

Access to Public Wireless Facilities at ISSI

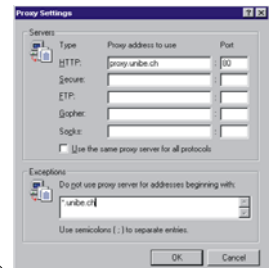
General Information

In order to have access to the wireless or plug-contact access points you need to own a **user credentials** (i.e. a combination of userid and password) issued by the IT service department of ISSI. As a staff member of ISSI you already have an account which is usually the one you use when logging into your Desktop. As a registered member of an official congress, team or workshop held at the ISSI you will get a temporary account during the registration process. Please keep in mind that **this account is for your personal use and is not intended for use by other people**. Be also advised that malicious and illegal use of the infrastructure can be recorded and will be prosecuted.

1st step: connect to one of ISSI's wireless access points: *ISSI_Wireless01* (1st & 2nd floors) *ISSI_Wireless02* (3rd floor)

2nd step: Setting a Proxy in your web-browser, **HTTP ONLY** (necessary for all participants including Ethernet connections). Please setup your proxy before you start authenticating.

IE	Tools → Internet Options → Connections → LAN Settings → Advanced
Netscape / Mozilla	Edit → Preferences → Advanced → Proxies → Manual Proxy Configuration
Firefox 1.x **	Tools → Options → General → Connection settings → Manual Proxy Config.
Firefox 2.x **	Tools → Options → Advanced → Network → Settings → Manual Proxy Config.
Firefox 3.x **	Same as 2 with the exception of manually accepting the certificate when authenticating
Mac Safari	System Preference → Network → Proxies → Web Proxy



HTTP-Proxy: **proxy.unibe.ch** **port 80**
No Proxy for: *.unibe.ch; *.issibern.ch (Internet Explorer) .unibe.ch, .issibern.ch (Mozilla / Firefox)

** Mac users (Firefox only): instead of clicking on Tools, you should click on Firefox and then Preferences

3rd step: Authentication

- **HTTPS:** If you start up your browser, you will automatically be prompted to authenticate. Use your credentials to log in. Please keep in mind that although the authentication itself is encrypted, the subsequent traffic is NOT, i.e. you should not send passwords or other confidential data over this connection (wireless!). **This is the reason why plaintext applications that require authentication (POP, IMAP, Telnet and FTP) to server inside the university campus are not permitted.**
- **VPN clients:** you should only join one of ISSI's wireless access points and then simply open the VPN connection without authenticating to our network.

Possible Problems with HTTPS-Authentication

During HTTPS authentication process you will get a window to confirm the acceptance of the server certificate. It states that the certificate is not a valid one. There is no security concern about that; just accept it and go ahead. Be aware that sometimes this smaller window is hidden behind the authentication window (especially in Internet Explorer), so when the authentication process takes a long time have a look behind the one in front. To shorten the authentication process it is good practice to install the server certificate permanently. *Be aware that the authentication will time out every 4 hours if computer is inactive.*

Settings for eMail

If you can not send any emails from your Email client program, then you should use our Outgoing Mailserver (SMTP) smtp.unibe.ch
Please do use any authentication for SMTP – this does not apply to Webmail users

Finally, if you have any problems, please Contact Saliba: saliba@issibern.ch Phone: 3251