

# Re: SBS Wireless policy

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-12/msg03151.html>

---

- *From:* Owen Williams [SBS MVP] <Owen@xxxxxxxxxxxxxxxxxxxx>
  - *Date:* Mon, 18 Dec 2006 14:00:06 -0500
- 

In article <1166404321.190221.135490@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, ajj3085@alum.rit.edu says...

This is in the IAS policy settings I'm assuming.

Correct: "Wireless LAN Access for Domain Computers" properties -> [Edit Profile] -> Authentication tab -> [EAP Methods] -> "Smart Card or other certificate" selected -> [Edit]

I have only two choices here and both are labeled vortex.hellmouth.local. One has no friendly name and has an issuer of the same. The other's friendly name is vortexDC and issued by hellmouthCA (the name of the CA I chose on the last reinstall. I'm now selecting the latter cert.

The latter cert sounds like the right one.

When you ran the CEICW, did you enter "vortex.hellmouth.local" as the "Web server name" on the "Web Server Certificate" page? Normally this should be the public DNS (or public IP) for your server, to enable remote access, e.g.:

MyServer.PublicDomain.com

(It can be left blank if you don't support remote access.) Sounds like you provided the private (internal) name instead. That's confusing (as you found) but I don't think it will affect the wireless configuration as long as you select the correct cert in IAS.

My setup is more or less vanilla, although I made a few minor changes outside of the wizards before I knew it was a no-no. Nothing to break any of the wizards and I can run them fine. I believe I corrected those errors.

Re: SBS Wireless policy

Just so you know, my docs assume a "standard" SBS configuration, meaning the wizards were used for all the basic setup. Most administrators tweak a few things outside the wizards, but the rule of thumb is: If a wizard can do it, use the wizard unless you REALLY know what you are doing \_in\_the\_context\_of\_ \_SBS\_ (not plain Windows Server 2003).

I actually don't have the Small Business Remote Access Policy rule at all. The others are there.

I believe Small Business Remote Access Policy is added by running the Remote Access Wizard (which configures VPN). I did run that even though I don't use VPN on my server (except for testing).

Advanced tab:  
Name Vendor Value  
Ignore-User-Dialin-Properties Microsoft True  
Service-type RADIUS Standard Framed  
Termination-Action RADIUS Standard RADIUS-Request

Interesting, I had deleted the policy and recreated it per your document, but only had the Service-type setting. I have now added the other settings.

Hmmm ... this could be significant! I'm glad you added the other settings.

Encryption tab: Everything EXCEPT "No encryption" should be selected.  
(The last step of the procedure I document "hardens" these settings once everything is working.)

I even had the No encryption checked, I have unchecked it.

Yeah, I believe "No encryption" is checked by default, and wireless access should work with it checked. But leaving it checked (in theory) permits an unencrypted connection which sort of defeats our purpose here! 8-)

and clicking [Edit] should show:

Certificate issued to: <yourSBS>.<yourdomain>.<yourTLD>  
Friendly name: <may be blank>

Re: SBS Wireless policy

Issuer: <your certificate authority>

Expiration date: <some time in the future>

Again, this is the cert we created (vortexDC issued by hellmouthCA).

Sounds like the right cert.

— Owen Williams [SBS MVP]

.