

## Re: Expired Recovery Agent EFS Cert

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-12/msg00092.html>

---

- *From:* Jeffrey <[noemail@xxxxxxxxxx](mailto:noemail@xxxxxxxxxx)>
  - *Date:* Fri, 09 Dec 2005 11:08:58 -0500
- 

Steven L Umbach wrote:

XP Pro of course may not need an RA to use EFS but if one is specified in GP then maybe it will not work if the RA is invalid much like W2K works? If that is the case then I would think the old RA should still be able to recover files encrypted prior to it's expiration until files are also updated with the new RA. --- Steve

This appears to be the case from what I saw. The RA was defined in Group Policy and did have an expired cert in the Group Policy. So whenever an XP client would try to encrypt a folder they would receive an error regarding the invalid certificate. Using rsop.msc did show the applied policy on the XP machine in question had an expired cert.

I was able to export the expired key pair and save it to CD for future use, from the reading I did while I worked on this issue, I should still be able to decrypt files that were created while it was valid. I think.

What I did was generate a new key pair using cipher /r and then added it to my group policy as my recovery agent. I had to remove the expired cert to get things working again, but once I did the XP machines in question could encrypt folders and files again. Both the expired key pair and current key pair have been exported and saved to CDs and placed in secure, safe locations.

Where I am at only three of us even use EFS on our machines, but from the reading it looks like one only needs to run cipher /u on their machine to update the keys to the new recovery agent, solving any problems of the old one having expired.

I welcome any additional comments or thoughts as to how or why the initial one expired or if it even should have. I hadn't dived into the hows and whys of EFS until this issue so I can only speak to what seemed to fix my situation.

Thanks for input!

Re: Expired Recovery Agent EFS Cert

Jeffrey

.