

Re: Computer and User Certificates Issues

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-09/0654.html>

From: William Teller (*WilliamTeller_at_discussions.microsoft.com*)

Date: 09/26/05

Date: Mon, 26 Sep 2005 14:52:05 -0700

I still haven't managed to resolve the issue. Mind you, I can think of precious little to try to further diagnose the problem.

Any further suggestions? I'd rather not resign myself to defeat on this...

"William Teller" wrote:

- > *Hello again,*
- >
- > *Thank-you Steven Umbach and jabrandt for the helpful posts! Unfortunately*
- > *the issue is still unresolved. More information on the issue follows:*
- >
- > *Yesterday, something very strange happened, the Automatic Certificate*
- > *Enrollment of User Certificates using the custom v2 User Certificate Template*
- > *on all Domain Clients suddenly started working. This is a good thing and a*
- > *bad thing. Good because it works ;). Bad because I have no idea why and I*
- > *have spent 30mins thinking about what I have done in the last two days and*
- > *come to the conclusion I haven't done anything! It's driving me insane that*
- > *now User Certificate Enrollment works for no apparent reason.*
- >
- > *1. I tried your suggestion Steven. On a client machine I can successfully*
- > *request the new custom v2 User Cert that supports auto-enrollment as well as*
- > *the included version 1 no autoenrollment User Cert manually through the MMC.*
- > *However, I can NOT request the custom v2 Computer Cert nor the included v1 no*
- > *autoenrollment Computer Cert. It seems that I can only request User Certs but*
- > *no Computer Certs!*
- > *2. Concerning permissions, these are the exact permissions I am using now:*
- > *Domain CA Security Permissions:*
- > *Administrators = Read*
- > *Domain Admins = Read + Issue and Manage Certificates*
- > *Enterprise Admins = Read + Issue and Manage Certificates + Manage CA*
- > *Authenticated Users = Request Certificates*
- > *Custom User Cert Security Permissions:*
- > *Authenticated Users = Read*
- > *Domain Admins = Read + Write + Enroll*
- > *Domain Users = Enroll + Autoenroll*
- > *Enterprise Admins = Read + Write + Enroll*
- > *Custom Computer Cert Security Permissions:*

microsoft.public.security: Re: Computer and User Certificates Issues

- > *Authenticated Users = Read*
- > *Domain Admins = Read + Write + Enroll*
- > *Domain Computers = Enroll + Autoenroll*
- > *Enterprise Admins = Read + Write + Enroll*
- > *All domain users and computers attempting autoenrollment ARE in the Domain*
- > *Users / Domain Computers groups. Also, it is worth noting that these*
- > *templates are duplicates of the respective computer/user base templates. Only*
- > *modification is the expiry time and the permissions to allow for*
- > *autoenrollment.*
- > *3. No unusual messages in the Application Log for the CA – everything seems*
- > *to be working fine. The CA can contact the DC fine – and the now working User*
- > *Cert autoenrollment seems to be proof of this.*
- > *4. The netdiag tool reported no problems whatsoever with the configuration!*
- > *5. The CA is running Windows Server 2003, Enterprise Edition.*
- > *6. Kerberos seems to be working fine. Using klist from the Windows Support*
- > *Tools (or Resource Kit can't remember which) with options 'tgt' and 'tickets'*
- > *on the CA returns the correct output.*
- > *7. This is a test lab environment with no Windows 2000 DC's. The domain is*
- > *at a Windows Server 2003 Domain Functional Level.*
- >
- > *I hope this information helps and I am baffled by the sudden successful*
- > *autoenrollment of User Certificates. It's maddening! One thought, are there*
- > *any GPO settings that could possibly prohibit installation and/or requests of*
- > *Computer Certificates? None come to mind but I may be wrong. Also, when I*
- > *attempt to request a Computer Cert it is worth noting the request does not*
- > *show up as a 'Failed Request' in the CA. Thanks for the help and any*
- > *additional correspondence in advance.*
- >
- > *Yours sincerely,*
- >
- > *William Teller*
- >
- >
- > *"jabrandt@online.microsoft.com" wrote:*
- >
- >> *So a couple of new things to check out.*
- >>
- >> *1. You created a custom V2 template but is this CA running Windows Server*
- >> *2003 Enterprise Edition? Standard Ed. of the OS will not issue custom*
- >> *templates.*
- >>
- >> *2. A 2003 CA requires Kerberos authentication so if for some reason you fail*
- >> *Kerberos and use NTLM you will be denied access. A tool such as Klist or*
- >> *Kerbtray will show if you have a TGS Kerberos ticket from that machine.*
- >>
- >> *3. A 2003 CA with SP1 installed will not function properly in a Windows*
- >> *2000 AD that does not have the 2003 Schema extension installed. Either*
- >> *install the Schema extension or uninstall SP1.*
- >>
- >> *James*
- >>

