

Re: Automatic enrollment of user certificates

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-01/0317.html>

anonymous_at_discussions.microsoft.com

Date: 01/06/04

Date: Tue, 6 Jan 2004 09:31:52 -0800

Brian

Thanks for your extensive response – I will definitely look into this.

Jem

>-----Original Message-----

>In article <09b001c3d467\$9e555ba0\$a501280a@phx.gbl>,

>anonymous@discussions.microsoft.com says...

>> *Hello + A Gu'id Ne'er to You!*

>>

>> *I have setup an Enterprise Root CA on Windows 2003 in a*

>> *Windows 2000 AD.*

>>

>> *I am using the certificates in conjunction with RADIUS*

>> *(IAS) on a Win2003 machine to provide 802.1x auth for*

>> *ethernet clients via an HP ProCurve switch as a trial.*

>> *(The plan is to deploy wifi later) The clients are XP*

>> *XP1.*

>>

>> *My question is... it is possible to automatically*

>> *enroll*

>> *user certificates on a client machine. Obviously it is*

>> *possible to do this for computer certs via a GPO.*

However

>> *if the connection breaks (as will happen with wifi) the*

>> *reconnection demands a user cert not a computer cert –*

>> *and*

>> *it is not ideal to have to install certs on client*

>> *machines manually.*

>>

>> *TIA*

>>

>> *Jem*

>>

>Hi Jem,

>

>Yes it is possible. There are a few requirements:

microsoft.public.win2000.security: Re: Automatic enrollment of user certificates

- >1) *You apply the Windows Server 2003 schema extensions*
(you should have
>done this to install the enterprise CA).
>
>2) *You create a version 2 certificate template that*
enables
>autoenrollment for a group that the user is a member of
that allows
>Client authentication (duplicate the user signing only
version 1
>template).
>
>[http://www.microsoft.com/technet/prodtechnol/windowsserver
2003/deploy/co
>nfeat/ws03crtm.asp](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/deploy/colnfeat/ws03crtm.asp)
>
>3) *You need to enable autoenrollment in Group Policy.*
This must be done
>from a 2k3 server or from a xp computer with the 2k3
adminpak installed.
>Details are in the following whitepaper. Ensure that the
GPO is defined
>at the OU where the *user* accounts are defined, not the
computer
>accounts.
>
>[http://www.microsoft.com/technet/prodtechnol/windowsserver
2003/plan/auto
>enro.asp](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/plan/autoenro.asp)
>
>*The combination will allow autoenrollment to any XP*
computers that are
>domain members. This does not work for 2k computers, only
2k3 computers.
>
>*Brian*
>
>