

Re: ADFS Not Compatible with FIPS?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg00769

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 11 Sep 2006 21:24:32 -0500
-

Here's a blog post I found by .NET security luminary Shawn Farkas that sheds a little more light on this:

<http://blogs.msdn.com/shawnfa/archive/2005/05/16/417975.aspx>

It doesn't really suggest whether there is a practical solution to this particular problem though.

Joe K.

Joe Kaplan-MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>

"Susieber" <Susieber@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:9EEF070B-6B09-476D-A01D-3B35A36F101B@xxxxxxxxxxxxxxxxxxxx

Thanks, Joe. I re-enabled SChannel, but got no events. Then the client generated a different error (none of this seems to be consistently reproducible) - and the error was FIPS-specific:

This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms.

Some research led me to find out that It's looking like ASP .NET 2.0 uses the AES algorithm, but it is not a FIPS-compliant algorithm. See <http://support.microsoft.com/kb/911722/en-us?spid=8940&sid=291>.

We are going to try a workaround mentioned in that article - it's a <machineKey> entry to add to the claimapp's web.config file.

"Joe Kaplan" wrote:

Do you still have Schannel event logging enabled in debug mode? Do you get

Re: ADFS Not Compatible with FIPS?

any interesting errors on the machine that is establishing the connection?

This might be something that can be configured around, especially if it is the SSL part of ADFS and not the token signing part. I've never dealt with this problem though, so I really don't know. This might be worth opening an official support inquiry with MS to ensure that it gets taken care of.

Joe K.

--

Joe Kaplan—MS MVP Directory Services Programming
Co—author of "The .NET Developer's Guide to Directory Services Programming"

<http://www.directoryprogramming.net>

--

"Susieber" <Susieber@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:6CE110B6-34AC-4AB4-964F-36D1CE9E3EDC@xxxxxxxxxxxxxxxxxxxx>

Has anyone out there tried enabling FIPS—compliant algorithms on Windows Server in an ADFS environment?

We just discovered that this setting is the cause of many of our past ADFS configuration failures. When we enable `_cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing_` in the domain security policy, the ADFS trust breaks.

The ADFS client can access the Web server with the TLS 1.0 setting enabled in IE. But the federation servers stop talking to each other, and the client gets the `discoverclientrealm` page but eventually just gives up after that with a page not displayable type error.

According to the MSKB, this FIPS setting affects Terminal Services and EFS, so it doesn't surprise me that it affects ADFS.

Re: ADFS Not Compatible with FIPS?

Anyone else been able to track down a fix (other than disabling FIPS)?

TIA,
Susie