

How to add a domain user as a Data Recovery Agent

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-06/msg00209.html>

- *From:* "dln" <dnadon_nospm@xxxxxxxxxxxxx>
 - *Date:* Fri, 30 Jun 2006 12:48:41 -0500
-

Hello All,

I just want to start by stating that I know very little about how to properly implement a PKI – I've been trying to pick things up as I go, but I know that I have a lot more to learn on the topic. Please excuse any questions or statements that appear naive, or unknowledgeable.

I'm trying to figure out how to add a non-privileged, domain user account as a Data Recovery agent. I've got a Windows 2003 native mode domain and a W2K3 based Root CA installed and the CA's root certificate has been added to the domain's "Trusted Root Certification Authorities". For the two user accounts that I want to act as data recovery agents, I've granted them read and enroll permissions on the EFSRecovery template and then made sure that the EFS Recovery Agent certificate template is published by my Root CA. I can enroll both users for an EFS Recovery Agent certificate. I don't know if everything I've done up to this point is correct, but since I got the certificate, I've proceeded under the assumption that it is.

I then go to the Default Domain Policy for my domain, and under Computer Configuration->Windows Settings->Public Key Policies->Encrypting File System, I add the users as data recovery agents. I can "Create a data recovery agent" for the Domain Administrator account and I've tested the domain admin in regards to recovering encrypted files – this much works. However, I can't seem to get my non-admin users to act as recovery agents. This is what I've tried so far:

1. Exported the users' enrolled certificates to a file and then used the GPMC to import them into the Default Domain Policy
2. Used the certificate manager MMC snap-in to copy the certificate from the user's local store to the user's AD account and then used the GPMC to browse the directory for the user.
3. Copied the EFSRecovery template to a new template, granted the same users the read, enroll, and autoenroll permissions; issued the template on the CA; ensured the users received their certificate; and then enrolled them as in step 2.
4. Delegated authority to the GPO to the recovery agent users and then used GPMC to enroll the users as I did the Domain Admin.

How to add a domain user as a Data Recovery Agent

In all cases, I was able to add the appropriate users as recovery agents. However, all newly encrypted files never have the non-admin users listed as Data Recovery Agents, only the Domain Administrator account is ever listed. I can even create another account that is a domain admin and add them to the GPO and that admin account will also show up as a Data Recovery Agent for newly encrypted files. This problem seems to be limited to non-admin accounts.

What am I doing wrong? Do I have the root CA configured improperly or is there some trick about adding data recovery agents that I've missed? If anybody could shed some light on the problem, I would greatly appreciate it.

Thanks,

DLN

.