

Install CA and Setup Wireless Connection in the Wireless Client

This is the third document in a series of 3. First Use the document Lab Setup, then Domain Controller, and finally WAP Enterprise

We have two steps:

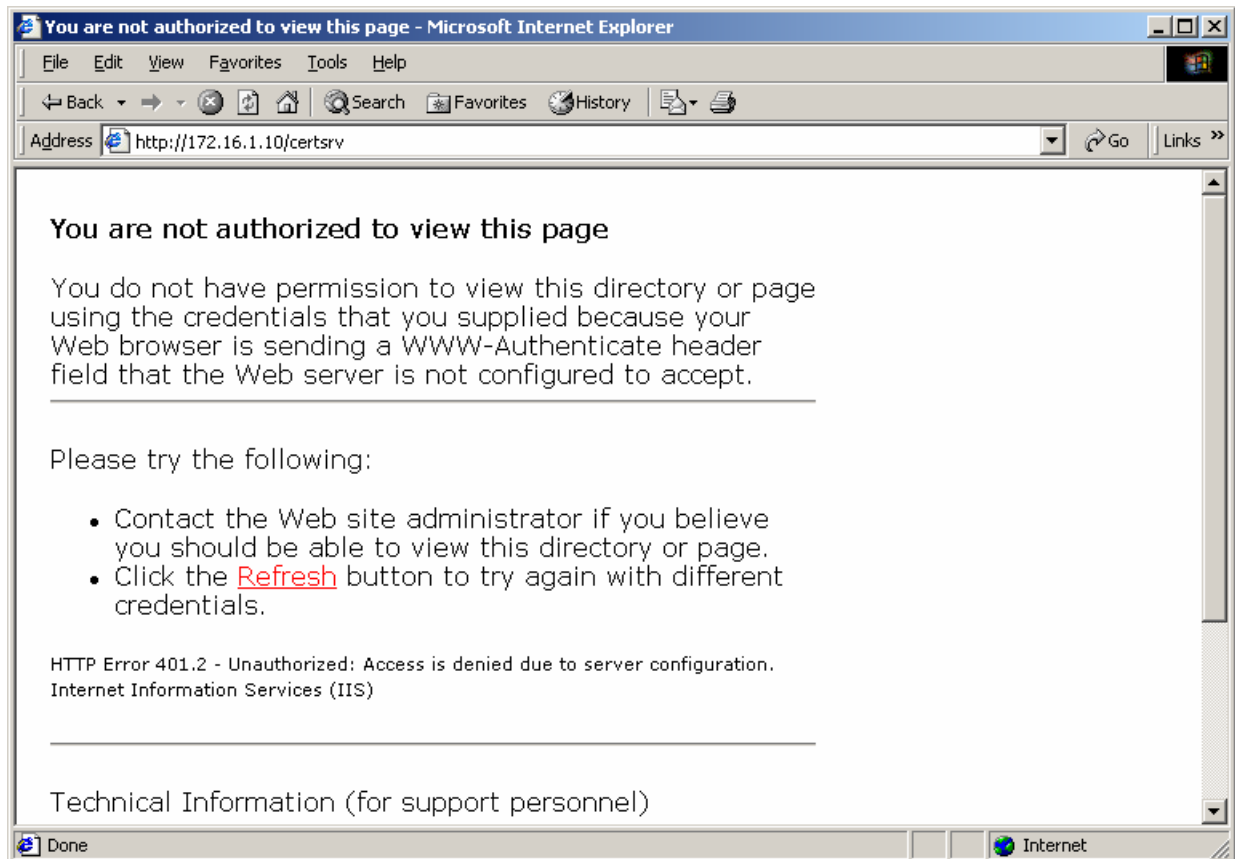
- Install the CA certificate on the IAS server into the wireless client, and
- Setup the wireless connection in the wireless client.

The configurations of the AP are done as part of the Lab Setup document.

1. Installing the CA in a Wireless client

1.1. Connect to the IIS server URL

1. Start Internet Explorer
2. Enter in the Address box the URL: `http://<server_name or IP address>/certsrv`.
In our scenario the IP address is 172.16.1.10

