Microsoft NPS Configuration Guide

Updated 04/04/2023

Contents:

- **How-to videos**
- **Configuration Guide**
- **Configuration guide Addenda**
- **Windows Server 2012R2 NPS Enable Support for TLS 1.2**

How-to videos

Produced by eduroam(UK):
https://www.youtube.com/playlist?list=PLbKeiLya4JyA_6A10XKhnCzEY4eyApG4M [1]

eduroam how to guide - Certificate requests (on a standalone CA or for the Jisc Certificate Service)
eduroam how to guide - Certificate requests (on an enterprise CA)
eduroam how to guide - Installing NPS
eduroam how to guide - Templates and configuring NPS (Part I)
eduroam how to guide - Configuring NPS (Part II)
eduroam how to guide - Configuring NPS for multiple SSIDs

How-to Configuration Guide Document

Produced by eduroam(UK): contains screenshots specifically for eduroam(UK)

>>> eduroam(UK) Microsoft NPS Configuration Guide [2] <<< Note addenda detailed in section below

(The above contains Windows Server 2016 screenshots and incorporates relevant material from the Geant / UNINETT (Norway) document. At the time of production it presented a definitive all-in-one guide to deploying NPS for eduroam - but is now in need of the addition of some supplementaty material which is available in sister documents on this website).

Configuration guide ADDENDA

1) Ref. Section 17 Visitor Connection Policy pattern matching regex expression for forwarding authentication requests to NRPS - please see item in section 5 of:
https://community.jisc.ac.uk/library/janet-services-documentation/faqs-e... [3]

For an organisation with a realm ending in .ac.uk the following regex is recommended - to be used in the Connection Request Policy for eduroam Visitors ('proxy to eduroam') in the Condition: User Name box. It will result in auth requests with usernames that contain common non-eduroam realms not being forwarded to the NRPS:

```
@{1}(?!((.*\.(ax\.edu|ac\.edu|ax\.uk$|sc\.uk$|au\.uk$|ac\.ik$|ac\.u$|ac\.k$|ac\.ukj$|local))|((myabc|gmail|g
0-9a-zA-Z\.]+\.[-0-9a-zA-Z\.]+))$
```

2) IMPORTANT Advisory - only for organisations using Windows Server Certification Authority to generate the server certificate for the NPS ORPS.

December 2021: With the introduction of Android 12 it has come to light that the implementation of the X509v3 Extension: Basic Constraints in Windows Certification Authority appears to contain a bug which results in certificate validation (and hence authentication) failure with Android 12 when the technically accurate recommendations set out in https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [4] are strictly followed.

If you have created the CSR for your server certificate with BasicConstraints: CA:FALSE *critical* the pathlen parameter on the certificate will be zero. This will cause authentications with Android 12 to fail. You can test your certificate through the 'Check realm reachability' test on CAT in your Profile panel. Static connectivity test; Show server certificate details; scroll down to the Extensions and check the basicConstraints result. basicConstraints: CA:FALSE,pathlen:0 indicates that there is a problem and you should regenerate your server certificate setting BasicConstraints:CA:FALSE to NOT be 'critical'.

When creating your server certificate CSR and following section 8 of the NPS guide p31, on the Extensions tab, under Basic Constraints you should NOT tick the 'Make the basic constraints extension critical' box (and NOT tick the 'Enable this extension' box).

Note - organisations using commercial Certification Authorities for the provision of RADIUS server certificates, should continue to set Extension: Basic Constraints CA:FALSE but there is no need to mark this as 'critical' (it was only ever noted as problem with Mac OS X 10.8 (Mountain Lion) and most CAs disregard this anyway).

3) Ref. Section 14 Accounting

Accounting packets must not be sent to the NRPS, so the tick boxes should be left blank. (Do not forward network access start and stop notifications to the NRPS.)

4) Adding an NPS Server to Multiple Domains (within an AD forest)

If you have multiple domains within your AD, for instance you are a multi-college organisation each with its own domain (and realm) but where the domains are all within a single AD forest, there are two options with regard to provision of NPS services. You can deploy separate NPS servers, each dedicated to handling authentications for the domain it is a member of. Alternatively you can enable a single NPS server (or set of servers) to handle authentications for the various realms in use within the group organisation by registering the NPS(s) in the relevant domains for whose realms you wish it to perform authenticatication duties.

See: https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-register [5]

To provide an NPS with permission to read the dial-in properties of user accounts in a domain within Active Directory that the NPS is not a member of, the NPS must first be registered that domain. Administrator or equivalent privileges are required.

Using the GUI:

- On the domain controller go to Server Manager > click on 'Tools' > click on 'Active Directory Users and Computers'. The Active Directory Users and Computers console will open.
- In the console tree, navigate to the domain where you want the NPS to read user account information and then click on the 'Users' folder.
- In the details pane, right-click 'RAS and IAS Servers' and then click 'Properties'. The RAS and IAS Servers Properties dialog box will open.
- In the 'RAS and IAS Servers Properties' dialog box, click the 'Members' tab, add each of the NPSs that you want to register in the domain and then click 'OK'.

Alternatively you can use the command line. To register an NPS in another domain using Netsh commands:

- Open Command Prompt or Windows PowerShell.
- Type the following at the command prompt: netsh nps add registeredserver domain server, and then press ENTER.

Microsoft Windows 2012R2 NPS Enable Support for TLS 1.2

Microsoft NPS Configuration - Ensure Support for TLS 1.2

Microsoft blog about supporting TLS 1.2 - TLS 1.2 support at Microsoft | Microsoft Security Blog

How to enable TLS 1.2 video - see instructions at 3:55 - 5:50 mins - https://www.youtube.com/watch?v=NR-N65cDzi0&list=PLbKeiLya4JyA_6A10XKhnC... [6]

How to enable TLS documentation - https://community.jisc.ac.uk/library/network-and-technology-service-docs... [7] for Windows Server 2012, support for TLS 1.2 was introduced via update Security Update for Windows Server 2012 (KB2977292). But to enable TLS after you install the security update, you must add a DWORD value that is named TlsVersion to the following registry subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasMan\PPP\EAP\13

The value of this registry key can be 0xC0, 0x300, 0xC00, or any OR'ed combination of these values - you should support TLS 1.0, 1.1 and importantly 1.2

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-configuration-guide

Links
[1] https://www.youtube.com/playlist?list=PLbKeiLya4JyA_6A10XKhnCzEY4eyApG4M
[2] https://support.eduroam.uk/files/eduroam(UK)%20Microsoft%20NPS%20Configuration%20Guide.pdf
[3] https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs
[4] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[5] https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-register
[6] https://www.youtube.com/watch?v=NR-

N65cDzi0&amp;list=PLbKeiLya4JyA_6A10XKhnCzEY4eyApG4M&amp;index=3
[7] https://community.jisc.ac.uk/library/network-and-technology-service-docs/tls-12-and-updated-radius-requirements