



**This guide is valid for any device running MikroTik OS
Tested on RouterOS 6.x**

To integrate Chillifire Hotspots with a device running MikroTik OS first of all you have to have an account with Chillifire. You can create a free Chillifire account on <http://www.chillifire.net> .

There is nothing special to consider in the setup of the Chillifire account, which you can configure any way you like to, free, pay-per-use, voucher based, online-payment, your own logo, colour scheme etc. Next step is to configure your Mikrotik device.

1) Reset Router to default settings

You need to setup your MikroTik router by using Winbox. Winbox is the graphical user interface for configuring the MikroTik Router OS. You can download [Winbox from MikroTik's website](#). Once downloaded just connect your PC to the MikroTik device via LAN cable to an Ethernet port other than eth1, while connecting the device to the internet on eth1. Click on Winbox to open the programme; it should recognise the Mikrotik device and allow you to connect it.

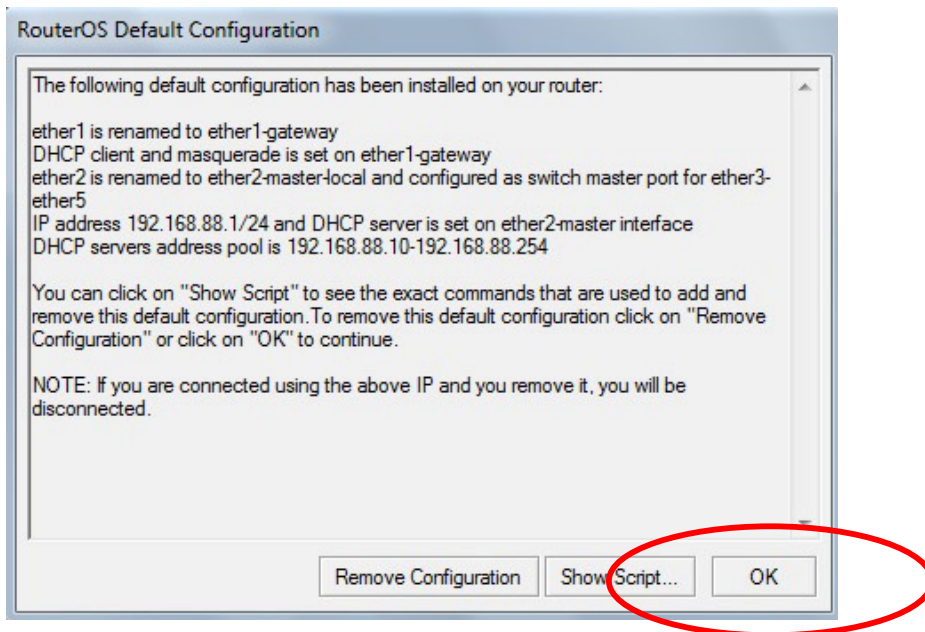
We will assume for the purpose of the setup that all possible RouterOS modules have been loaded. As a minimum the ntp package has to be added to the standard set of packages. Please refer to RouterOS support or forum if you are unsure how to add packages. Here is what your package list should look like (System->Packages):

Name	Version	Build Time	Scheduled
ntp	6.2	Aug/02/2013 10:37:21	
routeros-mipsbe	6.2	Aug/02/2013 10:37:21	
advanced-tools	6.2	Aug/02/2013 10:37:21	
dhcp	6.2	Aug/02/2013 10:37:21	
hotspot	6.2	Aug/02/2013 10:37:21	
ipv6	6.2	Aug/02/2013 10:37:21	
mpls	6.2	Aug/02/2013 10:37:21	
ppp	6.2	Aug/02/2013 10:37:21	
routing	6.2	Aug/02/2013 10:37:21	
security	6.2	Aug/02/2013 10:37:21	
system	6.2	Aug/02/2013 10:37:21	
wireless	6.2	Aug/02/2013 10:37:21	