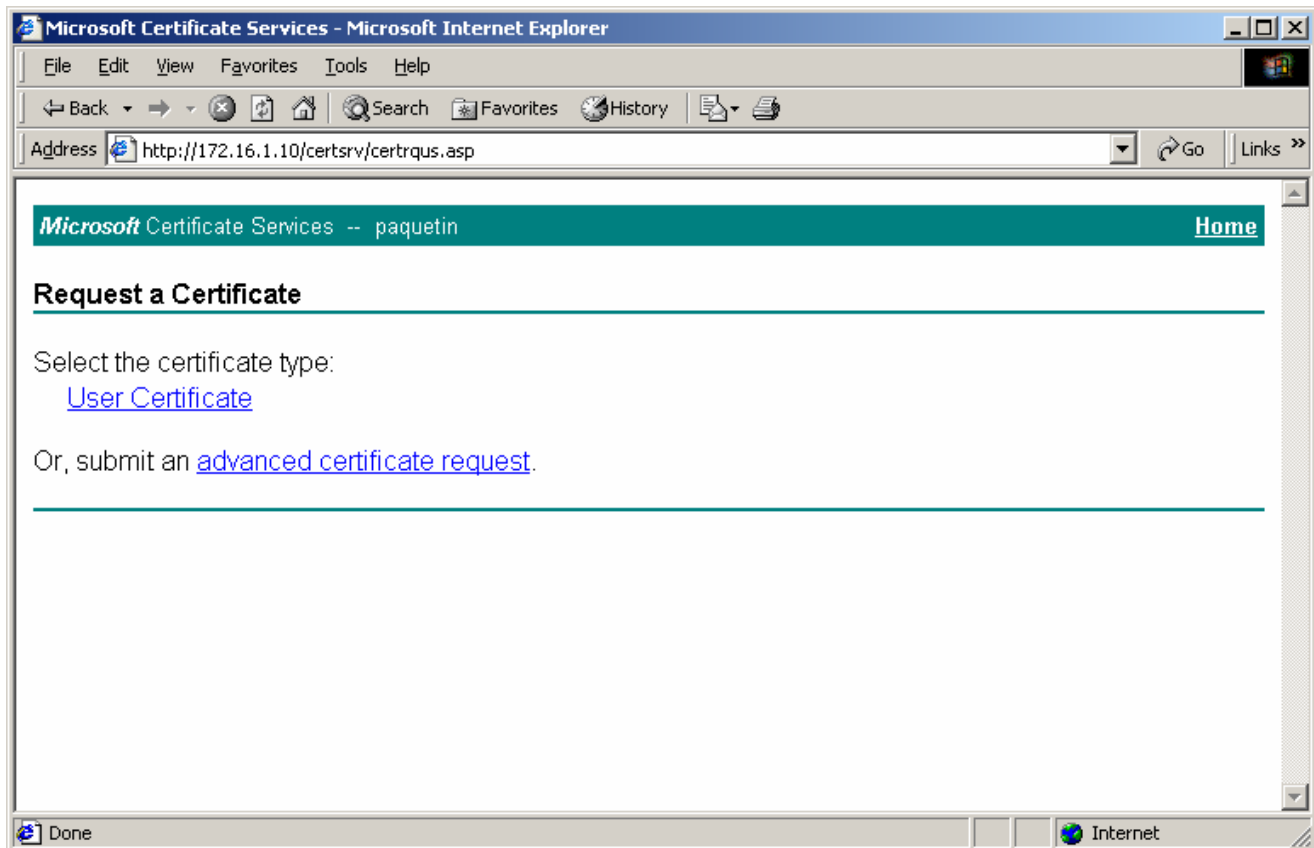


3. As soon as you connect, the Enter Network Password window displays, as show on the next page.



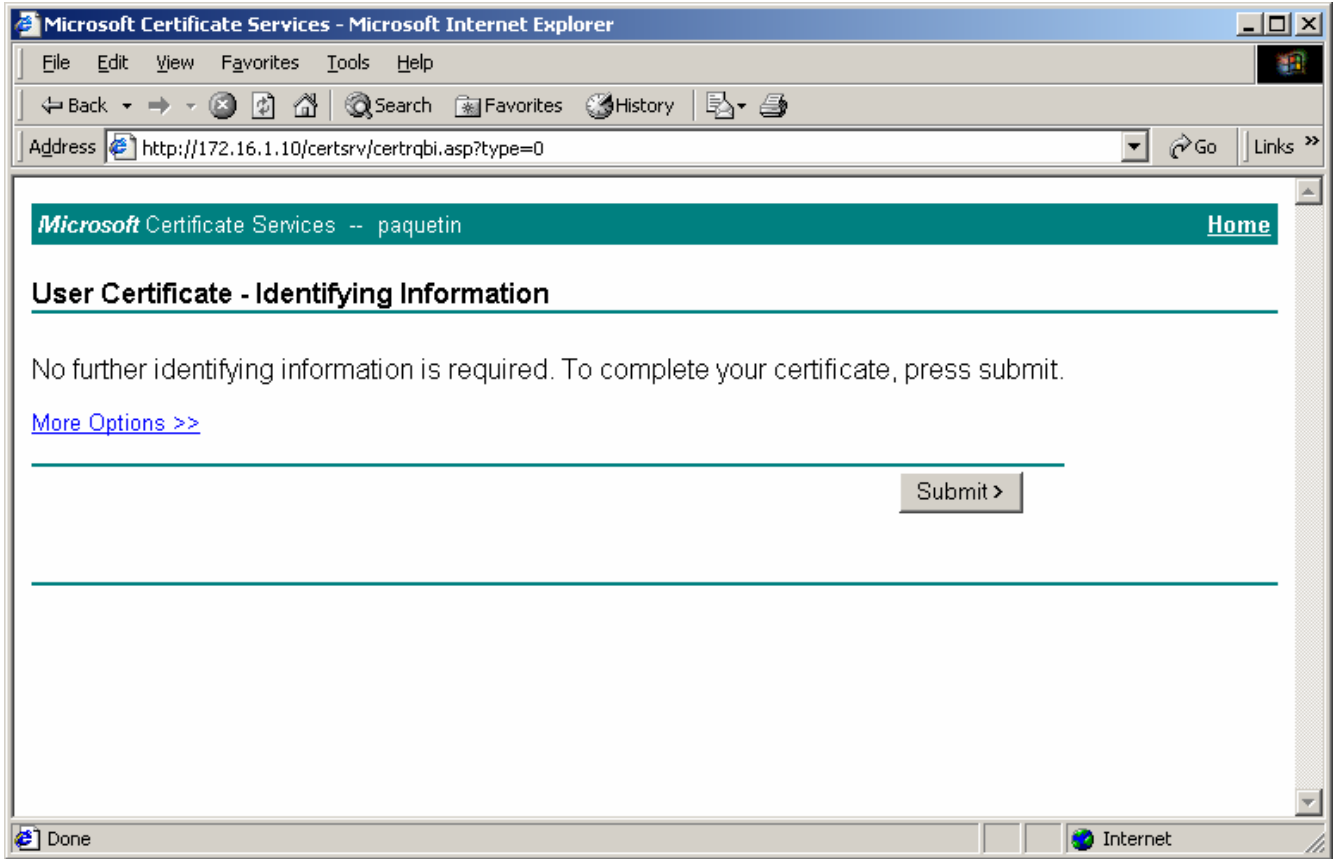
4. Enter the same username and password combination that was established in the Domain Controller document.

The Microsoft Certificate Services page displays



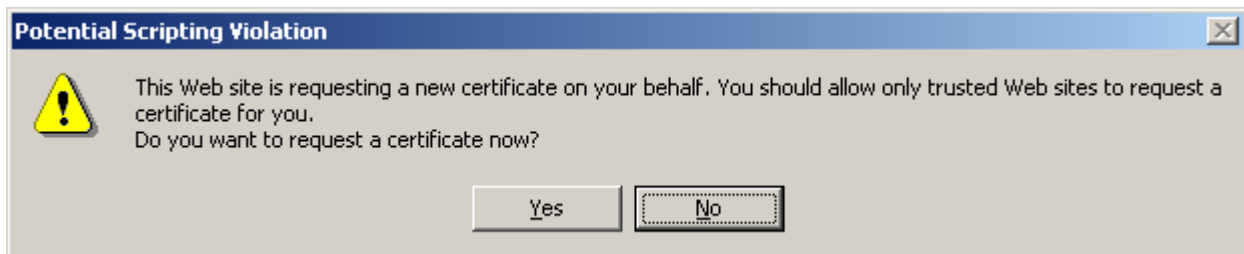
5. Click the link User Certificate
You might be requested to download an Active C control. Allow it.

