



Internet access system through the Wireless Network of the University of Bologna

Printable service summary document: the updated version is available online at the following address <http://www.unibo.it/almawifi>

A WPA security access system has been implemented on every access point according to the requirements of WI-FI Alliance, which guarantees complete encryption of all the traffic flows. In more detail, the WPA system has been configured with TKIP and EAP (IEEE 802.1x) standards, where active directory users of the University DSA are validated by a centralized Radius Server.

We remind you that user credentials should be activated by setting a personal password via the following website <https://www.dsa.unibo.it>

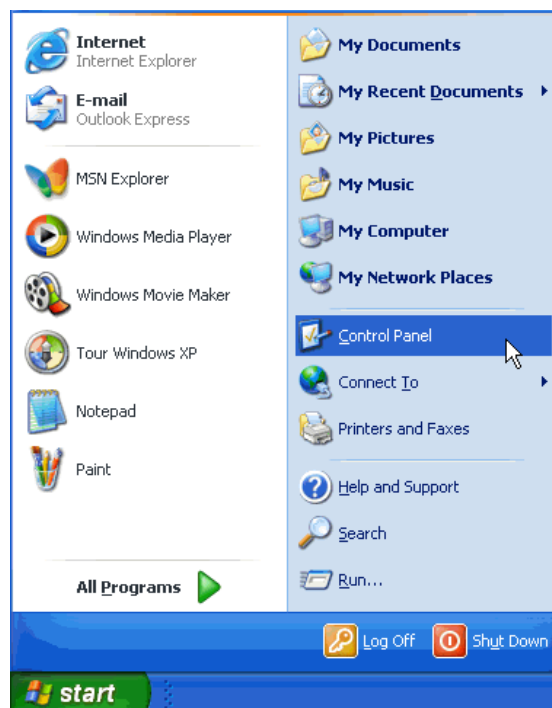
For further information about connection problem please consult FAQ ALMAWIFI at <http://www.unibo.it/almawifi>

Client configuration using Windows XP

The operating system must preliminarily be patched by installing the Service Pack no.2 in the machine, which includes the update for the management of remote connections.

A new Internet connection must be configured on the basis of the parameters listed here below, which are described here in a step-by-step manner .

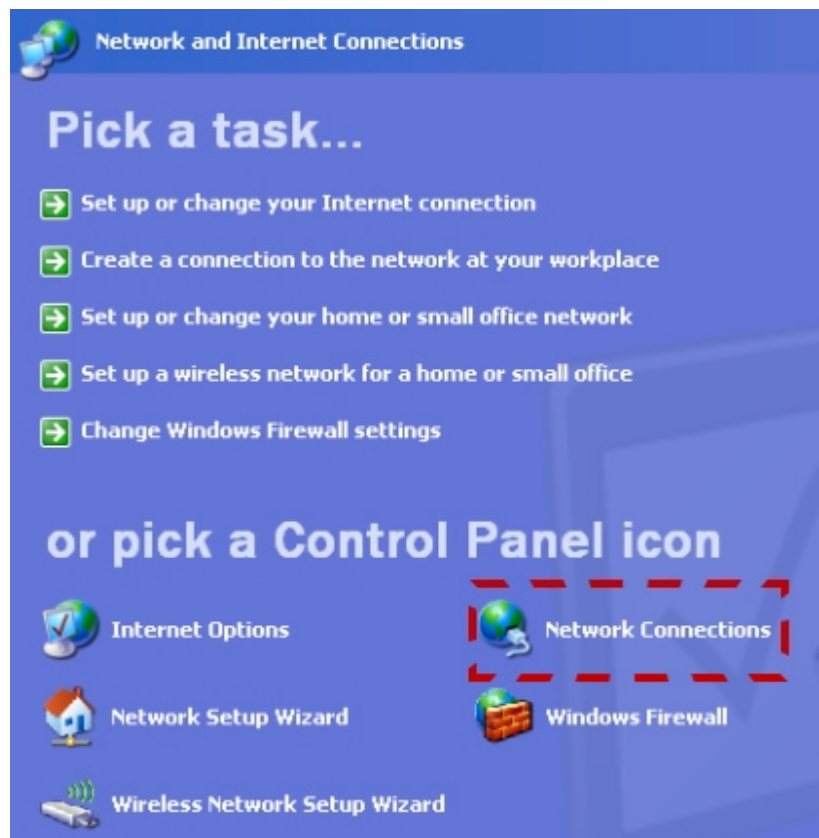
Click **START** and **Control Panel**:



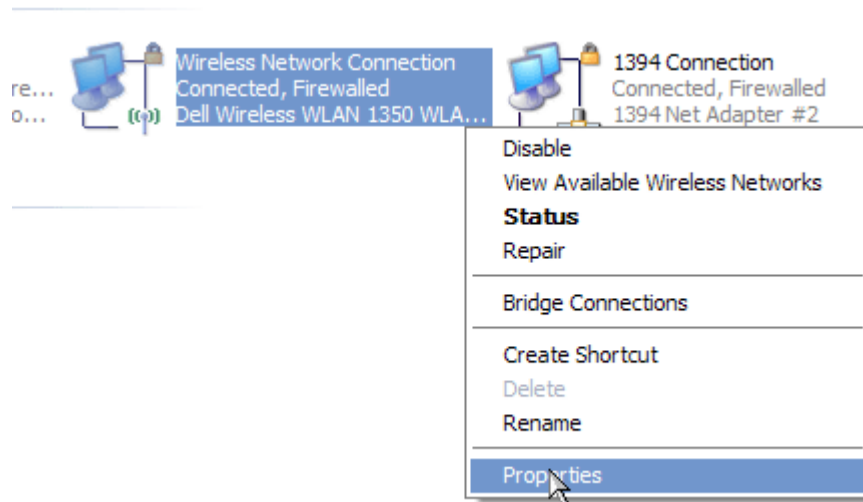
Click on the icon that says **"Network and Internet Connections"**:



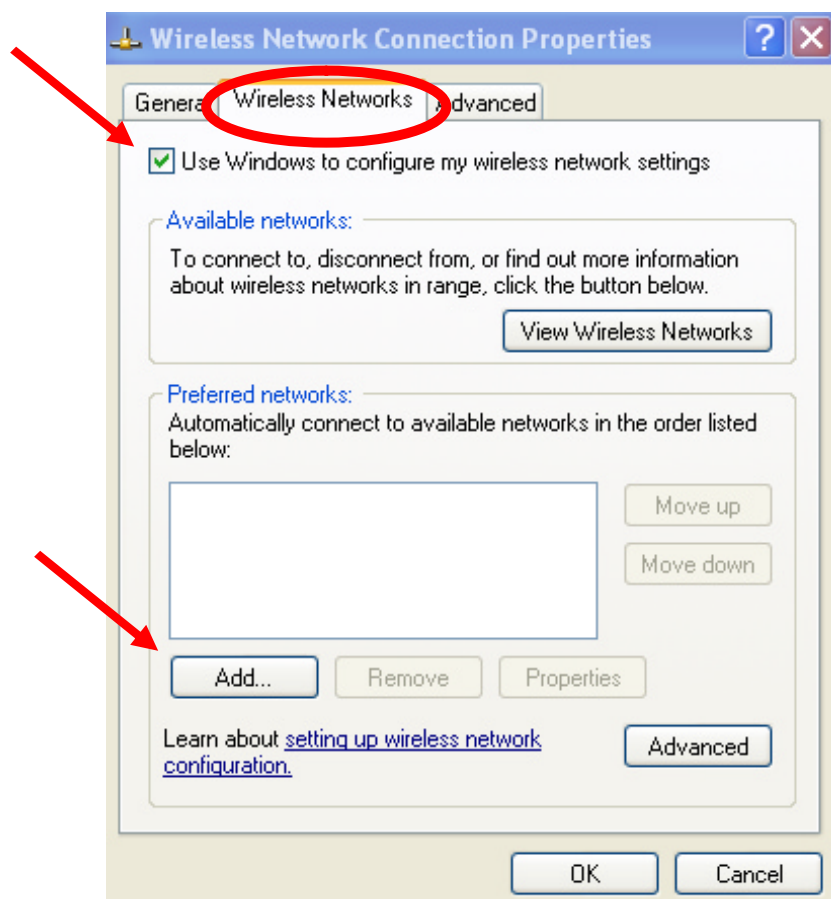
Once you are in there. Click on the icon that says **"Network Connections"**:



