß	Authentication Type The Authentication Type condition specifies the authentication methods required to match this policy.	
7	Allowed EAP Types The Allowed EAP Types condition specifies the EAP types required for client computer authentication method configuration to match this policy. Use of this condition requires that EAP is also configured in connection request policy.	
	Framed Protocol	~
	Add Cance	ł

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

Select condition		_	$\times$
Select a condition, and the	Authentication Method X		
Connection Properties	Specify the authentication methods required to match this policy.		^
from the RADIUS	CHAP EAP	questing access	
The Access Client I The Access Clien from the RADIUS	Extension     MS-CHAP v1     MS-CHAP v1     MS-CHAP v1	questing access	
Authentication The Authenticatic	MS-CHAP v2 MS-CHAP v2 CPW	ı.	
Allowed EAP Ty The Allowed EAP configuration to n policy.	☐ PEAP ☐ Unauthenticated	n method ection request	
Framed Protoco	OK Cancel		~
L		Add Cancel	

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

New Network	Policy					×
	Specify C Specify the cor of one condition	<b>Conditions</b> nditions that determine wheth on is required.	er this network polic	y is evaluated for	a connection red	quest. A minimum
Conditions:						
Condition	ı	Value				
Authentio	cation Type	EAP OR PEAP				
Condition desc The Authentica	ription: ation Type conditi	on specifies the authentication r	nethods required to m	atch this policy. Add	Edit	Remove
			Previous	Next	Finish	Cancel
New Network	Policy					×
	Specify A	ccess Permission				

	Configure whether you want to grant policy.	etwork access or deny network access if the connect	tion request matches this
<ul> <li>Access gran</li> <li>Grant acces</li> </ul>	ited s if client connection attempts match the	conditions of this policy.	
<ul> <li>Access deni</li> <li>Deny access</li> </ul>	ied s if client connection attempts match the	onditions of this policy.	
Access is de Grant or den	stermined by User Dial-in properties (which	overide NPS policy) es if client connection attempts match the conditions of t	his policy.
		Previous Next Finis	h Cancel



On the Configure Authentication Methods page click Add...

New Network	Policy	$\times$
	<b>Configure Authentication Methods</b> Configure one or more authentication methods required for the connection request to match this policy. For E authentication, you must configure an EAP type.	AP
EAP types are n EAP Types:	negotiated between NPS and the client in the order in which they are listed.	
Add Less secure Microsoft Er User can User can Encrypted a Unencrypted Allow clients	Add EAP Authentication methods: Microsoft: Smart Card or other certificate Microsoft: Protected EAP (PEAP) Microsoft: Secured password (EAP-MSCHAP v2) Microsoft: Secured password (EAP-MSCHAP v2) OK Cancel authentication (CHAP) ed authentication (CHAP) ed authentication (CHAP) ts to connect without negotiating an authentication method.	
	Previous Next Finish Cancel	

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.

Edit Protected EAP Prope	arties	×		
Select the certificate the s A certificate that is config Policy will override this cer	server should use to prove its identity to the client. ured for Protected EAP in Connection Request tificate.			
Certificate issued to:	radius-nps-guide.sirhowy.dev.ukfederation.org.uk	$\sim$		
Friendly name:	radius-nps-guide.sirhowy.dev.ukfederation.org.ul			
Issuer:	Sirhowy NPS guide eduroam service			
Expiration date: 08/03/2019 17:13:21				
Enable Fast Reconnect Disconnect Clients with Eap Types	out Cryptobinding			
Secured password (EAP-N	ISCHAP v2) Move Up			
	Move Dow	n		
Add Edit	Remove OK Cancel			

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



New Network	Policy	×
	<b>Configure Authentication Methods</b> Configure one or more authentication methods required for t authentication, you must configure an EAP type.	he connection request to match this policy. For EAP
EAP types are n EAP Types:	negotiated between NPS and the client in the order in which they ar	e listed.
Microsoft: Prot	Edit Remove	ove Up ve Down
Less secure Microsoft Er User can Microsoft Er User can Encrypted a Unencrypter Allow clients	authentication methods: ncrypted Authentication version 2 (MS-CHAP-v2) n change password after it has expired ncrypted Authentication (MS-CHAP) n change password after it has expired authentication (CHAP) id authentication (PAP, SPAP) s to connect without negotiating an authentication method.	
	Previou	s 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.

lew Network Policy		×
Configure S NPS applies settin matched.	Settings ngs to the connection	n request if all of the network policy conditions and constraints for the policy a
Configure the settings for this netwo If conditions and constraints match	rk policy. the connection reque	est and the policy grants access, settings are applied.
RADIUS Attributes Standard Vendor Specific	To send addition then click Edit. your RADIUS c	nal attributes to RADIUS clients, select a RADIUS standard attribute, and If you do not configure an attribute, it is not sent to RADIUS clients. See slient documentation for required attributes.
Routing and Remote Access	Attributes:	
Would fink and     Bandwidth Allocation     Protocol (BAP)     IP Filters     Encryption     IP Settings	Name	Value
	Add	Edit_ Remove
		Previous Next Finish Cancel