12 items



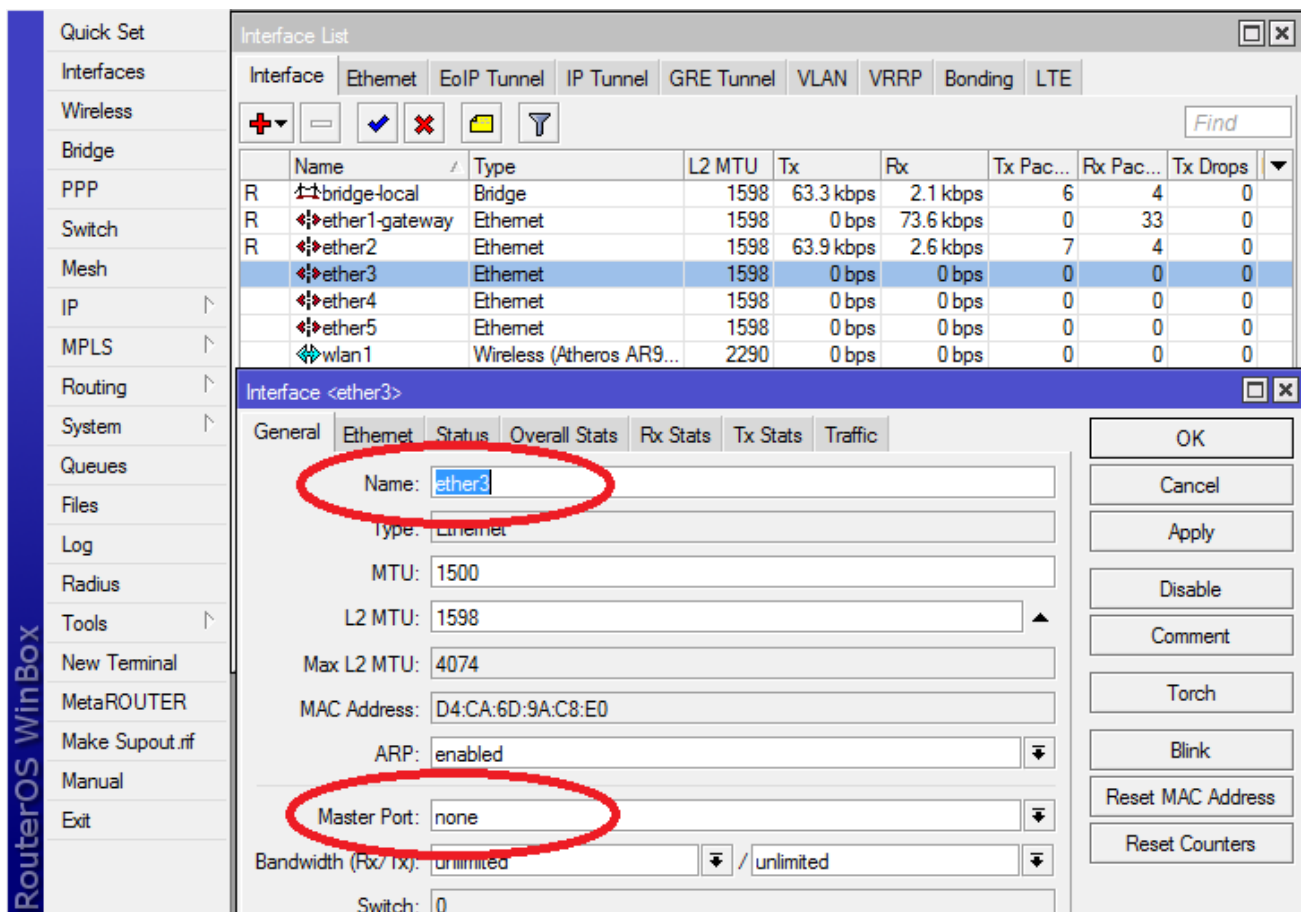
Before starting you **must** reset your router to default configuration. Do that within Winbox at System->Reset Configuration. Even if you reset with the reset button, do perform a software reset afterwards, as it reinstates the default configuration, which gives your router a known starting point. The router will reboot and you need to reconnect. When you see a message about RouterOS Default Configuration press 'OK'.



2) Set up interfaces

Next step is to set up the interfaces and prepare them to receive the hotspot configuration file. We recommend to remove the slave configuration of the Ethernet ports and make them all masters. They can then be individually assigned to either be hotspot controlled or grant free access to the internet. This has the advantage that you can assign, say, Ethernet port#2 to have free Internet access and assign ports #3, #4 and #5 to be hotspot controlled. This gives configuration gives you the continued to access and configure the router using Winbox through a LAN cable connection. When the configuration has been successfully concluded this access will be no longer required, and can be switched over to hotspot control as well, if you wish.

Here is an example for Ethernet port #2, which we have renamed for 'ether3-slave' to 'ether3' and switched 'Master Port' to 'none'. Note that the WAN interface **must** be named ether-1-gateway, the default name.



