

# Re: Explanation required for using RRAS / L2TP/IPSEC and certificates for VPN connection

**Source:**

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.ras\\_routing/2004-06/0144.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.ras_routing/2004-06/0144.html)

---

**From:** Danny (*d\_codling\_at\_hotmail.com*)

**Date:** 06/09/04

Date: 9 Jun 2004 08:03:19 -0700

Thank You, the information you have provided is very beneficial, and also very thorough, thanks again for your time!

Regards

Danny

"James McIllece [MS]" <jamesmci@online.microsoft.com> wrote in message news:<Xns95029934A4537jamesmcionlinemicros@207.46.248.16>...

> *d\_codling@hotmail.com (Danny) wrote in*

> *news:b3587fea.0406070652.55e09f57@posting.google.com:*

>

>> *Hi all,*

>>

>> *I'm trying without success to configure RRAS in win2k to use*

>> *certificates for authentication. I've seen many docs around the*

>> *Internet explaining various elements of this, but I'm still stumped.*

>>

>> *What type of certificate should I request from my stand-alone CA?*

>>

>> *When I install the certificate after issuing it, where does it go?*

>>

>> *I've tried creating Server Authentication / client authentication*

>> *certificates but whenever I go into RRAS, edit profile for my policy,*

>> *select authentication I get the 798 error, no certifications for EAP.*

>>

>> *I'm sure I'm missing something so obvious here, can anyone explain*

>> *things a little more*

>>

>> *Thanks*

>>

>

> *Hi Danny --*

>

> *It is most likely that the certificates as you configured them on the CA do*

- > *not meet the minimum certificate requirements for a cert used for server*
- > *authentication. When your RRAS server has a cert that meets the minimum*
- > *requirements, it is automatically selected by RRAS/remote access policy*
- > *(RAP). (In other words, when there is a valid cert on the machine, RAP*
- > *selects that cert by default.)*
- >
- > *Certificates are kept in the "certificate store" of the machine. ("Store"*
- > *as in "storage area.") You can view the certificates (and their properties)*
- > *on the machine by opening the Microsoft Management Console (Start, Run,*
- > *type "mmc" and hit enter) and adding the certificates snap-in to the*
- > *console.*
- >
- > *There are two certificate stores on a machine -- the Current User store and*
- > *the Local Computer store. You can add both stores to the snap-in so that*
- > *you can view them from the same console (and then you can save the console*
- > *for later use). For more MMC info see*
- > *<http://www.microsoft.com/windows2000/techinfo/planning/management/mmcsteps>.*
- > *asp*
- >
- > *Some tips:*
- >
- > *The server cert must be in the Local Computer cert store. Also, when you*
- > *configure the cert templates, make sure the server cert has the server*
- > *authentication purpose in Enhanced Key Usage extensions. Do not substitute*
- > *the "All" purpose for the "Server Authentication" purpose or the cert is*
- > *invalid.*
- >
- > *If possible, use the Web enrollment tool to enroll the cert on the server.*
- >
- > *If clients are domain members, you can autoenroll client computer*
- > *certificates (but not user certs) using Group Policy. That is a little*
- > *complicated to set up, but is much easier than manually installing certs on*
- > *all clients. Clients must have the Client Authentication purpose in ECU*
- > *extensions, not the "All" purpose.*
- >
- > *Some resources that are recommended:*
- >
- > *Step-by-Step Guide to Setting up a Certification Authority*
- > *<http://www.microsoft.com/windows2000/techinfo/planning/security/casetupstep>*
- > *s.asp*
- >
- > *Step-by-Step Guide to Advanced Certificate Management*
- > *<http://www.microsoft.com/windows2000/techinfo/planning/security/advcertstep>*
- > *s.asp*
- >
- > *The following topic is from Windows Server 2003 Help, and I know you are on*
- > *W2K, but much of the information is applicable to your situation so you may*
- > *find it helpful: "Network access authentication and certificates" in*
- > *Windows Server 2003 IAS or VPN Help, or on the web at*
- > *[Re: Explanation required for using RRAS / L2TP/IPSEC and certificates for VPN connection](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-</a></i></li></ul></div><div data-bbox=)*

microsoft.public.win2000.ras\_routing: Re: Explanation required for using RRAS / L2TP/IPSEC and certificates for VPN con

- > *us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/prodd*
- > *ocs/en-us/sag\_VPN\_und15.asp.*
- >
- > *Hope that helps...*