IIS 7 Error "A specified logon session does not exist. It may already have been terminated." when using https

Asked 7 years, 11 months ago   Active 22 days ago   Viewed 97k times

▲

73

▼

🔖

13

🕓

I am trying to create Client Certificates Authentication for my asp.net Website.

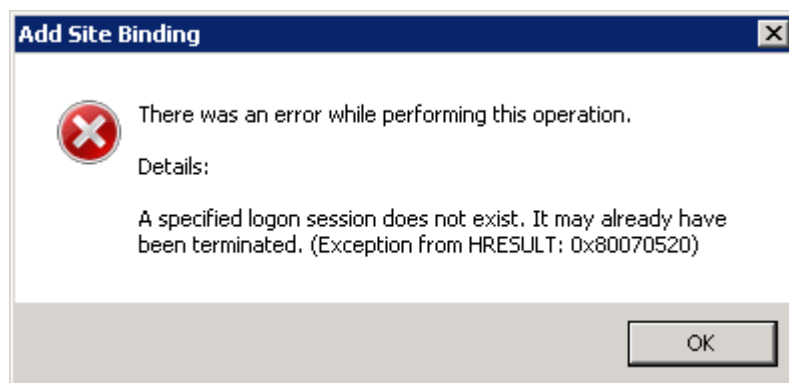In order to create client certificates, I need to create a Certificate Authority first:

> makecert.exe -r -n "CN=My Personal CA" -pe -sv MyPersonalCA.pvk -a sha1 -len 2048 -
> b 01/01/2013 -e 01/01/2023 -cy authority MyPersonalCA.cer

Then, I have to import it to IIS 7, but since it accepts the .pfx format, i convert it first

```
pvk2pfx.exe -pvk MyPersonalCA.pvk -spc MyPersonalCA.cer -pfx MyPersonalCA.pfx
```

After importing MyPersonalCA.pfx, I try to add the https site binding to my Web Site and choose the above as SSL Certificate, but I get the following error:

Add Site Binding   ✕

❌ There was an error while performing this operation.

Details:

A specified logon session does not exist. It may already have been terminated. (Exception from HRESULT: 0x80070520)

                                    OK

Any suggestions?

asp.net   iis   ssl   client-certificates

Share   Improve this question   Follow

asked Feb 19 '13 at 8:41

enb081
3,291 ● 11 ● 37 ● 64

I ve some problem – Adnane ARHARBI Aug 10 '17 at 19:48

**Join Stack Overflow** to learn, share knowledge, and build your career.   Sign up   ✕

79

I ran across this same issue, but fixed it a different way. I believe the account I was using changed from the time I initially attempted to set up the certificate to the time where I returned to finish the work, thus creating the issue. What the issue is, I don't know, but I suspect it has to do with some sort of hash from the current user and that is inconsistent in some scenarios as the user is modified or recreated, etc.

To fix it, I ripped out of both IIS and the Certificates snap-in (for Current User and Local Computer) all references of the certificate in question:
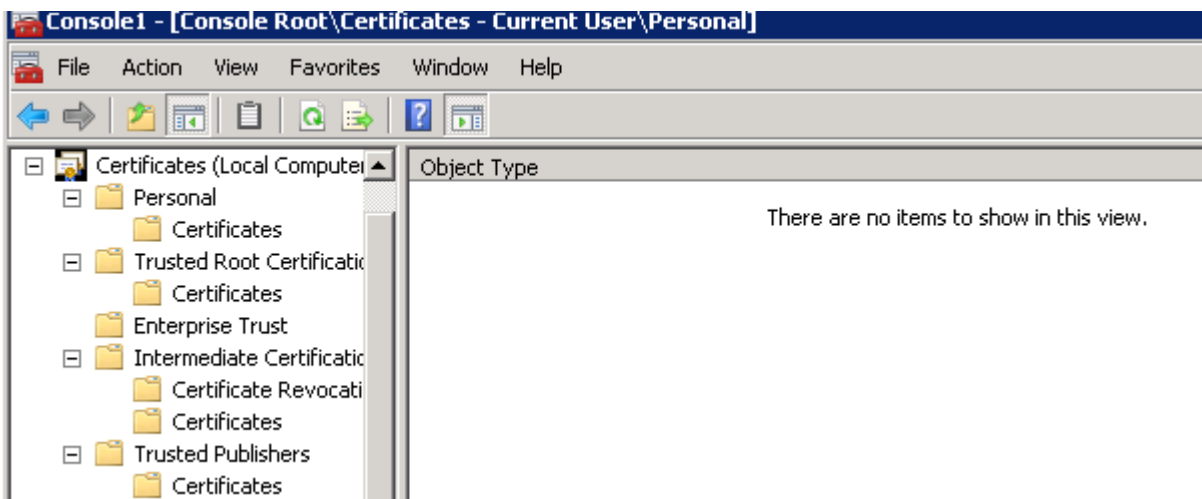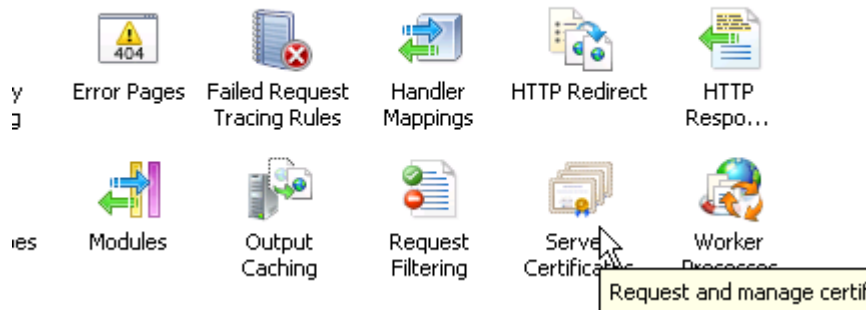
Next, I imported the *.pfx file into the certs snap-in in MMC, placing it in the Local Computer\Personal node:

