

# Re: ADAM using SSL Problem

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-03/msg01496](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-03/msg01496)

---

- *From:* Rod Clingaman <[RodClingaman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:RodClingaman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 23 Mar 2007 02:35:05 -0700
- 

Thanks Lee. I apologize for the mistake, but I meant to state:  
After I exported the cert to Desktop/mycert.prx  
Next I import into the Certificates – Service (ADAM1) \ Personal \  
Certificates.

No luck :(

"Lee Flight" wrote:

Hi

the cert requested for the service needs to be in the ADAM service personal store not the ADAM service Trusted root store which may explain why you are not seeing a private key.

Lee Flight

"Rod Clingaman" <[RodClingaman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:RodClingaman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:536CEE03-6F59-4B29-B8C2-9307C93BC37B@xxxxxxxxxxxxxxxxxxxx](mailto:news:536CEE03-6F59-4B29-B8C2-9307C93BC37B@xxxxxxxxxxxxxxxxxxxx)

On the ADAM server(windows 2003), I add a snap/in and show the Certificates for current user, and for the ADAM service account.

Next I browse to <http://somehost/certsrv/>  
Clicked on "Download a CA certificate, certificate chain, or CRL"  
Clicked on "install this CA certificate chain."  
I then seen the certificate in the snap-in at: Certificates – Current User \ Trusted Root Certification Authorities \ Certificates.  
I copied that certificate and pasted it in the Certificates – Service (ADAM1) \ Trusted Root Certification Authorities \ Certificates.

Next I browse to <http://somehost/certsrv/>  
Clicked on "Request a certificate" then "advanced certificate request", then

## Re: ADAM using SSL Problem

"Create and submit a request to this CA". I make the following modifications to the default values:

Name: the FQDN of the ADAM server  
Friendly Name: the FQDN of the ADAM server  
Type of certificate: Server Authentication Certificate  
Create new key set  
CSP: Microsoft RSA SChannel Cryptographic provider  
Mark keys as exportable  
Request format: PKCS10

Then I submit the request and install the certificate.

I then seen the certificate in the snap-in at: Certificates – Current User  
\  
Personal \ Certificates.  
Then I Right click the certificate and All tasks – Export.  
Yes, export the private key, don't enter a password.  
Store it on the Desktop/mycert.prx  
Next I import into the Certificates – Service (ADAM1) \ Trusted Root  
Certification Authorities \ Certificates.

Then I restart the ADAM service and launch LDP (on the ADAM server) and use the FQDN, the SSL port, and check the SSL box. I get the following error:

```
ld = ldap_sslinit("FICTIONWDA001.FIC.DEV", 50053, 1)
Error 0 = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3)
Error 81 = ldap_connect(hLdap, NULL)
Server error: empty
Error 0x51: Fail to connect to FICTIONWDA001.FIC.DEV.
```

I noticed that the RSA\MachineKeys directory that gets mentioned in allot of articles, never gets a new file when I install the certificates. There are 6 old files in there with long hash names.

The server also acts as a domain controller.

Any advice is greatly appreciated!