The User Certificate Identifying Information page displays



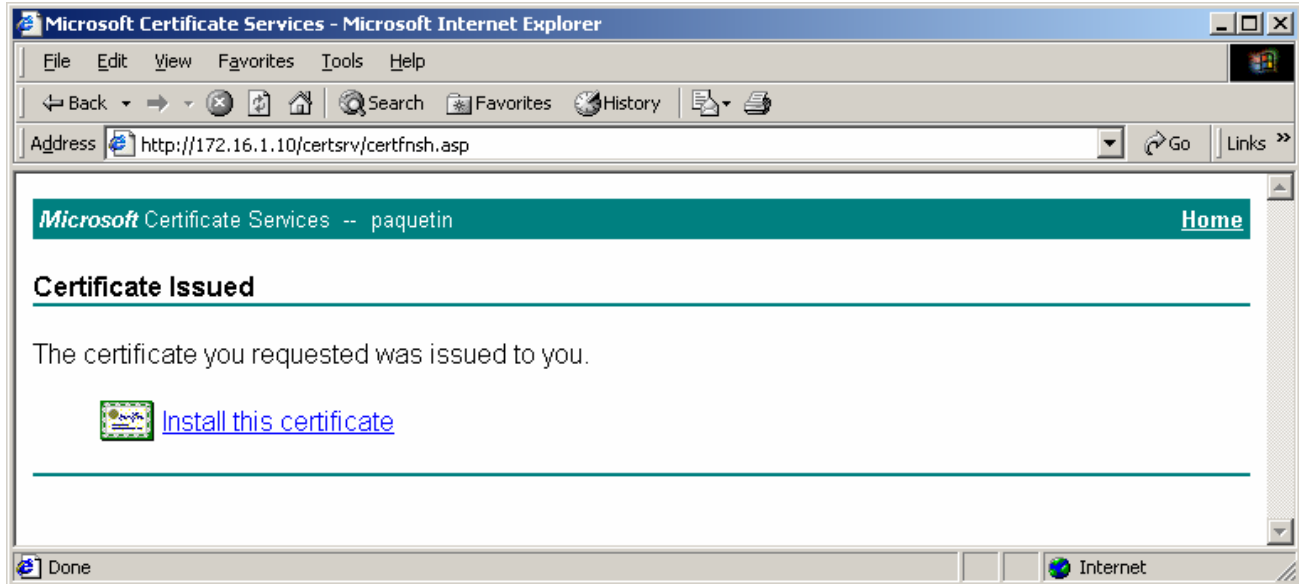
6. Click Submit

The Potential Scripting Violation Alert Box displays



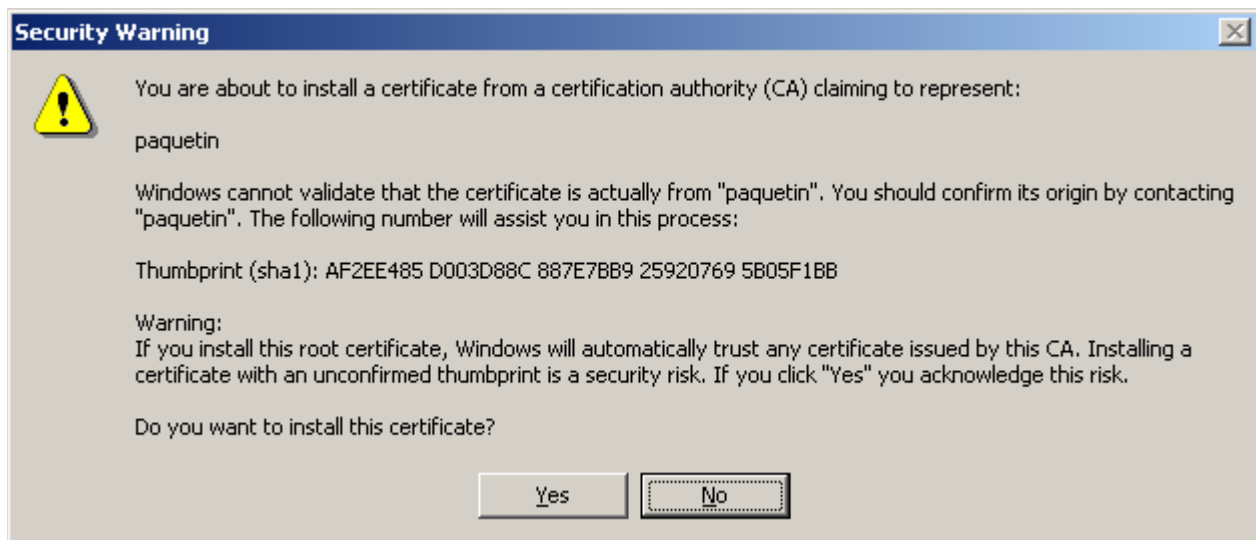
7. Click Yes

The Certificate Issued page displays



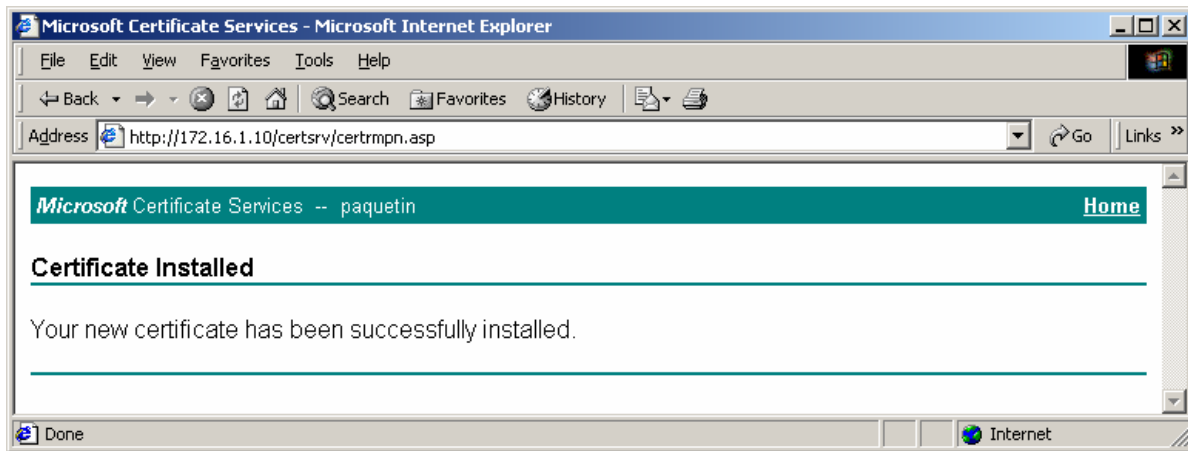
8. Click the link Install this certificate