1. Right-click the Certificates node under Personal (under Local Computer as the root)

2. All Tasks -> Import

3. Go through the Wizard to import your *.pfx

From that point, I was able to return to IIS and find it in the Server Certificates. Finally, I went to my site, edited the bindings and selected the correct certificate. It worked because the user was consistent throughout the process.

Join Stack Overflow to learn, share knowledge, and build your career.

Sign up   ✕

similar set of permissions to take your cert with them and import it anywhere else. Obviously that's not optimal.

Share   Improve this answer   Follow

answered Sep 15 '14 at 18:54

Mike L
4,483 ● 4 ● 32 ● 51

1   In my case the problem was that I imported a *.cer file into the certificate store. Make sure to import a *.pfx file into the certificate store. – MarioVW Mar 18 '16 at 19:04

1   It seems as though following these steps (rather than importing directly into Server Certificates) brings in the intermediary certs as well, which seems significant. – Katstevens Jul 11 '16 at 9:34

All I can say is thanks @Mike L -- this is literally the only thing that worked for me. – pim Mar 16 '17 at 21:00

I used this solution. However, GoDaddy only gave us a *.crt* file for our new certificate, so to extract the private key from the previous certificate (using openssl) and then create a *.pfx* from this (and the *.crt*) and import that. – Jonathan Williams Aug 22 '18 at 10:13

Adding another possible solution. For me it was because I imported the certificate within IIS instead of from the Windows Certificate Manager. – ryanulit Feb 6 '20 at 15:33
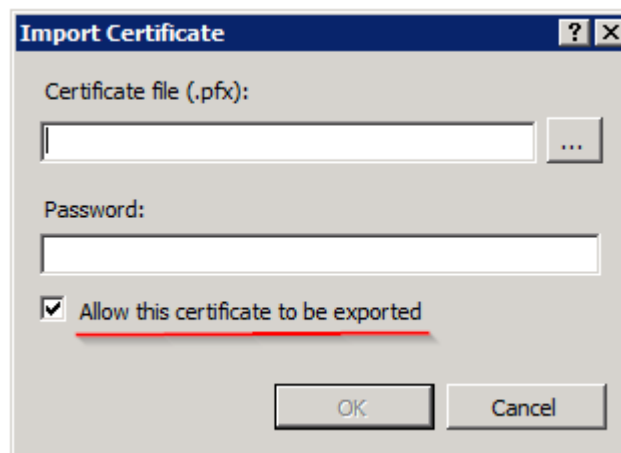

58

Security warning: what the checkbox really means is that the certificate can be read by users that shouldn't be able to read it. Such as the user running the IIS worker process. In production use the other answer instead.

Happened to me too, and was fixed by ensuring that "Allow this certificate to be exported" is **checked** when you import it:

(thanks to this post!)

Share   Improve this answer   Follow

edited May 23 '17 at 12:26

Community ♦

answered Oct 18 '13 at 14:09

Roman Starkov

I first had to remove the certificate under the MMC snap-in certificate store "Certificates (Local Computer)/Personal" and the in the same store, I right clicked and selected import and then imported the certificate marking it as exportable. – Jonathan Oliver Dec 15 '13 at 2:26

2   @aboy021: No you don't. The password which you enter will be used to encrypt the certificate again, but you can choose any password and it does not need to match the original one that was used to import the certificate. – lanoxx Jan 20 '14 at 14:12

6   This is a major security risk. Anyone with administrative access can export your private key. Use Mike L's answer instead. – Steven De Kock Dec 16 '14 at 16:52

3   @romkyns You're right, but you'd need third party tools to do it. When the key is exportable, non-administrative users with read permissions (can be managed with MMC) can also export the private key. In this case it would include the IIS worker process ... – Steven De Kock Dec 24 '14 at 14:08 ✎

This must be some kind of IIS bug, but I found the solution.