New Network Policy	×
Configure NPS applies set matched.	Settings ings to the connection request if all of the network policy conditions and constraints for the policy ar
Configure the settings for this net If conditions and constraints matc	rork policy. the connection request and the policy grants access, settings are applied.
RADIUS Attributes         Image: Standard         Image: Vendor Specific         Routing and Remote         Access         Image: Bandwidth Allocation         Protocol (BAP)         Image: IP Filters         Image: Encryption         Image: 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 encryptions 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.         If 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 X	
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches thi policy.	S
<ul> <li>Access gra Grant acces</li> <li>Access de Deny acce</li> <li>Access is o Grant or de</li> </ul>	anted uss if client connection attempts match the conditions of this policy. nied uss if client connection attempts match the conditions of this policy. determined by User Dial-in properties (which override NPS policy) my access according to user dial-in properties if client connection attempts match the conditions of this policy.	
	Previous Next Finish Cancel	

**Jisc** 



Then click Finish on the Completing New Network Policy page.

ew Network Po	licy		
	Completing Nev	w Network Policy	
You have succe <b>neh</b>	ssfully created the followir	ng network policy:	
olicy conditio	ons:		
Condition	Value		
Allowed EAP Ty	pes Microsoft: Protected	d EAP (PEAP)-Microsoft: Smart Card or other certificate OR Microsoft: Protected EAP	(PE
Policy settings	r.	1/ek-e	
Policy settings Condition	:	Value	
Policy settings Condition Authentication I Access Permiss	:: Method	Value EAP Grant Access	
Policy settings Condition Authentication I Access Pemiss Ignore User Dia	: Method ion	Value EAP Grant Access False	
Policy settings Condition Authentication I Access Permiss Ignore User Dia Extensible Auth	: Method ion I-In Properties entication Protocol Metho	Value EAP Grant Access False od Microsoft: Protected EAP (PEAP)	
Policy settings Condition Authentication I Access Permiss Ignore User Dia Extensible Auth To close this wizz	: Method ion I-In Properties entication Protocol Metho ard, click Finish.	Value EAP Grant Access False ad Microsoft: Protected EAP (PEAP)	
Policy settings Condition Authentication I Access Permiss Ignore User Dia Extensible Auth	: Wethod ion I-In Properties entication Protocol Metho ard, click Finish.	Value EAP Grant Access False od Microsoft: Protected EAP (PEAP)	

**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.

	entication P	roperties							
verview	Conditions	Constraints	Settings						
Policy na	me:	local a	uthentication						
Policy S If enab	State led, NPS eva	luates this pol	icy while per	forming authoriza	ation. If disabled,	NPS does not e	evaluate this poli	cy.	
🗹 Poli	cy enabled								
Access If cond access	Permission ditions and co s. <u>What is ac</u>	onstraints of t	he network sion?	policy match the	connection req	uest, the policy	r can either gran	t access or deny	
• Gran	nt access. Gri	ant access if t	he connectio	on request match	es this policy.				
ODen	y access. De	ny access if th	ie connectio	n request matche	es this policy.				
🗹 Igno	re user accoi	unt dial-in prop	erties.						
If the auth	e connection orization with	request match network polic	es the cond y only; do no	itions and constra t evaluate the di	aints of this netwo al-in properties of	ork policy and the user accounts	ne policy grants a	access, perform	
Network Select or Vend select	k connection the type of n dor specific, t Unspecified.	method etwork access out neither is re	server that equired. If y	sends the conne our network acce	ection request to l ess server is an 8	NPS. You can s 02.1X authentic	elect either the r cating switch or v	network access se vireless access po	rver type int,
Networ Select or Veno select	k connection the type of n dor specific, t Unspecified. e of network	method etwork access out neither is re access serve	s server that equired. If yo r:	sends the conne our network acce	ection request to a server is an 8	NPS. You can s 02.1X authentic	elect either the r ating switch or v	ietwork access se vireless access po	rver type int,
Networ Select or Veno select I Typ Ur O Ven	k connection the type of n dor specific, t Unspecified. e of network nspecified ndor specific:	method etwork access out neither is re access serve	s server that equired. If ye	sends the conne our network acce	ection request to ess server is an 8	NPS. You can t 02.1X authentic	elect either the r ating switch or v	ietwork access se vireless access po	river type int,
Networ Select or Veno select I Ur Ur Ur Veno 10	k connection dor specific, t Unspecified. e of network nspecified ador specific:	method etwork access out neither is n access serve	e server that equired. If y	sends the conne our network acce	ction request to ess server is an 8	NPS. You can e 02.1X authentic	velect either the r	ietwork access se vireless access po	erver type int,

Network Policies				
Network policies allow you to designate who is authorized under which they can or cannot connect.	to connect t	to the network and t	he circumstance	es
Policy Name	Status	Processing Order	Access Type	S.
ocal 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

🥪 N	🥪 Network Policy Server – 🗆 🗙						$\times$
File	Action	View Help					
<pre> </pre>		?					
> 10 > 10 > 10 > 10 > 10	NPS (Local) > □ R > □ P ■ A > ■ T	Import Configuration Export Configuration Start NPS Service Ston NPS Service	NDC (I D on in	Server (NPS) allows you to create and enforce organization-wide netw set authentication, and connection request authorization.	ork acce	ss policies	for
		Register server in Ad	ctive Directory	uration			•
		View >		scenario from the list and then click the link below to open the scenario wizard.			
		Help		al-Up or VPN Connections	$\sim$		
			RADIUS server When you configure allow NPS to authent RADIUS clients).	rver for Dial-Up or VPN Connections figure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that uthenticate and authorize connections from Dial-Up or VPN network access servers (also called s).			
	Configure VPN o			or Dial-Up 🕒 Learn more			
Advanced Config				guration			•
<		>	Templates Conf	iguration			•
Import	NPS co	nfiguration	*				

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

Jisc



Network Policy Server

 $\times$ 

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?

ОК	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	