

Re: 802.1x authentication for wireless issues w/ ISA 2004

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-04/msg03318.html>

- *From:* JP <JP@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 19 Apr 2007 13:16:03 -0700
-

I might head to staples on the way home and buy a cheap one to try out. I have two identical D-link DWL7100AP. They do support WPA-EAP and the radius server. There could be something in them that is now incompatible. No new firmware or software available for a year or so.

No errors in the group policy update. I rebuilt my cert authority completely from scratch and the certs rolled out as expected. Still no wireless connection. Just the connect and reconnect over and over on two different laptops that are extremely different.

I was happy to see the event log you sent of a successful connection. I think this may hold the key. The part on my event that troubles me is below:

```
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = <none>
Authentication-Server = <undetermined>
Policy-Name = <undetermined>
Authentication-Type = <undetermined>
EAP-Type = <undetermined>
```

Where is a proxy policy coming from? It seems like we are trying to only authenticate the computer and this is trying to authenticate the user and not very well at that.

--

Many thanks,

JP

"Owen Williams [SBS MVP]" wrote:

In article <C4F99CDE-9489-41AF-B50B-9A295AF69346@xxxxxxxxxxxxxxxx>, JP@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx says...

Inline ...

Re: 802.1x authentication for wireless issues w/ ISA 2004

Well the IAS logging finally started to work. It generates a lot of information and I can't understand what to look for.

If you can post perhaps 10 lines from the IAS log, that may be helpful.

My laptops seem to get hung on Validating Identity. This cycles every 10 seconds or so and seems to keep adding a new entry into the IAS log. In the event viewer on the IAS box. I see a granting of access but then an error message logged soon after. Then it all starts again. I will attach events below. The authenticated event looks suspicious to me. It states to use windows to authenticate all users. but has nothing listed for the authenticator. I thought I was only trying to authenticate a user and that was setup in the group policy as computer only.

You are actually trying to authenticate the COMPUTER, not the USER – at least with 802.1x/EAP-TLS. The USER will be separately authenticated at logon (via username & password). It sounds like you have the GPO set correctly ("computer only") but if you have anything set to require user authentication in the GPO, you will need to fix that –or– add a user cert as well as a computer cert.

The ISA server monitoring does not show anything for the various IP that represent my IAS server or the client laptops. If i turn the radius setting on in IAS and point the wap to the ISA/SBS box, I can see quick radius connect and disconnect messages in the ISA monitoring. Then nothing appears in the event log or IAS log on the IAS server machine. It skips IAS basically. If I point the WAP at the IAS server computer then no radius messages appear in ISA and the usual events and logs appear on the IAS server computer. So I think ISA may not be creating the issue.

I am inclined to agree, but I am not 100% certain yet.

I'm thinking at this point that it may be a certificate issue? I am considering killing and rebuilding my certificate authority. I only use it for this authentication anyway so it shouldn't mess any thing up.

Perhaps, but I am thinking it may be a WAP issue – see below.

Re: 802.1x authentication for wireless issues w/ ISA 2004

Owne asked for a system diagram which I will put immediately below. Then I will show the events. Sorry for all the trouble and I really appreciate your help.

Phone line

DSL Modem

Nic card for internet on the SBS BOX

SBS box has Cert server, ISA and RAS on it plus all the other stuff

LAN nic on SBS BOX

Switch

Plugged into the swith is of course the SBS server, my other server that has the IAS on it, all my client computers, and the WAP.

Thanks – this is essentially the same as the sample I provided.

Event Type: Information

Event Source: IAS

Event Category: None

Event ID: 1

Date: 4/18/2007

Time: 6:41:24 PM

User: N/A

Computer: SERVER1

Description:

User host/laptop.xxx.local was granted access.

Fully-Qualified-User-Name = <undetermined>

NAS-IP-Address = 192.168.16.40

NAS-Identifier = WAP1

Client-Friendly-Name = WAP1

Client-IP-Address = 192.168.16.40

Calling-Station-Identifier = 00-0E-35-E4-A1-95

NAS-Port-Type = Wireless – IEEE 802.11

NAS-Port = 1

Proxy-Policy-Name = Use Windows authentication for all users

Authentication-Provider = <none>

Authentication-Server = <undetermined>

Policy-Name = <undetermined>

Authentication-Type = <undetermined>

EAP-Type = <undetermined>

At first blush, this looks normal. But a comparison with a comparable entry from my server shows some possible problems. Specifically, on my network:

Fully-Qualified-User-Name = SBSDomain\laptop\$

Authentication-Provider = Windows

Policy-Name = Wireless GPO Name

Authentication-Type = EAP

EAP-Type = Smart Card or other certificate

I can tell you from personal observations the value of Fully-Qualified-User-Name (and of some of the other fields) can be different than what I show here. However, I checked IAS Event 1 messages on 2 separate SBS networks with 3 separate WAPs (Belkin F5D-72304-4 v1444, LinkSys WRT54gL, and D-Link DIR-655) and `_none_` of them showed `<none>` or `<undetermined>` for the five fields I list.

The missing info from fields based on GPO information (Policy-Name, Authentication-Type, and EAP-Type) makes me wonder whether the GPO has been properly applied to the wireless computer. When you look at the wireless configuration of that computer, does it match what you configured in the GPO? Any GPO-related errors in the wireless computer's event logs?

Event Type: Error
Event Source: IAS
Event Category: None
Event ID: 16
Date: 4/18/2007
Time: 6:41:27 PM
User: N/A
Computer: SERVER1
Description:
A RADIUS message with the Code field set to 2, which is not valid, was received on port 1812 from RADIUS client WAP1. Valid values of the RADIUS Code field are documented in RFC 2865.

I have never seen this event, but the message is useful, though curious. It suggests there is a problem between the RADIUS (IAS) server and the WAP due to an invalid Code field in a RADIUS message. The curious part is that RFC 2865 says this about the Code field:

Code

The Code field is one octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, it is silently discarded.

RADIUS Codes (decimal) are assigned as follows:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge

Re: 802.1x authentication for wireless issues w/ ISA 2004

12 Status-Server (experimental)

13 Status-Client (experimental)

255 Reserved

So, contrary to the event message, Code 2 is valid. What I am wondering is whether Code 2 is valid when an Access-Accept message (apparently) arrives 3 seconds after access has (supposedly) already been granted (the first event you posted).

Any possibility you can try a different WAP?

-- Owen Williams (SBS MVP)