The Security Warning Alert Box displays

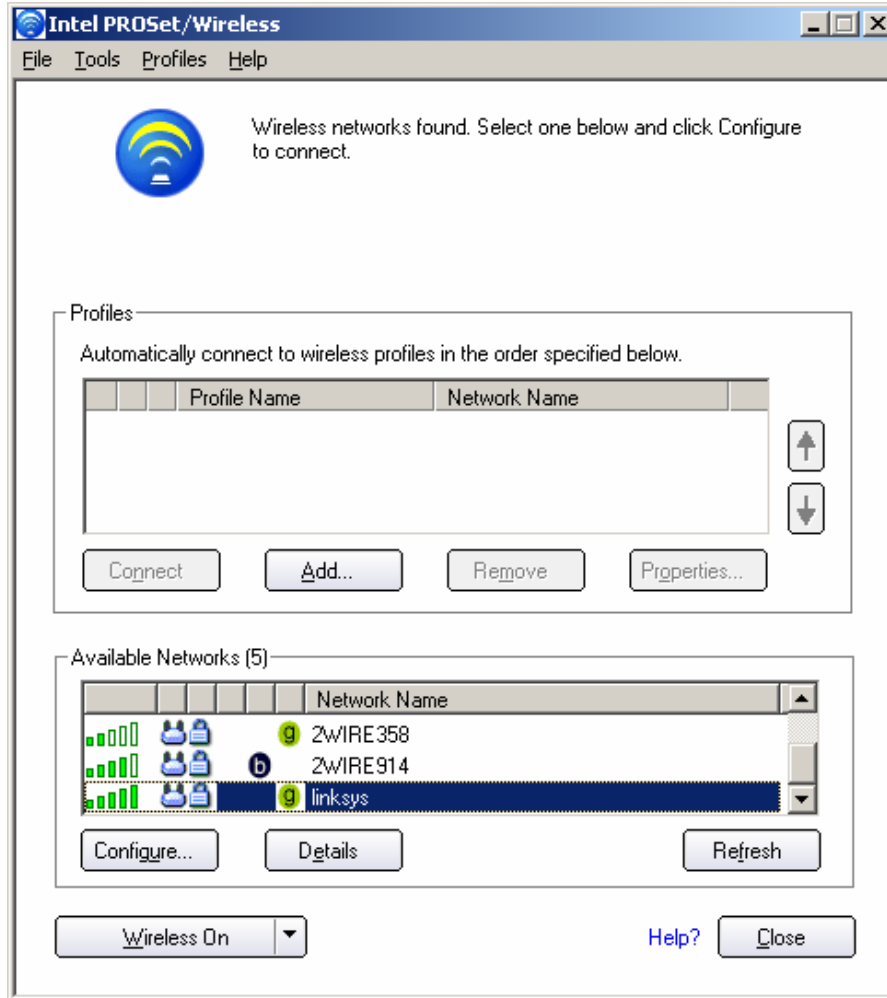


9. Click Yes

The Certificate Installed page displays



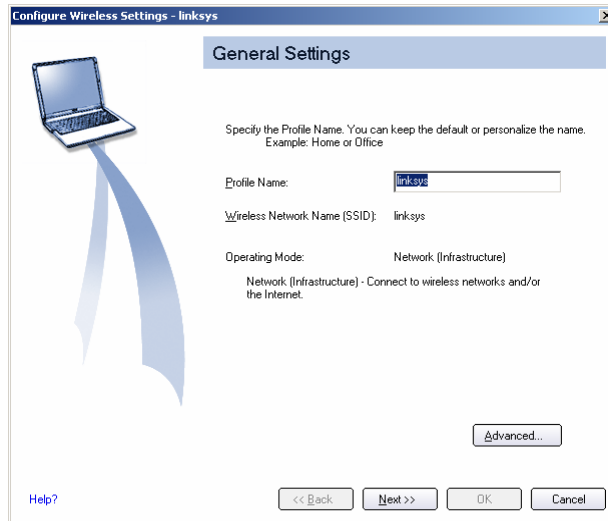
2. Setting up the wireless client



The Linksys router shows in the list.

1. Select it
2. Click Configure

The Configure Wireless Settings - linksys window displays



- 3. Click next

The Security Settings window displays



- 4. Click next

The next Security Settings window displays

Configure Wireless Settings - linksys

Security Settings

Select the appropriate security settings for your wireless network. Your network administrator can help with these settings.

Network Authentication: WPA - Enterprise

Data Encryption: AES - CCMP

Enable 802.1x

Authentication Type: PEAP Cisco Options...

Step 1 of 2 : PEAP User

Authentication Protocol: MS-CHAP-V2

User Credentials: Use the following

User Name: laptop

Domain: bringsjoy.com

Password: *****

Confirm Password: *****

Use a Client Certificate on this wireless network Select...

