Authentication between ldap and novell, using aruba as wlan provider

View Votes

Posted November 20th, 2007 by **Aghiad Boukai**
in Enterprise Lockdown

dears
good day
i have this installation
i'm using aruba 2400 controller, and using 802.1x authentication with ldap using wpa2-aes.
and i have novell server which has some application to run.
my problem is i'm facing three login to run my script, while when i use wired i do only one login.
first of all i have to login to my desktop, then login to wlan, then login to novell client then i have to run my application and script.
i read some where that i have to use odyssey Access client, this will merge the authentication for novel and wlan at the same time.
this should work, because my problem start when i loged to novell after logging to windows. (while novel needs network connection to login)

in novel client there's an option is that use odyssey client with novell, but when i check this box, the odyssey doesnt work and it didn't give me any loggin, it says requesting for authentication, authentication failed, it doesnt ask me about user name and password.

can any body help me if he knows about this issue?

regards

‹ Checkout Laptops

Basic Policy Requested ›

Flag as offensive Subscribe post **0 points**

Comments

Dears again new update on

On January 9th, 2008 **Aghiad Boukai** says:

Dears
again new update on this issue, if i want to use ACS , could this works?
and do you know what is the mechanism for this authentication?

thanx in advanced

reply Flag as offensive **0 points**

Dears sorry for being late,

On December 13th, 2007 **Aghiad Boukai** says:

Dears
sorry for being late, actually i was loosing the IP because there was another software which was trying to do configuration.
i stopped that one and now i'm working fine
thanx colin, patrick for help

regards

reply Flag as offensive **0 points**

Got it working?

On December 13th, 2007 **Patrick Tierce** says:

Just curious if you have it working now or not. If so, what'd you end up doing?

reply Flag as offensive **0 points**

dearattached is the immages

On January 9th, 2008 **Aghiad Boukai** says:

dear
attached is the immages which shows that i need to creat new connection,
now after i get one single sign on , i loose my ip after arround one minute, till i do reconnect the odyysey.
did you face this b4?
regards

reply Flag as offensive **0 points**

thanx for your help i'm

On December 9th, 2007 **Aghiad Boukai** says:

thanx for your help
i'm trying this, but it's not logging me on.
in the main Novel login page, there's 802.1x tap , there's two option
-login using odyssey client
-strip user name from user name.

this inforce me to creat new connection.

one more doubt, you told me to change from sitting, which sitting exactly you are talking about.
regards

reply Flag as offensive **0 points**

LDAP + Novell + Encryption + No Radius Server

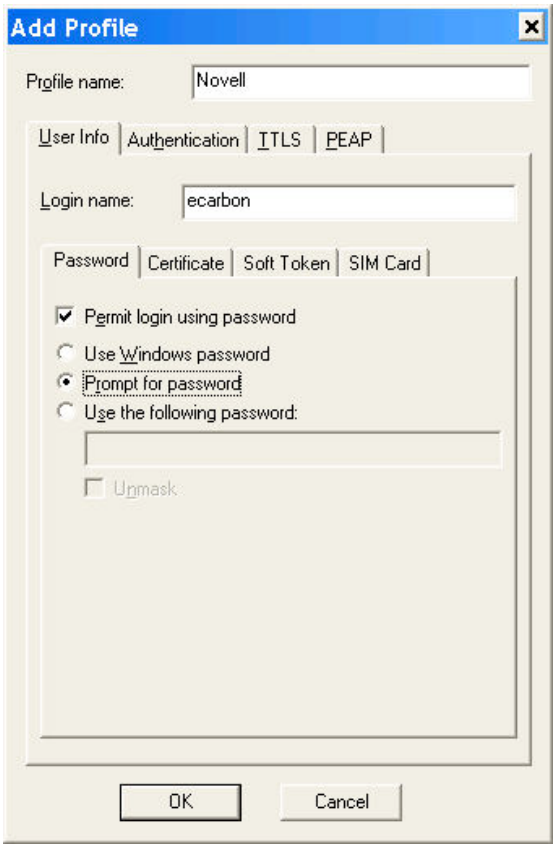
On November 27th, 2007 **Colin Joseph** says:

Aghiad,

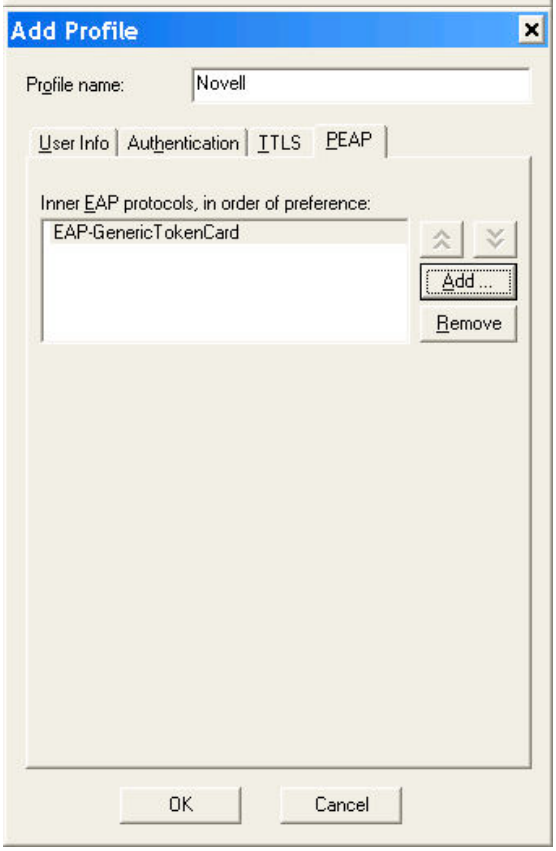
If you have an Aruba 2400, you do not need a radius server. This is what you need to do:

