

Re: IAS with PEAP and Airespace (now Cisco 1000)

Source:

<http://www.tech-archive.net/Archive/Internet/microsoft.public.internet.radius/2005-10/msg00016.html>

- *From:* "Lori" <Lori@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 14 Oct 2005 09:54:04 -0700
-

For what it's worth, we also tried using EAP-TLS (I changed the IAS, created a wireless user template on the CA, added computer and user certificates to the client and changed the authentication to smart card or other certificate). Unfortunately, it doesn't work either. The event viewer messages remain exactly the same, the IASSAM.log is exactly the same with the exception that the Allowed EAP type is 13 instead of 25, and the RASTLS log shows the following:

```
[5704] 15:39:55:563: EapTlsBegin(DOMAIN\LoriTest)
[5704] 15:39:55:563: SetupMachineChangeNotification
[5704] 15:39:55:563: Verifying caller...
[5704] 15:39:56:375: Unauthorized use of TLS attempted
```

"James McIllece [MS]" wrote:

```
> "=?Utf-8?B?TG9yaQ==?=" <Lori@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
> news:20D63876-9698-4252-85D4-48436B03C422@xxxxxxxxxxxxxx:
>
>> I have configured WPA RADIUS authentication with an Airespace AP (now
>> called a Cisco 1000) using IAS on our 2003 server (which is also
>> running the CA). I used the MS Win2003 step-by-step guide for setting
>> up secure wireless access in a test lab
>> (http://www.microsoft.com/downloads/details.aspx?FamilyID=0f7fa9a2-e113-415b-b2a9-b6a3d64c48f5&displaylang=en). When I try to connect from
>> any client (our clients are all XP SP2), I receive the following
>> message in the System Log:
>>
>> Source IAS
>> Event ID: 3
>> Access request for user DOMAIN\LoriTest was discarded.
>> Fully-Qualified-User-Name = domain.edu/Staff/Admin &
>> Finance/OCST/Users/Lori Test
>> NAS-IP-Address = 10.15.7.252
>> NAS-Identifier = LowndesAS1
>> Called-Station-Identifier = 00:0B:85:03:18:21:labwireless
```

Re: IAS with PEAP and Airespace (now Cisco 1000)

>> Calling-Station-Identifier = 00:0E:35:E7:25:A1
>> Client-Friendly-Name = LabAS1
>> Client-IP-Address = 10.15.7.252
>> NAS-Port-Type = Wireless - IEEE 802.11
>> NAS-Port = 25
>> Proxy-Policy-Name = Use Windows authentication for all users
>> Authentication-Provider = Windows
>> Authentication-Server = <undetermined>
>> Reason-Code = 1
>> Reason = An internal error occurred. Check the system event log for
>> additional information.
>>
>> There are no other entries in the System log (other than repeats of
>> this one).
>>
>> The IASSAM.log shows the following:
>>
>> [4804] 10-13 10:33:45:421: Creating EAP session
>> [4804] 10-13 10:33:45:421: NT-SAM Names handler received request with
>> user identity DOMAIN\LoriTest.
>> [4804] 10-13 10:33:45:421: Username is already an NT4 account name.
>> [4804] 10-13 10:33:45:421: SAM-Account-Name is "DOMAIN\LoriTest".
>> [4804] 10-13 10:33:45:421: NT-SAM Authentication handler received
>> request for DOMAIN\LoriTest.
>> [4804] 10-13 10:33:45:421: Validating Windows account DOMAIN\LoriTest.
>> [4804] 10-13 10:33:45:421: Sending LDAP search to fsuad2.domain.edu.
>> [4804] 10-13 10:33:45:421: Successfully validated windows account.
>> [4804] 10-13 10:33:45:421: NT-SAM User Authorization handler received
>> request for DOMAIN\LoriTest.
>> [4804] 10-13 10:33:45:421: Using native-mode dial-in parameters.
>> [4804] 10-13 10:33:45:421: Sending LDAP search to fsuad2.domain.edu.
>> [4804] 10-13 10:33:45:421: Successfully retrieved per-user attributes.
>> [4804] 10-13 10:33:45:421: Allowed EAP type: 25
>> [4804] 10-13 10:33:45:421: Setting max. packet length to 1296.
>> [4804] 10-13 10:33:45:499: RasEapBegin failed: Access is denied.
>> [4804] 10-13 10:33:45:499: Caught COM exception: Access is denied.
>>
>> And the RASTLS.log shows:
>>
>> [4804] 10:33:45:421: EapPeapBegin
>> [4804] 10:33:45:421: Verifying caller...
>> [4804] 10:33:45:499: Unauthorized use of PEAP attempted
>> [4804] 10:33:45:499: EapPeapBegin done
>>
>> It works if we use WebAuth or WPA-PSK, so the AP is functioning
>> properly. All Cisco can determine from their logs is that the request
>> to the RADIUS server is timing out.
>>
>> I've gone over our configuration many times, and although there's got
>> to be something we're missing, I am completely baffled as to why this
>> isn't working. Any help in deciphering these errors would be great.

Re: IAS with PEAP and Airespace (now Cisco 1000)

>>
>> Thanks,
>> Lori
>
> It sounds like your client computers are either not configured to use PEAP
> or they do not trust the CA that issued the server certificate to the IAS
> server (you *do* have a server cert configured in remote access policy,
> right?).
>
> Other issues to check are that the AP is configured to allow EAP, and that
> the shared secret on the IAS server and the AP are identical.
>
> --
> James McIllece, Microsoft
>
> Please do not send email directly to this alias. This is my online account
> name for newsgroup participation only.
>
> This posting is provided "AS IS" with no warranties, and confers no rights.
>
>

• **Follow-Ups:**

- ◆ **Re: IAS with PEAP and Airespace (now Cisco 1000)**
 ◇ From: James McIllece [MS]

• **References:**

- ◆ **IAS with PEAP and Airespace (now Cisco 1000)**
 ◇ From: Lori
- ◆ **Re: IAS with PEAP and Airespace (now Cisco 1000)**
 ◇ From: James McIllece [MS]

- Prev by Date: **Re: PEAP 802.1x IAS – only works if previously logged in over wired connection.**
- Next by Date: **Re: No domain controller available**
- Previous by thread: **Re: IAS with PEAP and Airespace (now Cisco 1000)**
- Next by thread: **Re: IAS with PEAP and Airespace (now Cisco 1000)**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**