

Re: Enabling a Certificate template

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-01/0116.html>

From: awib (awib_at_discussions.microsoft.com)

Date: 01/04/05

Date: Tue, 4 Jan 2005 03:33:02 -0800

Hi Steven,

thanks for that, after checking this am, of course I am running Server 2003 standard.

Can I just run past you again what i want to do.

I want any authorised user in the active directory to be able to log over wireless connection to the domain via an "authorised lap top", It was my intention to "pre authorise" the laptop with a certificate issued by the certifacte authority (this being the EAP-TLS bit). The authentication on the domain would require both the laptops certificate and the users domain login to be valid.

I was proposing to use Radius of course to manage the certificate authentication to the device, and allow my users to authenticate with ads over the top of that. Preferably at the point of logging on to the laptop. For the certification service to work in this way requires Server Enterprise. Can I upgrade the server to the enterprise version (given that this is for education, the cost is not significant), and will this allow me to meet my objective.

If not, can I pre-issue a certificate to the laptop as a setup process with server 2003 standard with GPO, if so how do I create the EAP-TLS certificate. If I can upgrade, will this require a DCPRMO back to a standalone server with all that intails etc.

Regards

Andrew

"Steven L Umbach" wrote:

> OK. I would suggest that when you create the new template that you might
> want to consider that the private keys not be exportable so that they can
> not export their certificate/private key unless there is a particular need
> for such. Also by default you will need to have an email address in each
> user's account properties in AD that will be included on the certificate. If
> you do not have a need for that, you can remove that requirement from the
> template you create also under subject name. Users on Windows 2000 computers
> and earlier can not obtain a certificate via autoenrollment [version 1
> computer certificates can be obtained via automatic request]. Keep in mind
> that by default any domain user can add up to ten workstations to the domain

microsoft.public.security: Re: Enabling a Certificate template

- > *which means that a domain user could possibly join an unauthorized computer*
- > *to the domain and*