microsoft.public.security: Re: Computer and User Certificates Issues

> > "Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message
> > news:eaJEGSFwFHA.3720@TK2MSFTNGP14.phx.gbl...
> > > Can you request any certificate at all via the mmc snapin for either user
> > > or computer such as the standard version 1 templates?? That will help
> > > determine if there is just a problem with that one certificate template or
> > > requesting certificates in general. Also use the Management Console for
> > > the CA and go to the CA properties for security to make sure authenticated
> > > users have the allow permission for request certificates. Check the logs
> > > on the CA [system/application] for anything that may indicate a problem
> > > contacting the domain controller and verify that you can ping the domain
> > > controller from the CA by fully qualified domain name and IP address. Also
> > > run the support tool netdiag on the CA to see if any related problems are
> > > discovered such as dns, dc discovery, or trust/secure channel. --- Steve
> > >
> > >
> > > "William Teller" <WilliamTeller@discussions.microsoft.com> wrote in
> > > message news:7145382C-6D0D-4F09-B011-30448A72FC9B@microsoft.com...
> > > > Thanks for the help.
> > > >
> > > > I have double checked the permissions on each duplicate certificate, they
> > > > are exactly as follows:
> > > >
> > > > New Computer Certificate:
> > > > Authenticated Users = Read
> > > > Domain Computers = Read, Enroll, Autoenroll
> > > > Domain Admins = Read, Write, Enroll
> > > > Enterprise Admins = Read, Write, Enroll
> > > >
> > > > New User Certificate:
> > > > Authenticated Users = Read
> > > > Domain Users = Read, Enroll, Autoenroll
> > > > Domain Admins = Read, Write, Enroll
> > > > Enterprise Admins = Read, Write Enroll
> > > >
> > > > I have checked the Failed Requests folder on the CA and there are no
> > > > failed
> > > > requests. I have also tried manually enrolling for a computer certificate
> > > > through the Computer Certificates MMC Snapin. When I requested a
> > > > certificate
> > > > I could see the new duplicate computer certificate for autoenrollment and
> > > > could select it. But when I clicked finish I got the following message:
> > > >
> > > > "The certificate request failed because of one of the following
> > > > conditions:
> > > > -The certificate request was submitted to a Certification Authority
> > > > (CA)
> > > > that is not started.
> > > > -You do not have the permissions to request certificates from the
> > > > available CA's."
> > > >
> > > > Issue still not resolved, but trying hard to find out more info. The