10

1- Export *MyPersonalCA.pfx* from IIS.

2- Convert it to **.pem**:

```
openssl pkcs12 -in MyPersonalCA.pfx -out MyPersonalCA.pem -nodes
```

3- Convert it back to **.pfx**:

```
openssl pkcs12 -export -in MyPersonalCA.pem -inkey MyPersonalCA.pem -out MyPersonalCA.pfx
```

4- Import it back to **IIS**.

Share   Improve this answer   Follow

answered Feb 19 '13 at 11:04

enb081
3,291 ● 11 ● 37 ● 64

Nobody probably cares about this anymore, but I just faced this issue with my IIS 7 website binding. The way I fixed it was going to the Certificate Authority and finding the certificate issued to the server with the issue. I verified the user account that requested the certificate. I Then logged into the IIS server using RDP with that account. I was able to rebind the https protocol using that account only. No exports, reissuing, or extension changing hacks were needed.

7

Share   Improve this answer   Follow

answered Dec 26 '13 at 14:21

SkankyMidget
71 ● 1 ● 1

We had the same issue due to incorrectly importing the certificate into the Current User Personal certificate store. Removing it from the Current User Personal store and importing it into the Local

Share **Improve this answer** **Follow**

user5186956

> 2   I would say this is generally the right answer because it is such an easy mistake to make. If you start the certificate manager using Certmgr.msc you get the personal store rather than the computer store. That means the logons are different. Instead you have to use mmc and then add the snap-in which allows you to select computer store. – OnceUponATimeInTheWest Oct 19 '17 at 9:27

▲

5

▼

↺

In our case this problem occurred because we have installed the certificate in a Virtual Machine and made an image of it for further use.

When creating another VM from the image previously created the certificate sends the message.

To avoid this be sure to install the certificate on every new VM installed.

Share **Improve this answer** **Follow**

Paulo Dinis
76 ● 1 ● 2

▲

3

▼

↺

Instead of importing the cert from IIS, do it from MMC. Then goto IIS for binding.

Share **Improve this answer** **Follow**

Kuldeep Heggana
31 ● 1

> My issue was that IIS wasn't importing the full certificate chain (i.e. parent cert), but only the child cert. – ErikusMaximus Nov 25 '19 at 20:58

> this answer was the easiest solution for me, still not sure what was wrong though. – Etienne Apr 6 '20 at 1:38

▲

2

▼

↺

I got this error due to wrong openssl command-line during export PKCS #12 certificate. -certfile key was wrong. I exported certificate again and it was imported successfully.

Share **Improve this answer** **Follow**

Der_Meister
4,283 ● 2 ● 38 ● 47

▲

I had the same issue. Solved by removing the certificate from de personal store (somebody put in

Share Improve this answer Follow

answered Jun 10 '15 at 7:36

Edgar
21 ● 1

2

In my case it was because the World Wide Publishing Service user didn't have permissions to the certificate. After installing the certificate, access the certificates module in MMC and right-click the certificate with the issue. Select "Manage Private Keys..." from the "All Tasks" menu and add the above user. This was SYSTEM user in my case.

Share Improve this answer Follow   edited Sep 2 '15 at 11:00   answered Sep 2 '15 at 7:01

user2034250
55 ● 6

2

According to the MSDN blog post, this can happen when the current user account doesn't have permission to access the private key file which is under the folder "**C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys**". Apparently this can be resolved by granting the user account / user group **Full Access** permission to the above folder.

I've come across the same issue, and was able to resolve it by simply re-importing the .pfx file with the **Allow this certificate ti be exported** checkbox **selected**.
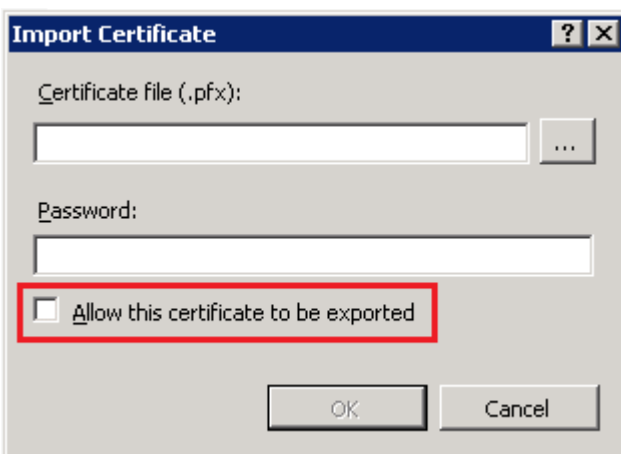
> However, this method imposes a security risk - as any user who has access to your IIS server will be able to export your certificate with the private key.