The screenshot shows the Mikrotik WinBox interface configuration for 'ether3'. The 'Interface List' window is open, showing a table of interfaces. The 'ether3' interface is highlighted. Below it, the 'Interface <ether3>' configuration window is open, showing the following settings:

Interface	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops
R	bridge-local	Bridge	1598	63.3 kbps	2.1 kbps	6	4
R	ether1-gateway	Ethernet	1598	0 bps	73.6 kbps	0	33
R	ether2	Ethernet	1598	63.9 kbps	2.6 kbps	7	4
	ether3	Ethernet	1598	0 bps	0 bps	0	0
	ether4	Ethernet	1598	0 bps	0 bps	0	0
	ether5	Ethernet	1598	0 bps	0 bps	0	0
	wlan1	Wireless (Atheros AR9...)	2290	0 bps	0 bps	0	0

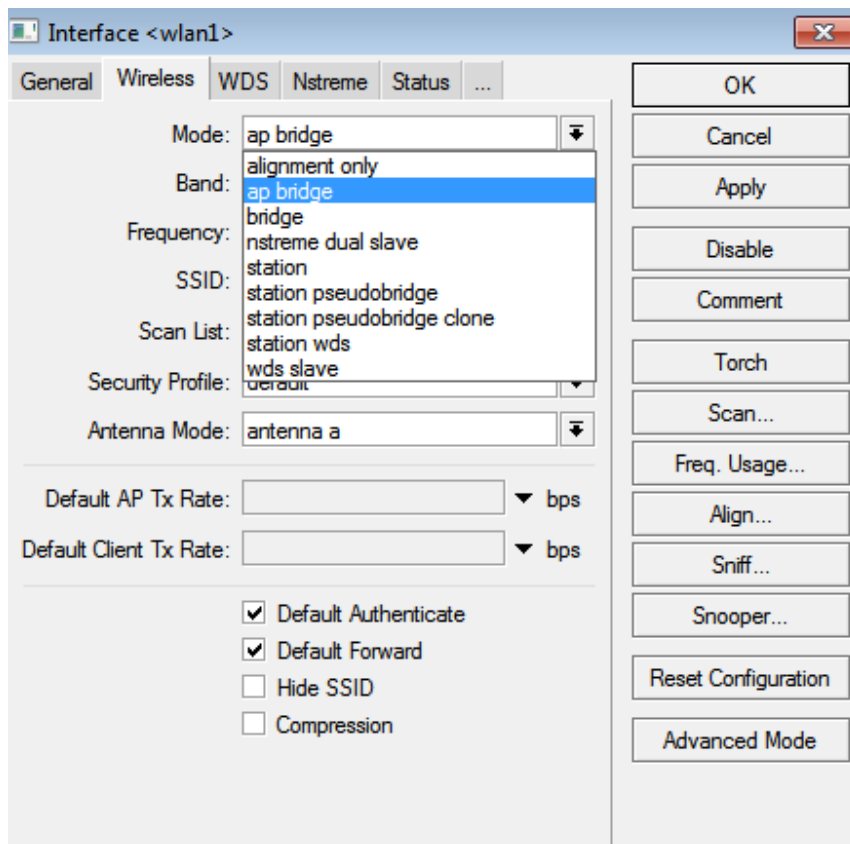
The configuration window for 'ether3' shows the following fields:

- Name: ether3
- Type: Ethernet
- MTU: 1500
- L2 MTU: 1598
- Max L2 MTU: 4074
- MAC Address: D4:CA:6D:9A:C8:E0
- ARP: enabled
- Master Port: none
- Bandwidth (Rx/Tx): unlimited / unlimited
- Switch: 0

3) Wireless interfaces

For devices with wireless interfaces the same principle applies. We recommend to set hotspot controlled WLANs without encryption, and follow the naming convention 'wlan1', 'wlan2', ...