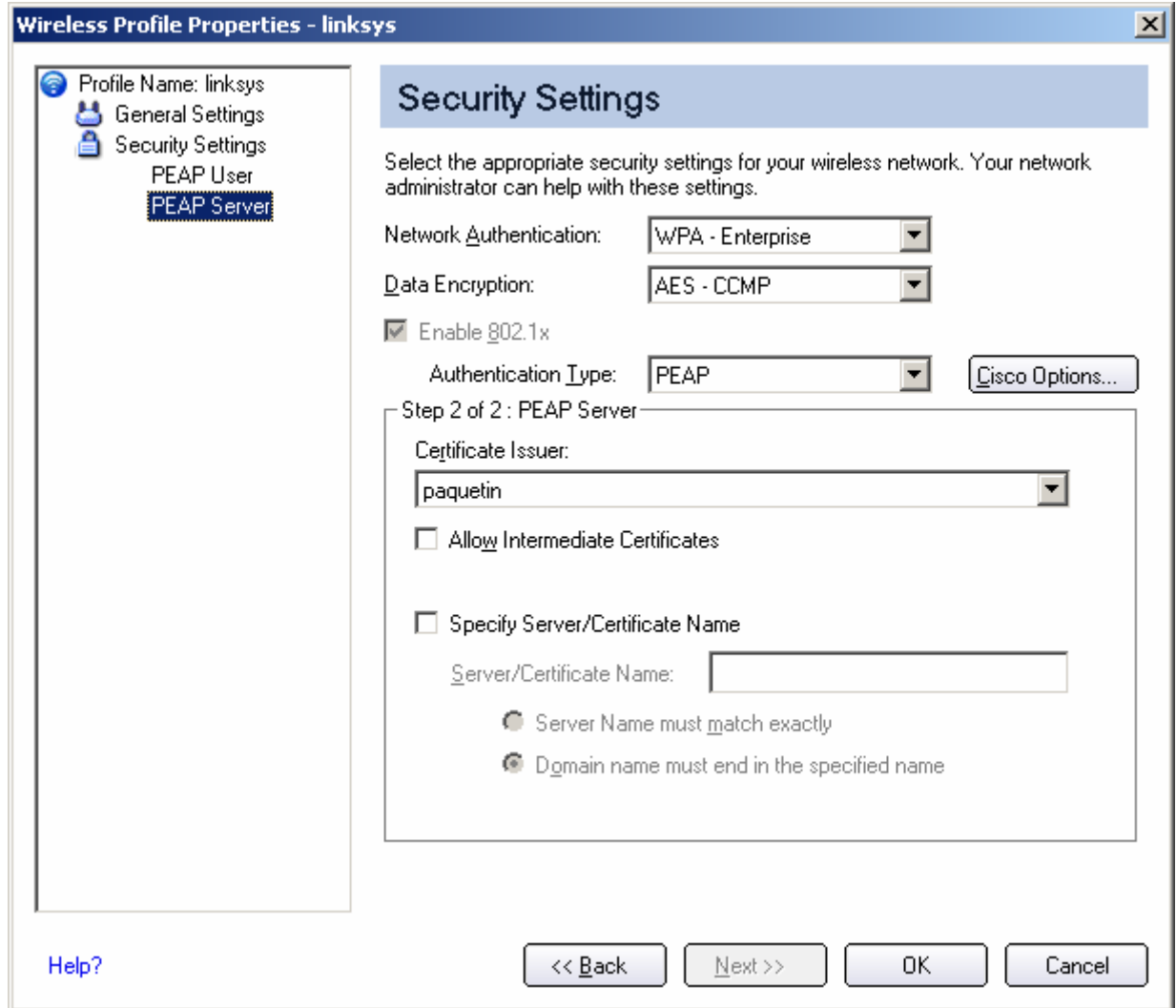
Roaming Identity: laptop

[Help?](#) << Back Next >> OK Cancel

The particular setting on this configuration is the Roaming Identity. It will be transmitted too, it should match the username.

5. Click Next

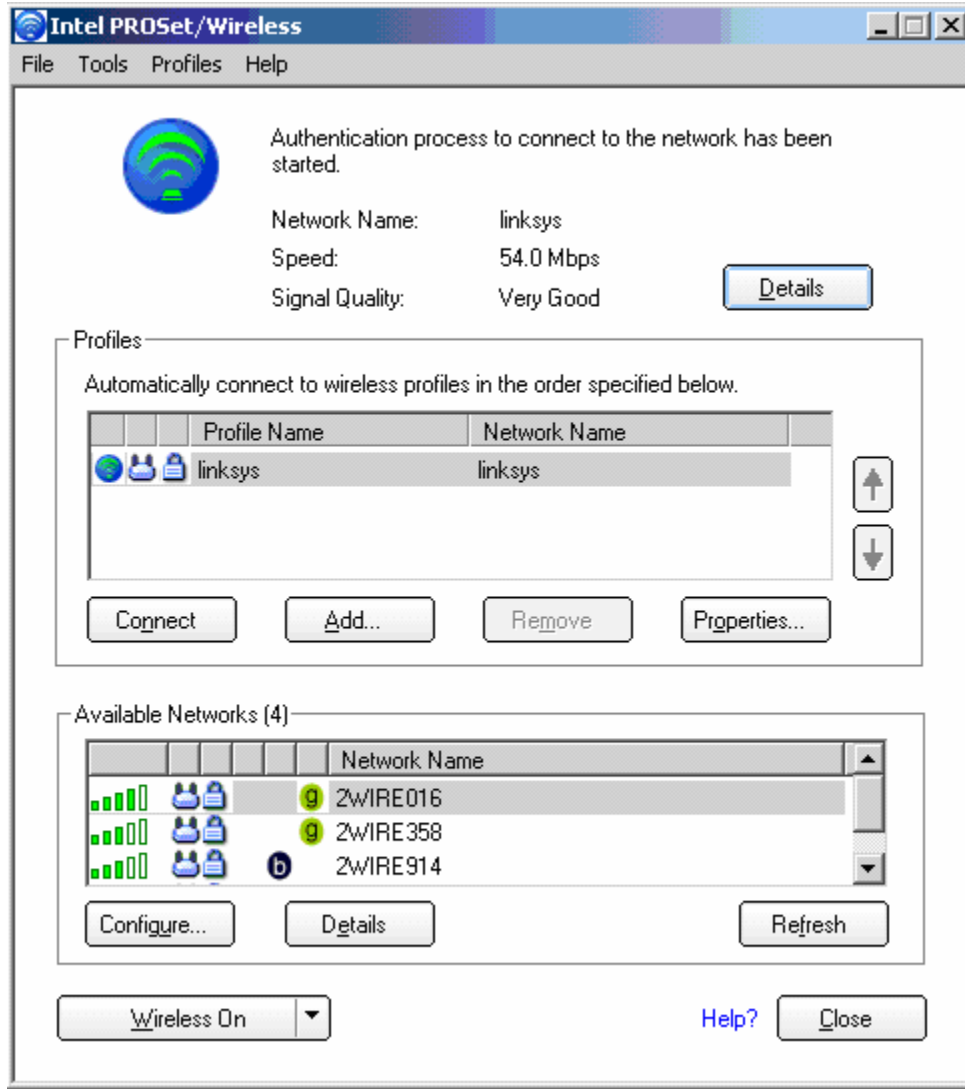
The next Security Settings window displays



Although in the screen above the Certificate Issuer paquetin is selected, it is not critical; the default option [Any trusted CA] is enough. This is done to show that the first step of installing a certificate was done OK. If our certificate issuer does not appear on the list, we need to start troubleshooting.

