

Re: Machine Authentication not working with wireless clients and IAS

Source:

<http://www.tech-archive.net/Archive/Internet/microsoft.public.internet.radius/2007-02/msg00017.html>

- *From:* "Lee" <weersl@xxxxxxxxxxxx>
 - *Date:* 7 Feb 2007 06:17:05 -0800
-

On Feb 2, 4:36 pm, Jeremy <Jer...@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Good Day,

Hopefully someone can help me with this, as it's driving me crazy. My test scenario is this:

Windows XP SP2 PC connecting to a wireless network provided by our Aruba network controller, which communicates with an IAS server via Radius. The IAS server is also a domain controller in our Windows 2003 domain, the same domain that the PC is a member of.

Wireless settings are WPA/TKIP, with PEAP for authentication. We also have a PKI infrastructure and a certificate assigned to, and installed on, the IAS server. The same root is trusted on the PC.

With all this setup, I can log in to the PC and authenticate perfectly, via the user account. However, as soon as I log out I receive event log errors about the Machine account not working, as such:

```
User host/houitlpwpatest.corpprep.avzprep.net was denied access.
Fully-Qualified-User-Name = CORPPREP\HOUITLPWPATEST$
NAS-IP-Address = 192.168.10.249
NAS-Identifier = <not present>
Called-Station-Identifier = 000B86029500
Calling-Station-Identifier = 00054E4BD816
Client-Friendly-Name = Aruba
Client-IP-Address = 192.168.10.249
NAS-Port-Type = Wireless - IEEE 802.11
NAS-Port = 0
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = <undetermined>
Authentication-Type = MS-CHAPv2
EAP-Type = <undetermined>
Reason-Code = 16
```

Re: Machine Authentication not working with wireless clients and IAS

Reason = Authentication was not successful because an unknown user name or incorrect password was used.

I've turned on IAS logging, and the following entry appears in the IASSAM.log file:

```
[752] 02-02 16:08:08:948: NT-SAM Names handler received request with user
identity host/houitlpwpatest.corpprep.avzprep.net.
[752] 02-02 16:08:08:964: Successfully cracked username.
[752] 02-02 16:08:08:964: SAM-Account-Name is "CORPPREP\HOUITLPWPATEST$".
[752] 02-02 16:08:08:964: NT-SAM Authentication handler received request for
CORPPREP\HOUITLPWPATEST$.
[752] 02-02 16:08:08:964: Processing MS-CHAP v2 authentication.
[752] 02-02 16:08:08:964: LogonUser failed: The account used is a computer
account. Use your global user account or local user account to access this
server.
```

And that's pretty much where I'm stuck. I think I included everything I know so far, if there's anything that I've left out or was unclear about, please let me know. Thanks in advance!

Jeremy

What I would do is create a group of wireless enabled computers. Add the computer objects to that group, then you add that group to the access policy and this should fix that problem. If the computers don't belong to the domain, then you will want to prompt for the username and password, and turn off machine authentication on the computer. I had this same problem. With Domain computers, I'm not sure why the computers need to auth, but they do for a first time login to work on that laptop.