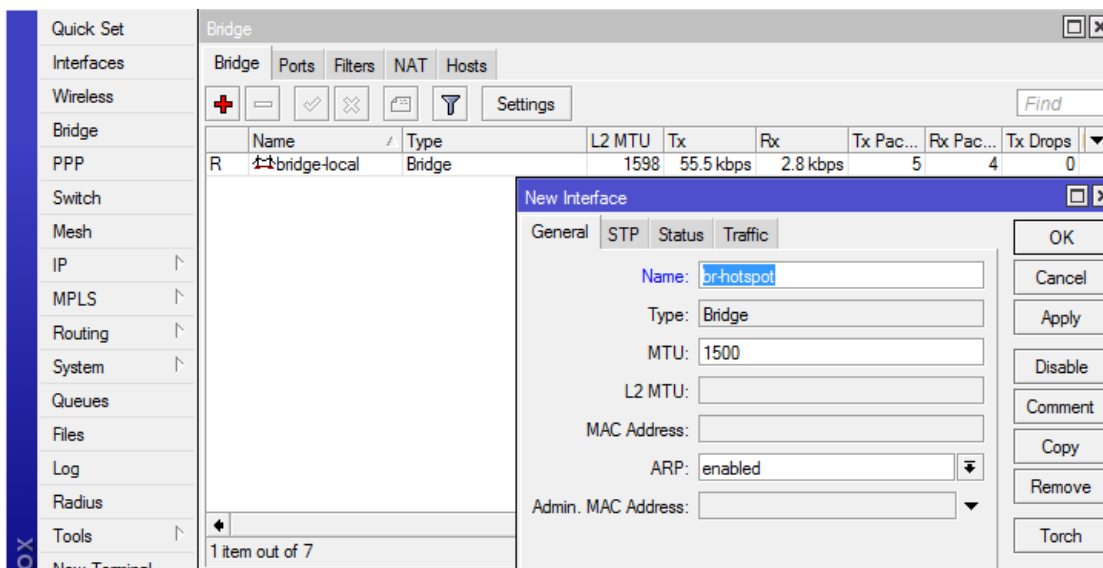
The router wireless interface(s) should be placed in 'ap bridge' mode. Click on Interface, double click wlan1, click Mode: and select 'ap bridge' and make sure the frequency is set to 2.4 b/G.



Please note that for devices with one or more WLAN(s) the default configuration does include a bridge called 'bridge-local'. You can safely ignore this bridge if it is there. Just leave it in place and do not touch it.

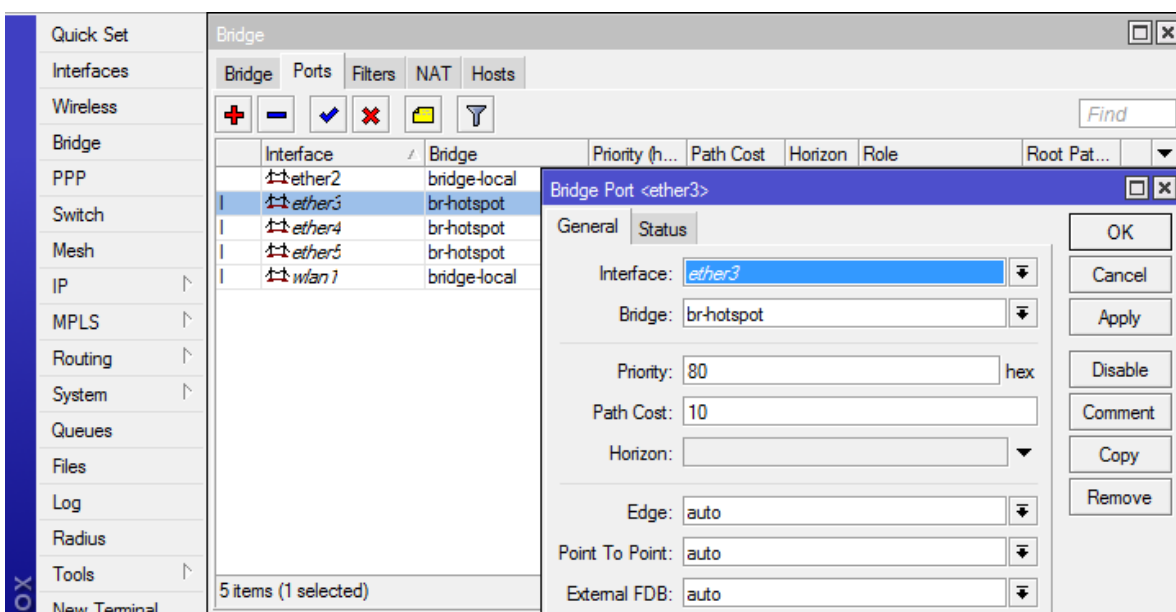
4) Create a hotspot bridge

The next step is to create a bridge, which **must** be named **'br-hotspot'**. We will use the bridge to assign the relevant Ethernet ports and WLANs to the actual hotspot configuration. We can only assign the hotspot configuration to one interface, but the bridge configuration allows us to bundle Ethernet and wireless into one entity, the bridge, which we can then assign to the hotspot configuration. Here the example:



And by clicking on the 'Ports' tab we can assign those interfaces to the bridge we just created. In this example we have assigned Ethernet ports #3, #4 and #5.