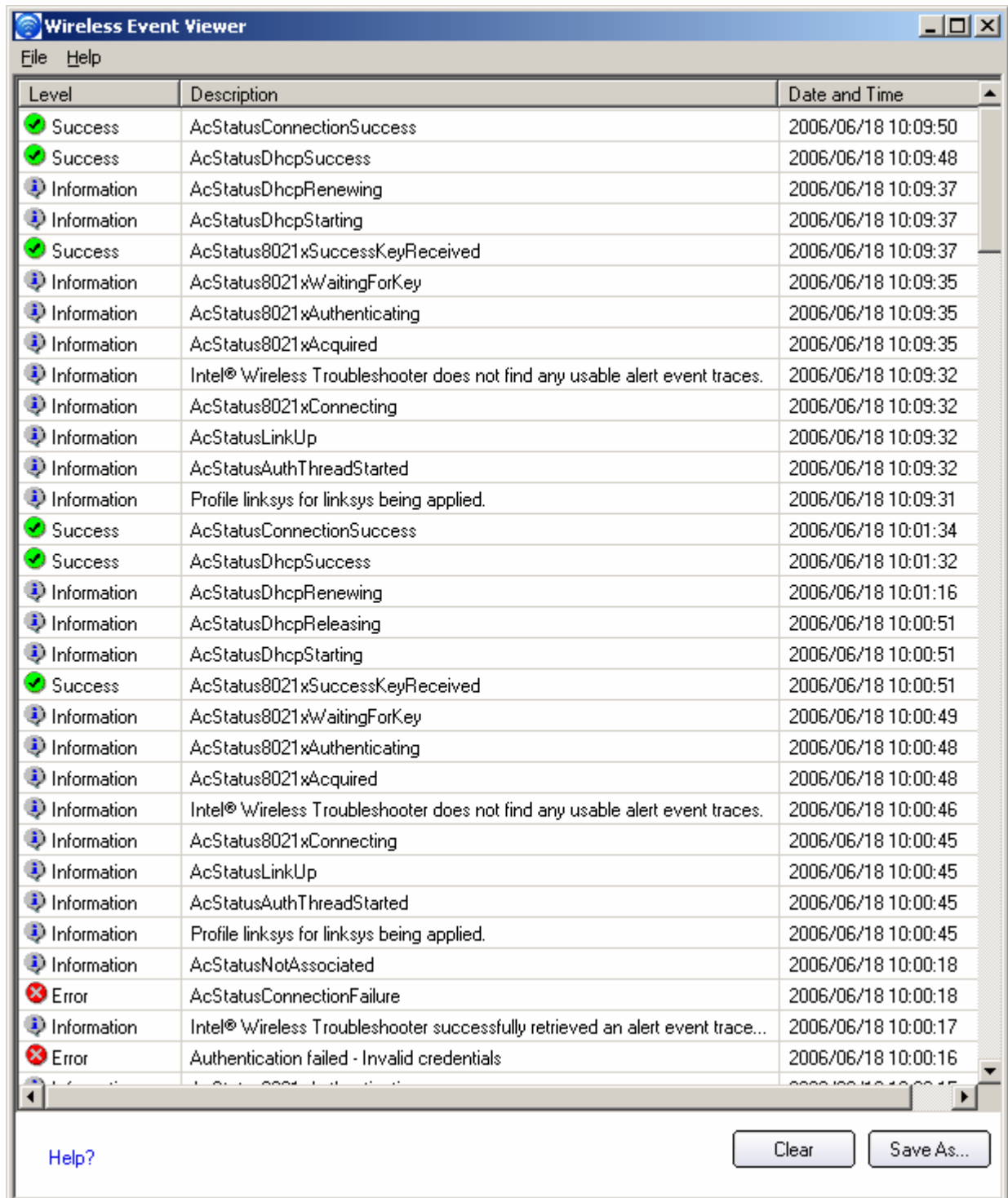
6. Click OK

The Intel PROSet/Wireless window displays



In our scenario, the window shows that the authentication process has started. It will take less than 30 seconds.

The Wireless Event Viewer window displays



This is the log that shows all the messages as the system authenticates. Notice all the individual steps. We are done!!!!