In my case, only I have access to my IIS server - therefore it was not a huge risk.

Share Improve this answer Follow

answered Feb 11 '19 at 10:57

Janaka Dissanayake
27 ● 5

2

specified logon session does not exist. It may already have been terminated." when using https"
below

1. Verify your pfx cert is healthy with correct private key

2. Run certutil and locate the certs 'unique Container name' - i used certutil -v -store my

3.Navigate to C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys and locate the system file that
corresponds to your Container name found above

4. Check permissions and ensure 'system' has full control to file.

Once applied i then checked IIS and was able to apply to https without error

Share   Improve this answer   Follow

answered Jan 7 at 4:02

opieo69
21 ● 1

1

I was getting a this error when trying to bind localhost pfx cert for my development machine.
Before i tried any of this above, tried something simpler first.

1. Closed any localhost dev site i had openned.

2. Stopped my IIS server and closed the manager

3. run the manager as Admin

4. Added all my https bindings, no errors or issues this time.

5. restarted iis

Everything seems to work after that.

Share   Improve this answer   Follow

answered May 4 '17 at 20:52

Yogurt The Wise
3,879 ● 4 ● 31 ● 40

1

I was getting same error whilst binding the certificate, but fixed after deleting the certificate and
importing again through mmc console.

Share   Improve this answer   Follow

answered Sep 16 '20 at 18:29

Ram
41 ● 2

---

1   Any explanation to why it fixed would much more helpful – Umang Sep 16 '20 at 23:33

Join Stack Overflow to learn, share knowledge, and build your career.   Sign up   ✕

▲

0

▼

I managed to fix this problem by importing the SSL certificate PFX file using Windows Certificate Manager.

http://windows.microsoft.com/en-us/windows-vista/view-or-manage-your-certificates

Share   Improve this answer   Follow

answered Sep 22 '15 at 6:18

jorel
808 ● 7 ● 15

▲

0

▼

I just had this issue today and feel compelled to post my solution in the hope that you will lose less hair than I've just done.

After trying the solutions above, we had to re-issue the SSL certificate from the SSL provider (RapidSSL issuing as a reseller for GeoTrust).

There was **no cost** with this process, just the five minute wait while the confirmation emails (admin@) arrived, and we gained access again.

Once we had the response, we used IIS > Server Certificates to install it. We did not need the MMC snap-in.

https://knowledge.rapidssl.com/support/ssl-certificate-support/index?page=content&id=SO5757

We kept a remote desktop window to the server open throughout, to avoid any issues with differing login accounts/sessions, etc. I do believe it is an IIS bug as another expert believes, as we only have one RDC account. What is most infuriating is that the very same certificate has been working perfectly for two months before suddenly "breaking".

Share   Improve this answer   Follow   edited Mar 29 '16 at 9:42

answered Mar 29 '16 at 9:32

EvilDr
7,382 ● 9 ● 55 ● 109

▲

0

▼

In my case I imported a newer version of a certificate (PFX for IIS) from StartSSL just recently and forgot to remove the old one, which somehow caused this error (now two certs sort of the same). I removed both of them, imported the proper one, and now it works.

Share   Improve this answer   Follow

answered Sep 10 '16 at 19:07

James Wilkins
5,308 ● 2 ● 34 ● 60

▲

Try :

Join Stack Overflow to learn, share knowledge, and build your career.

Sign up   ✕

2. Run "certlm.msc" and open Personal/Certificates

3. Delete any cert named "*.vsts.me" and "vsts.me"

4. Re-deploy

Share   Improve this answer   Follow

Vikas Gupta
9,051 ● 4 ● 25 ● 36

0

We found another cause for this. If you are scripting the certificate install using PowerShell and used the `Import-PfxCertificate` command. This will import the certificate. However, the certificate imported cannot be bound to a website in IIS with the same error as this question mentions. You can list certificates using this command and see why:

```
certutil -store My
```

This lists the certificates in your Personal store and you will see this property:

```
Provider = Microsoft Software Key Storage Provider
```

This storage provider is a newer CNG provider and is not supported by IIS or .NET. You cannot access the key. Therefore you should use certutil.exe to install certificates in your scripts. Importing using the Certificate Manager MMC snap-in or IIS also works but for scripting, use certutil as follows:

```
certutil -f -p password -importpfx My .\cert.pfx NoExport
```

See this article for more information: https://windowsserver.uservoice.com/forums/295065-security-and-assurance/suggestions/18436141-import-pfxcertificate-needs-to-support-legacy-priv

Share   Improve this answer   Follow

Ed Greaves
4,397 ● 2 ● 19 ● 19

Join Stack Overflow to learn, share knowledge, and build your career.

Sign up   ✕