microsoft.public.security: Re: Computer and User Certificates Issues

> > > security event log shows no access denied events by the way. Thank-you in
> > > advance for any additional help.
> > >
> > > Sincerely,
> > >
> > > William Teller
> > >
> > > "Steven L Umbach" wrote:
> > >
> > >> Check your duplicate template for the computer certificate and verify
> > >> that
> > >> domain computers group has read, enroll, and autoenroll permissions. On
> > >> your
> > >> CA use the Management Console for Certificate Authority and look in the
> > >> failed requests folder to see if you find anything there that may have
> > >> more
> > >> details on the reason the autoenroll failed. Try requesting a computer
> > >> certificate manually on one of the computers while logged on as a local
> > >> administrator using the mmc snapin for computer certificates to see if
> > >> that
> > >> works or not. You would need to go to the personal folder, right click
> > >> and
> > >> select all tasks – request new certificate. --- Steve
> > >>
> > >>
> > >> "William Teller" <WilliamTeller@discussions.microsoft.com> wrote in
> > >> message
> > >> news:3CB04962-A00E-4804-95EE-57ED421131CD@microsoft.com...
> > >> > Hello,
> > >> >
> > >> > I have setup a Windows Server 2003 box in a test environment as a
> > >> > RADIUS
> > >> > Server using IAS to familiarise with Wireless Networking
> > >> > Authentication
> > >> > (we
> > >> > are intending to deploy some Windows 2003 systems as RADIUS Servers in
> > >> > the
> > >> > near future). The authentication method that I am hoping to use is
> > >> > EAP-TLS,
> > >> > which I understand requires User and Computer Certificates. Hence, I
> > >> > installed a CA on the Server, and duplicated the User and Computer
> > >> > Certificate Templates, changing only the Expiration Times. Both
> > >> > Templates
> > >> > have Authenticated Users with Read Access, Domain Admins with Full
> > >> > Access.
> > >> > The new User Template has Domain Users with Enroll and AutoEnroll
> > >> > Access
> > >> > and
> > >> > the same for Computer Template except for Domain Computers group. We
> > >> > have
> > >> > configured the Domain Level GPO to grant Automatic Certificate

microsoft.public.security: Re: Computer and User Certificates Issues

>>>> > *Enrollment.*
>>>> > *However, when computers in the test environment update Group Policy*
>>>> > *they*
>>>> > *all*
>>>> > *contain the following events:*
>>>> >
>>>> > *Event Type: Error*
>>>> > *Event Source: AutoEnrollment*
>>>> > *Event Category: None*
>>>> > *Event ID: 13*
>>>> > *Date: 22/09/2005*
>>>> > *Time: 9:54:16 PM*
>>>> > *User: N/A*
>>>> > *Computer: EPT-101*
>>>> > *Description:*
>>>> > *Automatic certificate enrollment for local system failed to enroll for*
>>>> > *one*
>>>> > *LFN Computer certificate (0x80070005). Access is denied.*
>>>> >
>>>> >
>>>> > *For more information, see Help and Support Center at*
>>>> > *<http://go.microsoft.com/fwlink/events.asp>.*
>>>> >
>>>> > *Event Type: Error*
>>>> > *Event Source: AutoEnrollment*
>>>> > *Event Category: None*
>>>> > *Event ID: 13*
>>>> > *Date: 22/09/2005*
>>>> > *Time: 10:09:49 PM*
>>>> > *User: N/A*
>>>> > *Computer: EPT-201*
>>>> > *Description:*
>>>> > *Automatic certificate enrollment for local system failed to enroll for*
>>>> > *one*
>>>> > *LFN Computer certificate (0x80070005). Access is denied.*
>>>> >
>>>> >
>>>> > *For more information, see Help and Support Center at*
>>>> > *<http://go.microsoft.com/fwlink/events.asp>.*
>>>> >
>>>> > *Where have I gone wrong? These are XP SP2 clients, I previously tried*
>>>> > *enabling detailed Enrollment Logging but the additional events*
>>>> > *provided no*
>>>> > *extra information.*
>>>> >
>>>> > *Thank-you in advance for all corresspondence,*
>>>> >
>>>> > *William Teller*
>>>> >
>>>> >
>>>> >

microsoft.public.security: Re: Computer and User Certificates Issues

> > >
> > >
> >
> >
> >
> >