

Re: DRA is Decrypting Files when it shouldn't be!!!

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-01/msg00938.html

- *From:* Brian Komar [MVP] <bkomar@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 19 Jan 2006 17:07:01 -0600
-

Answers inline:

In article <C715850F-53CC-43A8-8EED-87F77BF49319@xxxxxxxxxxxxxxxx>, DJ@xxxxxxxxxxxxxxxxxxxxxxxxxxxx says...

- > Let's go over this again...
- >
- > OS setup:
- >
- > Installed a fresh copy of XP. Forget about extra RA's. There is only one RA
- > with this setup. I dedicated the Administrator's account as the RA.
- >
- > Problem:
- >
- > EFS is allowing the RA to decrypt 200 files that were encrypted BEFORE an RA
- > was actually created on the XP OS. My question is Why?
- >
- > I was told by "many people" that you have to setup the RA BEFORE enabling
- > encryption to get the RA to decrypt encrypted files.
- >
- > Steps I took:
- >
- > I created a user, encrypted 200 files. Logged off and logged on as
- > Administrator and created a RA. Rebooted and logged in as Administrator and
- > decrypted the 200 files.

When you encrypted the files, the default RA certificate was used. The default install will designate the first administrator account in XP as the DRA in a non-domain environment.

- >
- > In this case here, I created the RA after the files were already encrypted,
- > so why am I ABLE to decrypt the 200 files?

You need to check the certificate profile of the DRA user account. Run certmgr.msc and look to see how many EFS recovery agent certificates you have. Also, against the files, you can run EFSINFO /U /R /C which will show you for the files what the thumbprint of the certificates that were used during the encryption process.

Re: DRA is Decrypting Files when it shouldn't be!!!

>
> Anyway, to resolve the problem, you asked me to do an experiment and told me
> to "export" & "delete" the user's private key, before creating the RA. I did
> this, and now the RA cannot delete the 200 files (which is the way it suppose
> to work)

The goal is to not leave the RA's certificate in the user's profile. It is kind of a break glass in case of emergency (translated = import the certificate and private key only when needed).

>
> My question is, why did you suggest to "export" & "delete" the user's
> private key, then create the RA? And also why does this work and what did I
> do wrong?

You will be able to delete and work with the files when you import the cert and private key back into the profile. In fact, it can be imported into any profile, as the user name has absolutely nothing to do with the decryption process, only access to the private key of the DRA or the user.

>
> Thanks, Dave

>
> -----

>
>> So what did you exactly do? Create a user, encrypt some files, remove the
>> user's EFS certificate private key, create an RA, and not be able to decrypt
>> files as RA or did you use your current configuration where the RA could
>> decrypt user's files, remove user's EFS certificate private key, and RA can
>> no longer decrypt files?? Did you look to see if RA had more then one RA
>> certificate?? ---- Steve
>>
>>
>> "DJ" <DJ@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:C7D62C3E-C1AA-46A1-93E1-D66DE97010B5@xxxxxxxxxxxxxxxxxxxx
>>> Steve, I did what you said (below) and "exported" & "deleted" the user's
>>> private key and now it's acting correctly. Why is this?
>>>

• *Follow-Ups:*

- ◆ **Re: DRA is Decrypting Files when it shouldn't be!!!**
◇ From: Steven L Umbach

• *References:*

- ◆ **Re: DRA is Decrypting Files when it shouldn't be!!!**
◇ From: Steven L Umbach
- ◆ **Re: DRA is Decrypting Files when it shouldn't be!!!**
◇ From: Steven L Umbach
- ◆ **Re: DRA is Decrypting Files when it shouldn't be!!!**

Re: DRA is Decrypting Files when it shouldn't be!!!

◇ *From:* DJ

- Prev by Date: ***Re: repeated request for activation***
- Next by Date: ***Re: DRA is Decrypting Files when it shouldn't be!!!***
- Previous by thread: ***Re: DRA is Decrypting Files when it shouldn't be!!!***
- Next by thread: ***Re: DRA is Decrypting Files when it shouldn't be!!!***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***