

Re: EFS certificate renewal

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2004-07/4024.html>

From: Miha Pihler (*mihap-news_at_atlantis.si*)

Date: 07/29/04

Date: Thu, 29 Jul 2004 23:31:32 +0200

Hi Jason,

my answers are in-line. I hope they help,

"Jason Darst" <jason_register2000@yahoo.com> wrote in message
news:Xns9535A60259B9jasonregister2000yah@207.46.248.16...

- > *We use EFS in our organization and have a Windows 2003 Enterprise CA*
- > *issuing the certificates for it. We are approaching the renewal time*
- > *and I was looking for some details about how Windows 2000 or Windows XP*
- > *handles the renewal process from the client. I know the high level of*
- > *once the renewal period is reached, if auto-enrollment and renewal is*
- > *allowed in group policy the computer will request a renewal*
- >
- > *The questions come in because we have laptops that go for a long period*
- > *of time not connected to our network. So the following questions arise:*
- >
- > *What triggers a renewal request? Access of an EFS certificate? Login to*
- > *the PC? First bootup? Change in network interfaces? Change in IP*
- > *address?*

Group Policy. When client boots up, it will look for DC to connect to.

- > *If the computer is not connected when the renewal period is first*
- > *reached, what happens?*

Nothing. Again client tries to connect to DC and update group policy and perform tasks defined in group policy.

- > *If the first renewal request is not successful because the Enterprise CA*
- > *is not reachable (laptop is external to the network at the time) will it*
- > *retry?*

Yes, it will "retry" — or better said it will try to renew once it can connect to DC and CA server.

- > *If it retries, what is the trigger for it to retry and how often does it*
- > *do it?*

Re: EFS certificate renewal

I would say, till it has a valid certificate — but it can depend on your settings...

- > *If the expiration period is reached, and group policy says it is to use a*
- > *specified Enterprise CA and that CA is not reachable, will it still*
- > *generate a self signed certificate?*

Yes.

- > *Any answers to these questions would be much appreciated. The technet*
- > *documentation I can find just doesn't go to this level of detail. And*
- > *I'm worried that I'm going to have laptops that are sporadically*
- > *connected missing their renewal chances and issueing self signed*
- > *certificates, whicih would be a mess.*
- >
- > *Thank you.*