

## Re: SSL broken after Windows 2003 upgrade

**Source:**

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-11/0969.html>

---

**From:** David Wang [Msft] (*someone\_at\_online.microsoft.com*)

**Date:** 11/14/04

Date: Sun, 14 Nov 2004 04:05:33 -0800

Hmm, looks fine to me. All TCPView tells you is that IIS is listening on port 443. The svchost.exe you reference is "IIS". If you read basic IIS6 Architecture (

<http://www.microsoft.com/downloads/details.aspx?FamilyID=80a1b6e6-829e-49b7-8c02-333d9c148e69&DisplayL>  
)

, you will realize that IIS6 consists of 4 interacting pieces —

1. HTTP.SYS in kernel mode, which parses requests directly from TDI and routes them to the appropriate w3wp.exe based on configuration from WAS
2. WAS, inside the svchost.exe you point to — which basically orchestrates configuring HTTP.SYS based on data from the metabase, and monitors the w3wp.exe based on AppPool configuration. It runs no user code and based on its role, it is closest in identity to "IIS".
3. W3WP.EXE — which basically picks up requests from HTTP.SYS, communicates with WAS to do health monitoring, and executes all requests to consume requests and generate responses (which go back through HTTP.SYS directly)
4. INETINFO.EXE — legacy process. Just contains the metabase (IIS configuration data).

Try making a SSL request using WFetch and give what happens (

<http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLa>  
)

.

WFetch can make both a normal SSL request as well as a Client-Certificate SSL request and gives great control over exactly what you send over the wire — so you should be able to conclusively figure out where the 400 is coming from.

400 Bad Request indicates something that is wrong with the request itself — WFetch gives complete control over the request that is sent, so I want to know what is "400" about it. Using a web browser requires additional tools to figure out what was actually transported over HTTPS (since the browser won't tell you, and Network Trace won't tell you since it's all encrypted). Basically, get back to basics to determine what is wrong.

As for your other comments:

> *https:// worked fine in Windows 2000 Server for over a year:*

## microsoft.public.inetserver.iis: Re: SSL broken after Windows 2003 upgrade

- > – domain name "secure.mydomain.com"
- > – on an IP address shared with about 50 other websites (even though
- > MSKB tells me now this shouldn't work...)

There is nothing that says that HTTPS cannot be on a shared IP with multiple websites. People are generally completely confused about SSL, how it works and how to configure it, so there may have been some simplifications here and there (for the benefit of simplicity for the masses — too much detail can be a bad thing sometimes). What you have to realize is that HTTPS is uniquely identified based on two parameters — IP Address and Port — NO HOST HEADERS ALLOWED (Catch 22 problem in determining server certificate for SSL handshake BEFORE you can parse out the Host header to determine which website [and hence server certificate] to use). So, you can certainly have 51 unique bindings in the form of -- IP:80:<50 different host headers> along with IP:443: . Thus, the configuration you describe can either be done with exactly one website, or up to 51 different websites — all depends on your configuration needs.

In other words, Bindings != Websites. A website provides a mapping between a network binding and a physical namespace. Arbitrary number of mutually UNIQUE bindings can be mapped to the same physical namespace.s

- > – not requiring SSL connection, users could connect via http:// or
- > https:// without trouble.

Your configuration works for me on IIS6 as I just configured and tested it. I have a feeling it is just some odd configuration problem you've inherited by upgrading (vs clean install with migration) from IIS5. It's just not straight forward to figure out what problem it is because upgrade leaves old cruft around.

```
--
//David
IIS
This posting is provided "AS IS" with no warranties, and confers no rights.
//
"Paul" <paule@nospam-mindspring.com> wrote in message
news:009HxRayEHA.1928@TK2MSFTNGP10.phx.gbl...
Here is the XML from metabase.xml - this is the only site with a
SecureBinding that is not null. All other sites have SecureBindings=""
(IP address and domain name changed slightly below)
<IISWebServer Location ="/LM/W3SVC/38"
  LogPluginClsid="{FF160663-DE82-11CF-BC0A-00AA006111E0}"
  MD_ISM_ACCESS_CHECK="4660"
  SSLCertHash="19c4e3734ed15f22cd3cb1706c1fe5800b9fe63f"
  SSLStoreName="MY"
  SecureBindings="x.x.187.136:443:"
  ServerAutoStart="TRUE"
  ServerBindings="x.x.187.136:80:secure.ourdomain.com"
  ServerComment="Secure OurDomain Site"
>
</IISWebServer>
.....
Using SysInternal's TCPView, the only thing on the machine listening on port
443 is SVCHOST.EXE whose properties reveal:
```