Of course wireless WLANs can also be assigned to the bridge.



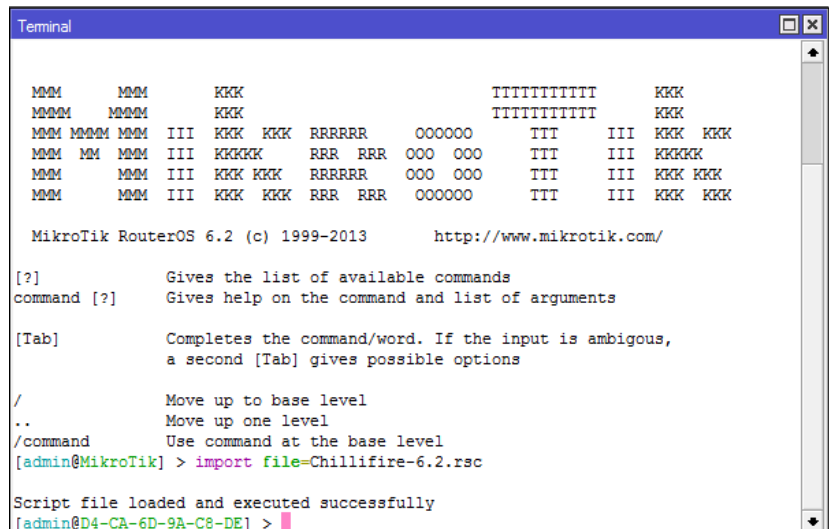


5) Import hotspot configuration

Next step is to load our hotspot configuration. It is stored in a file called 'Chillifire-x.y.rsc'. Simply open the 'Files' window in Winbox and drag the 'Chillifire-6.6.rsc' file (or the 'Chillifire-6.2.rsc' file if your RouterOS version is 6.5 or less) from your computer onto the RouterOS file system, depending on the RouterOS version you are using.

Once that is done, click on 'New Terminal' in Winbox, and type

```
/import file=Chillifire-6.6.rsc
```



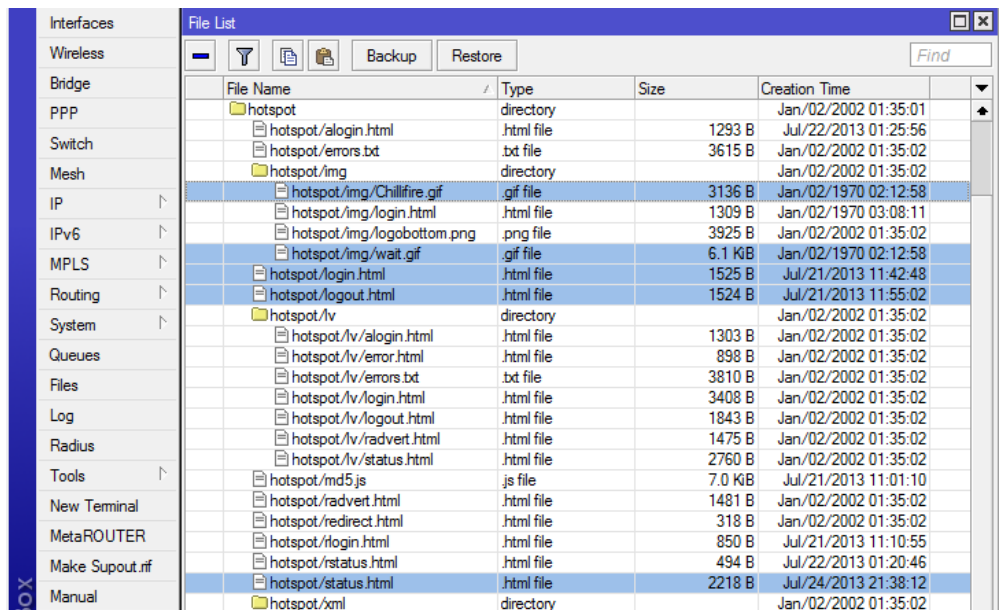
This will load the required configuration. You will receive positive feedback of the file being loaded and the script having been loaded successfully.