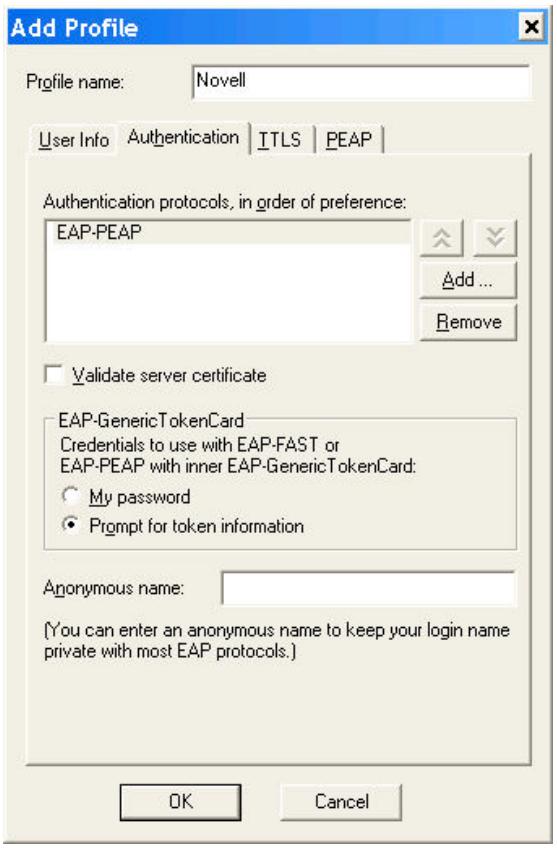
1. Setup an LDAP server on the Aruba Controller and test authentication to make sure it works under the "Diagnostics" tab.
2. Setup and SSID on the Aruba with your encryption
3. For 802.1x on that SSID, configure the Aruba 2400 to use "Termination" and use "EAP-GTC" as the Inner EAP Type
4. For the Odyssey Client, in your user profile, under the Authentication Tab, user EAP-PEAP for Authentication Protocol
5. For the Odyssey Client, in your user profile, under the "PEAP" tab use EAP-GenericTokenCard" for the Inner EAP Protocol
6. For the Odyssey Client, in your user profile, under user, enable "Permit Login using password" and "Use Windows Password"
7. Stop here and ensure that your client can authenticate using the profile that was setup.
8. Under Odyssey Client Administrator > Initial Settings, setup a profile with exactly the same thing as Steps 4 through 6.
9.. Under Settings> Windows Logon Settings check "Override Windows Logon Settings". Ensure that "Use Odyssey to Connect Prior to Windows Logon" is checked. Ensure that your wireless adapter is selected here.
10. Make sure that "Prompt to Connect" On Connection Failure is also highlighted, as well.

If you don't get single sign




Add Profile
Profile name:
Novell
User Info
Authentication
TTLS
PEAP
Login name:
ecarbon
Password
Certificate
Soft Token
SIM Card
Permit login using password
Use Windows password
Prompt for password
Use the following password:
Unmask
OK
Cancel


Add Profile
Profile name:
Novell
User Info
Authentication
TTLS
PEAP
Inner EAP protocols, in order of preference:
EAP-GenericTokenCard
Add...
Remove
OK
Cancel



edit reply **0 points**

thanx, i'll try it and i'll

On November 21st, 2007 **Aghiad Boukai** says:

thanx, actually i have no SBR and no radius server i'll try again tomorrow and i'll update you, by the way here is my email, if you have any capture plz send it to here
boukai@oxygen-me.com

regards

reply Flag as offensive **0 points**

Novell here too

On November 21st, 2007 **Patrick Tierce** says:

We have multiple agencies who we support that do exactly what you're trying to do. It's fairly involved, but very possible to do it. Here's a quick summary.

1. Yes, you need Odyssey OR the FREE SecureW2 TTLS-based client. We opted to use SecureW2 (http://www.securew2.com) everywhere. It works great, and allows "pre-logon" for the machine so you don't have to logon like you're describing. That way you can run all of your machine scripts and the user login script runs too when they logon.
2. We run Juniper SBR GEE and direct the EAP requests to another downstream SBR server which actually does the LDAP query against the Novell Enterprise server (runs LDAP against the Enterprise directory in Novell, but you knew that already).
3. You MUST grant proper permissions to the E-Directory in Novell or it won't work! It's the "trustee" rights you have to allow on the whole E-Directory.

4. The SBR server does it a bit "odd" in that it does a global "find" of the user first in E-Directory, then it just tries to logon to E-Directory with the user-supplied credentials. It it works, then the user must be "okay" with their userid/password. Had to do a packet trace to figure that one out... NOT fun.
5. Configure the Odyssey or SecureW2 client accordingly. I'd be happy to give electronic screen prints so you can see how we do it here if you'd like.
6. Pass back some value from the SBR server so the controller knows what role to assign. We use "Reply-Message" RADIUS attributes.

Just a note that you'll have to (from what I've heard) use TTLS for the EAP auth process.

Hope this gets you started. Let me know if you need more info.

reply Flag as offensive **1 point**

Post new comment

Your name:
Colin Joseph

Subject:

Comment: *

Web page addresses and e-mail addresses turn into links automatically.

Allowed HTML tags: <a>   <cite> <code>   <dl> <dt> <dd> <img>

Lines and paragraphs break automatically.

More information about formatting options

File attachments

Preview comment Post comment

Back to top