

Renewing certificates on Win 2K Pro

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-06/0346.html>

From: Nancy Kafer (*nkafer_at_homesteaderslife.com*)

Date: 06/28/05

Date: Tue, 28 Jun 2005 15:35:00 -0500

I am relatively new to PKI and am working with renewing certificates. I have a Win 2K3 Enterprise Edition server as my CA. I also have approximately 30 laptops (running Windows 2000) with VPN certificates. These certificates are set to expire during the next few months. I know that if I was running Win XP my certificates could auto-reenroll. However, I know that I have to use a script to renew my Win 2K machines. I have taken a copy of the Enroll.vbs script from the "Windows Server 2003 PKI Certificate Security" manual and modified it to account for our environment.

I have a few of questions about renewing certificates:

1) I have the issuance requirements on my VPN certificate set to "CA Certificate Manager approval" for enrollment and checked "Valid existing certificate" for re-enrollment. My issue is that when I run the enroll.vbs script my certificate request gets pended instead of automatically issuing a renewal. So then my script fails. I have made sure that I am specifying /renew as a command line parameter on my cscript command. When I uncheck the "CA Certificate Manager" checkbox and re-run the enroll.vbs script my certificate is issued. Why will the script not automatically renew my certificate when this box is checked? Is the re-enrollment requirement only valid for Win XP? I really don't want to uncheck this box because it is a security risk.

2) Is there a way that when I renew my certificate it uses the existing fields from the original certificate (e.g. Friendly name)? When I looked at the certificate generated via the enroll.vbs script I noticed my friendly name was gone (may have been other fields that were also different from the original certificate).

3) When I unchecked the "CA Certificate Manager approval" checkbox and ran the enroll.vbs script my script ran successfully. I looked at the certificate on my client and it was updated (verified because before I renewed the certificate I changed the validity period). When I look on my Certificate Authority I see a new issued certificate that corresponds to my renewed certificate only it had a different serial number. Is this normal? Should I leave the expired certificate listed in the Issued certificates?

Thanks for any help.

Nancy