

RE: IIS – use SSL 3.0 only

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-04/msg01889.html>

- *From:* v-jaluo@xxxxxxxxxxxxxxxxxxxxxxxx ("Jacky Luo [MSFT]")
 - *Date:* Thu, 12 Apr 2007 10:30:18 GMT
-

Hi Mark,

Thanks for posting here.

From the description, I understand the issue is that you want to only use SSL 3.0 for IIS 6.0. If I am off base, please don't hesitate to let me know.

By default, IIS supports a batch of protocols, including: TLS 1.0, PCT 1.0, SSL 2.0 and SSL 3.0. The protocol selection is controlled by clients-side. IE supports SSL2.0, SSL3.0 and TLS 1.0 (The configuration is in Internet Options->Advanced). For some special application, we can disable some protocol support on either server-side or client-side:

187498 Disable PCT 1.0, SSL 2.0, or SSL 3.0 on IIS
<http://support.microsoft.com/?id=187498>

<http://www.winnetmag.com/Windows/Article/ArticleID/7741/7741.html>

NOTE: This response contains a reference to a third party World Wide Web site. Microsoft is providing this information as a convenience to you. Microsoft does not control these sites and has not tested any software or information found on these sites; therefore, Microsoft cannot make any representations regarding the quality, safety, or suitability of any software or information found there. There are inherent dangers in the use of any software found on the Internet, and Microsoft cautions you to make sure that you completely understand the risk before retrieving any software from the Internet.

the client and the server negotiate a common protocol to help secure the channel. If the server and the client have multiple protocols in common, IIS tries to help secure the channel with one of the protocols that IIS supports. The protocol that IIS uses is selected in the following order of preference:

RE: IIS – use SSL 3.0 only

1. PCT 1.0
2. SSL 3.0
3. SSL 2.0

Sometimes, you may want to disable one or more of these protocols. You can do this if you change the registry.

So you can disable PCT 1.0 and SSL 2.0 by change the registry on the server in the IE configuration on the client,just select SSL 3.0

Hope this helps

Have a nice day!

Best regards,

Jacky Luo (MSFT)
Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

PLEASE NOTE: The partner managed newsgroups are provided to assist w