6) Upload html files

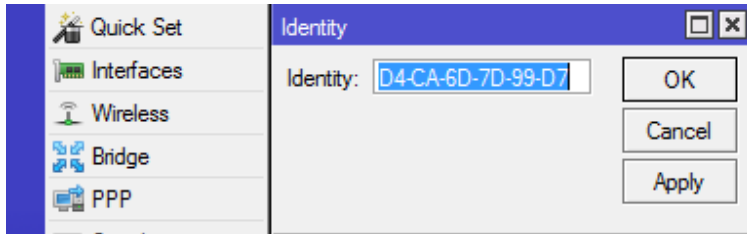
Next you need to upload a number of html and image files required to properly manage the flow of the hotspot screens. These files are:

- login.html
- logout.html
- status.html
- img/wait.gif
- img/Chillifire.gif

As previously just drag the files from your desktop to the /hotspot directory of the Files window in Winbox:



- 7) Next step is to register the router in the Chillifire Control panel. To get the relevant MAC address got to System->Identity in Winbox and copy the MAC address stored in there.



Then logon to the control panel with your account, go to Router->Router Data, and click on the 'Insert' button. Now choose the proper account or sub-account, fill in the location address and press Save.



Next step is to reboot the Mikrotik Router. After 5 minutes you should see a heartbeat in the control panel.

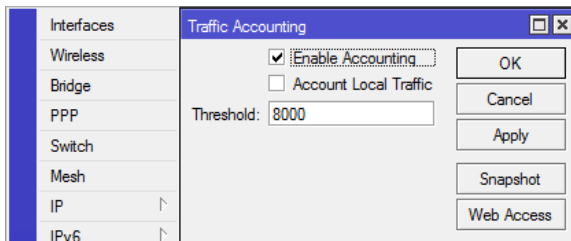


8) Remote access connection

To establish a remote access VPN connection between our hotspot management server and your router, we need to create a user and password on our VPN server for your router. Please raise a ticket on our support pages <http://support.chillifire.net> after you have registered your router in the previous step, requesting the establishment of a VPN connection.

9) Hotspot user IP accounting and logging (optional)

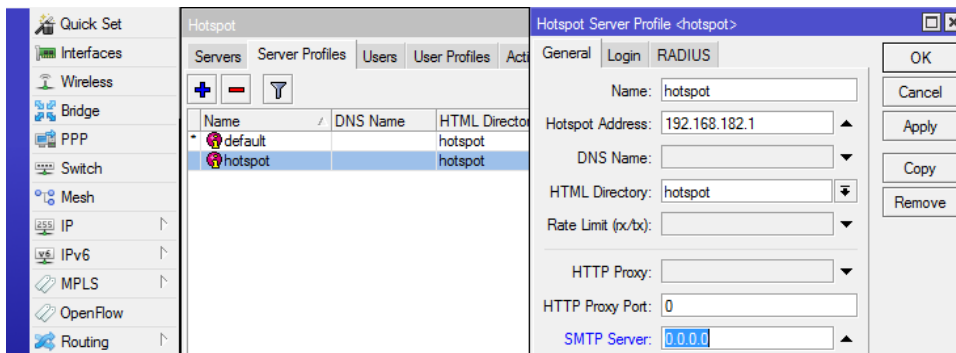
If you want to trace the meta data of the traffic that hotspot users create due to legal requirements in your jurisdiction, then make sure the 'Enable Accounting' field is ticked in the IP->Accounting menu.



10) Hotspot SMTP Server (optional)

In many cases corporate laptops or mobile devices running Microsoft Outlook or similar email clients have a designated SMTP server maintained in their configuration. In many cases ISPs do not allow the use of external SMTP on their network though, for fear of spam emails being created on their network. This has as a consequence that often such users cannot access email using their email clients. You can prevent this issue by redirecting all SMTP traffic through the ISP's SMTP server. That is the ISP that provides the broadband connection for the hotspot.

The SMTP server IP address can be added in the hotspot server profile:





11) Whitelist (optional)

To enable the whitelisting of devices you must first enable MAC based authentication in the hotspot profile (IP->Hotspot->Profile). Then you simply add the MAC number in the format XX:XX:XX:XX:XX:XX to the user manager (Tool->User Manager->User)

The related commands are:

```
/ip hotspot profile set <hotspot-profile-name> login-by=mac  
/tool user-manager user add username=XX:XX:XX:XX:XX:XX
```