## microsoft.public.inetserver.iis: Re: SSL broken after Windows 2003 upgrade

```
"C:\WINNT\System32\svchost.exe -k iissvcs"
-- Paul
"David Wang [Msft]" <someone@online.microsoft.com> wrote in message
news:%231ON$EXyEHA.1292@TK2MSFTNGP10.phx.gbl...
> This really sounds like you have a bad SSL Binding inherited from IIS5,
> thus
> HTTP.SYS isn't expecting anything to come over IP:443 and hence returning
> 400.  SSL Diag tells you that SSL should be working assuming the website
> connects -- which is where you are falling short.
>
> Look in %systemroot%\system32\inetsrv\metabase.xml for "SecureBinding" and
> please show them all here.
>
> Finally -- are you running any other servers that may be listening on port
> 443 on another IP:Port.
>
> --
> //David
> IIS
> This posting is provided "AS IS" with no warranties, and confers no
> rights.
> //
> "Paul" <paule@nospam-mindspring.com> wrote in message
> news:OxtnU6OyEHA.4028@TK2MSFTNGP15.phx.gbl...
>> the 'bad request' bad is a bit weird.
>> any error in event log ?
>
> Nope.
>
>> httperr ?
>
> Yes, the 400 Bad Request shows up for the http://x.x.x.x request
> (non-SSL)
> but I assume this is correct since the website IP address x.x.x.x is tied
> to
> the host header name "secure.mydomain.com" and there is no "blank"
> catch-all
> host header for it.
>
>> secure.mydomain.com is bind to own IP address ?
>
> Yes.
>
>> at the SSL section change 'default' to the IP address.
>
> Never was "(all unassigned)", I always had it set to the same IP address
> as
> the port 80 section above it.
>
>> restart IIS services.
>
> Done that about 100 times already <g>...
>
>
> Is there anything in the IIS metabase dump (XML) that I can look for as a
> clue to what the problem might be?
>
> Thanks.
> -- Paul
>
>
>>
```

microsoft.public.inetserver.iis: Re: SSL broken after Windows 2003 upgrade

```
>> --
>> Regards,
>> Bernard Cheah
>> http://www.tryiis.com/
>> http://support.microsoft.com/
>> http://www.msmvps.com/bernard/
>>
>>
>> "Paul" <paule@nospam-mindspring.com> wrote in message
>> news:OJyXEPHyEHA.1524@TK2MSFTNGP09.phx.gbl...
>>> https:// worked fine in Windows 2000 Server for over a year:
>>> - domain name "secure.mydomain.com"
>>> - on an IP address shared with about 50 other websites (even though
>>> MSKB
>>> tells me now this shouldn't work...)
>>> - not requiring SSL connection, users could connect via http:// or
>> https://
>>> without trouble.
>>>
>>> Upgraded this box to Windows 2003, now https:// is broken.
>>> - moved the secure site to its own IP address with no other sites on it
>>> (per the MSKB suggestion)
>>> - removed and reinstalled SSL cert (Thawte cert)
>>> - IIS manager says cert is good
>>> - Used SSLDiag to test, it says everything ok. SSL handshake
>>> successful.
>> I
>>> notice SSLDiag says it is talking HTTP/1.0 -- could it be that IE6 is
>>> talking HTTP/1.1 and that is the problem?
>>> - Don't see any other bindings on port 443 on any other sites (they are
>> all
>>> on other IP address anyway)
>>> - Default website is "off"
>>> - Administration website is "off"
>>> - Access to http://secure.mydomain.com is fine, returns default home
>>> page
>>> - Try https://secure.mydomain.com, get "page not found or DNS error"
>>> - Try the public static IP address http://x.x.x.x and get the
>>> default.htm
>>> home page
>>> - Try the public static IP address https://x.x.x.x and get prompted in
>>> browser with "certificate invalid" warning dialog box, say "yes,
>>> accept",
>>> then get 400 - Bad request. But maybe this is normal since the cert is
>> tied
>>> to the domain name, not the IP address?
>>> - Can connect via telnet to secure.mydomain.com port 443.
>>>
>>> Like I said, I had no problem whatsoever before upgrading to Windows
>>> 2003.
>>> No hardware or software changes. I am totally stumped, checked numerous
>>> MSKB articles, google searches, etc.
>>>
>>> Help!!
>>>
>>> TIA,
>>> Paul
>>>
>>>
>>>
>>>
```

microsoft.public.inetserver.iis: Re: SSL broken after Windows 2003 upgrade

>>  
>>  
>  
>  
>