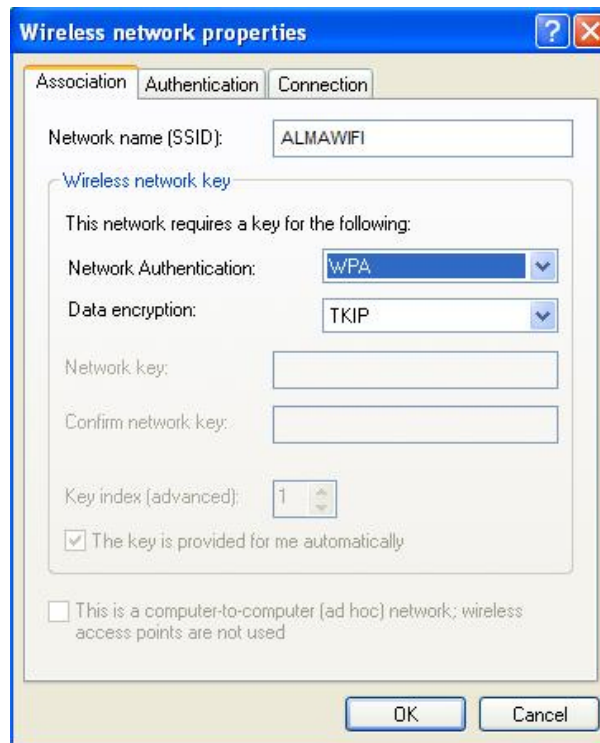
Now you will find your network cards listed here. You will need to right click on the card you want to enable file sharing. Select the properties menu Click on the icon that says **Wireless Network Connection**:



Click on **Wireless Networks**:
Verify the selection **“Use Windows to configure my wireless network settings”** is checked.
If in the box **“Preferred Networks”** click on **“Add”**.

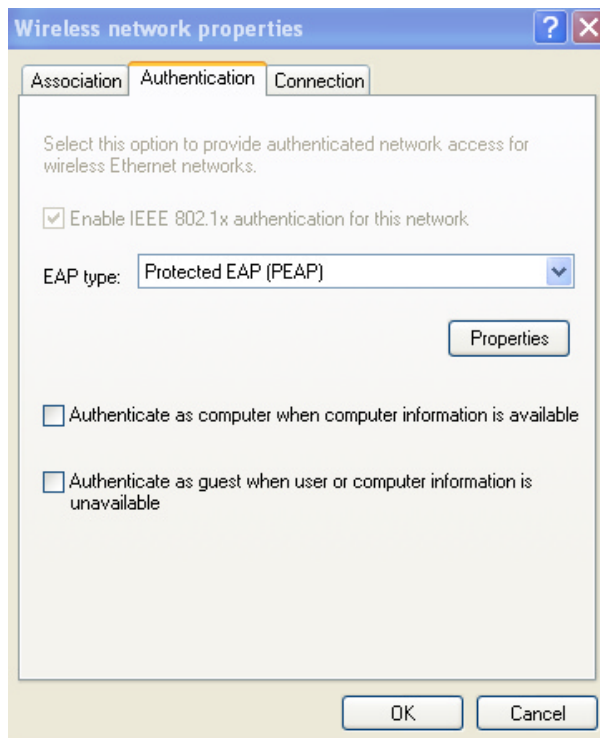


Verify the selection “Use Windows to configure my wireless network settings” is checked.
If in the box “Preferred Networks” the SSID **ALMAWIFI** already exists select it and click **Properties**
If does not appear Click on “Add” and complete the fields as shown in the picture below:



Set Network name (SSID) to **ALMAWIFI**, Network Authentication to **WPA** and Data encryption to **TKIP**.

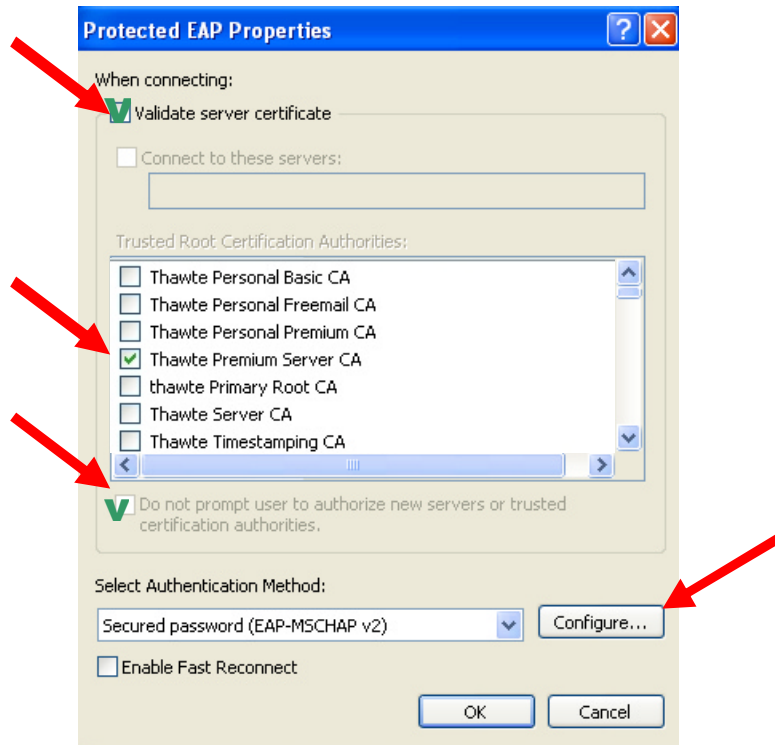
Click on “**Authentication**” and select the **ProtectedEAP (PEAP)** from the list of EAP type as below and the following options:



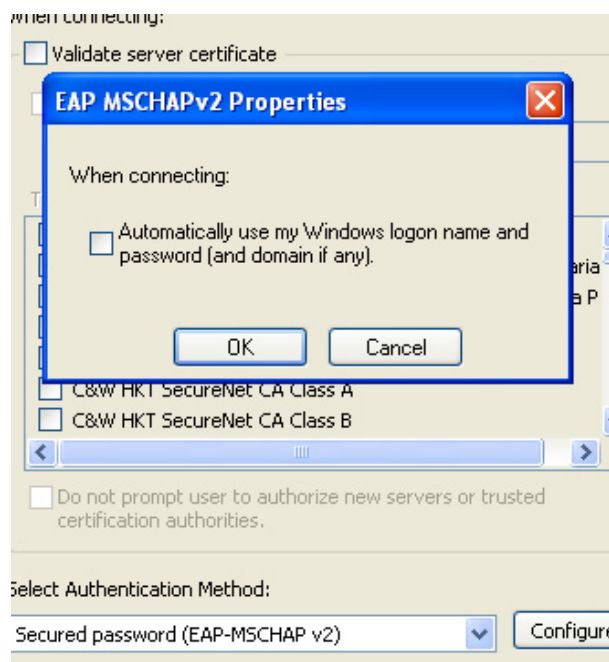
Note : "Enable IEEE 802.1x authentication for this network" will be ticked but grayed out.

Then click on "**Properties**" and fill in the fields required as below:

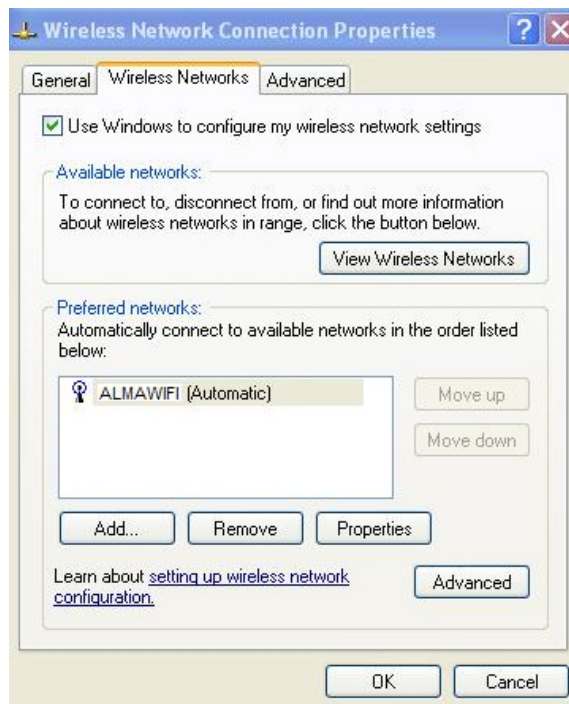
- select "**Validate server certificate**" if unchecked;
- select "**Thawte Premium Server CA**";
- check **Do not prompt user to authorize new servers or trusted certification authorities**
- select **Secured password (EAP-MSCHAP v2)** from the list of Authentication methods. Deselect "**Enable Fast Reconnect**";
- select **Configure**.



Click on "Configure" and deselect "**Automatically use my Windows logon name**":



After giving your **OK** for the **EAP MSCHAPv2 Properties** and click **OK** for the **Protected EAP Properties**, your PC screen page will appear as below:



To close the screen page click on **OK**.

The system will activate a dialogue balloon will appear in the systems tray prompting the user to **Select a certificate or other credentials**. By clicking on this dialogue balloon, a pop-up is opened where your USER ID and PASSWORD must be entered, as well as the domain; the User ID and the Password to be entered are the ones provided for registration to the Active Directory of the University, typically "name.surname". The domain is PERSONALE for staff of university, STUDENTI for students of university.



PERSONALE for staff of University
STUDENTI for students of University

Note : If Windows taskbar balloon-tips have been disabled, then you will not see the balloon. You will need to click on the wireless network icon in the taskbar to obtain the login window.

After this step, your credentials are checked via a remote Radius Server and, if the data provided are correct, the access is validated and an IP address is provided by a DHCP local server. From this moment on, validation is automatically performed by the operating system at every connection and the credentials need no longer be entered.