

# Re: IAS with WorkGroup machines

---

*Source:*

<http://www.tech-archive.net/Archive/Internet/microsoft.public.internet.radius/2008-02/msg00003.html>

---

- *From:* FenderAxe <fa@xxxxxxx>
  - *Date:* 07 Feb 2008 02:34:13 GMT
- 

=?Utf-8?B?SGFyaW5kcmEwMDA=? <Harindra000@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in <news:21753608-2D29-4888-A7C5-6EFF5FD27F2A@xxxxxxxxxxxxxx>:

I'm using EAP-MSCHAP V2 for WiFi Access using 3Com managed switch as RADIUS Client. Setup includes In house CA, AD, IIS, CA and IAS in a single ProLient server.

My IAS works all fine for domain computers with AD user accounts.

But, whenever non-domain (Work Group) system tries to connect to my internal network by using domain credentials; IAS denies it.

Event viewer contains event id 5052 (There is no domain controller available for domain ...) and 3 (Access request for user domain\ADUser is discarded; the user account domain can not be accessed) from source IAS.

How can I grant access for my mobile access clients without connecting them to my domain? (Many of them are vista\xp home)

Your comments are highly appreciated.

When you deployed your own CA, domain member computers automatically received the CA's certificate, which was stored in the certificate stores for the Local Computer and Current User, in the Trusted Root Certification Authorities store.

Because domain member computers have that certificate in the cert store, they trust certificates that are issued by your CA.

To deploy PEAP-MS-CHAPv2 for wireless clients, you must issue server certificates to IAS servers; after you have done that, the server uses the certificate during authentication to prove its identity to client

## Re: IAS with WorkGroup machines

computers. In turn, users provide credentials (user name and password) to prove their identities to IAS.

When the client computers receive the IAS server certificate, they check their Trusted Root Certification Authorities cert store to find out if they trust the CA that issued the server certificate. Your domain member computers can do this successfully, however any non-domain member computer that tries to connect cannot accomplish this, because they don't have the CA certificate in the Trusted Root Certification Authorities cert store.

The solution is to export the CA cert to removable media and then import the cert into the TRCA store for the Local Computer and Current User on non-domain member computers.

See the IAS Help topic "Network access authentication and certificates" for more info.

.