Wi-Fi Networks

Configuring access point and router modes.

In the current version, SafeUTM does not support Wi-Fi adapters. For wireless clients to work, it is necessary to use special wireless access points or Wi-Fi routers.

To access the internet, users connected via Wi-Fi must be authenticated on UTM, or the Wi-Fi router needs to be authenticated. It depends on the operating mode of the device distributing Wi-Fi.

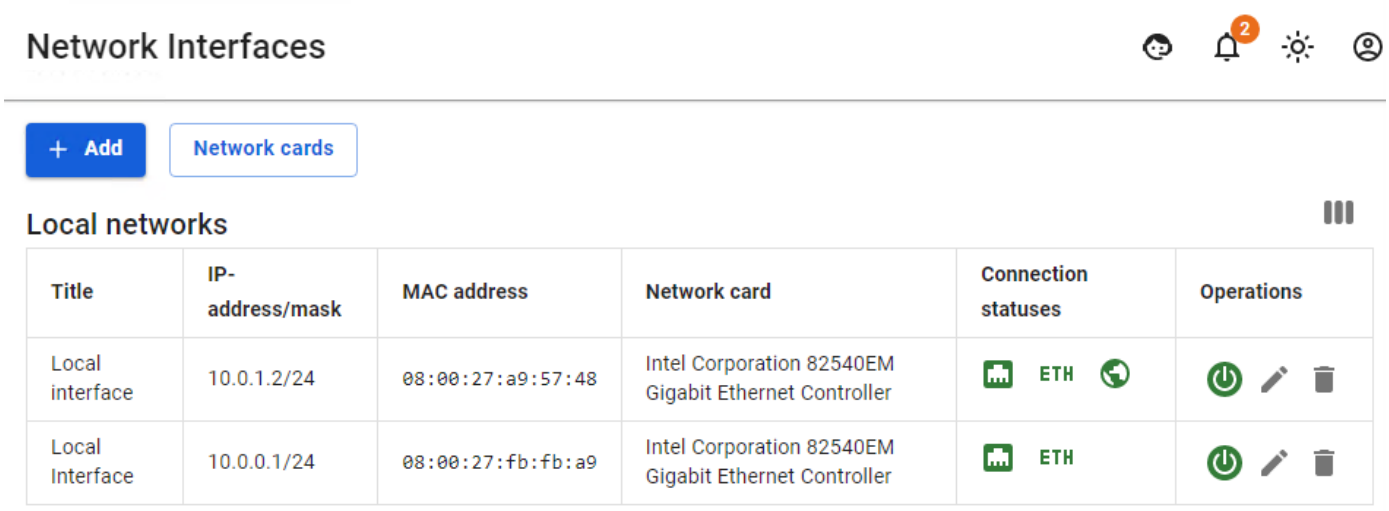
Access Point Mode (Bridge)

In this mode, the Wi-Fi device enables wireless clients to connect to the LAN.

To do this, you need to individually authenticate all wireless clients on SafeUTM. As a rule, the easiest way to do it is by IP authorization. Use the following recommendations for configuration:

- It is recommended to use a separate logical network for Wi-Fi clients with a configured **DHCP server**. At the same time, on the local SafeUTM interface, you need to add an IP address that serves as a gateway for this network.
- Using the **group addition of users** create a user group from the entire range of addresses allocated for the Wi-Fi network, or configure the automatic creation of users from the IP address range issued to devices.
- Using **content filter** and **firewall** configure necessary restrictions for Wi-Fi users.
- If the Wi-Fi router is connected to a separate UTM physical interface, then in the firewall, it is advisable to prohibit access from the wireless network to the local network.

An example of configuring the interface for clients connecting via Wi-Fi can be seen in the screenshot below:



- **10.0.1.2/24** – gateway for the wireless Wi-Fi network.
- **10.0.0.1/24** – gateway for the local Ethernet network.

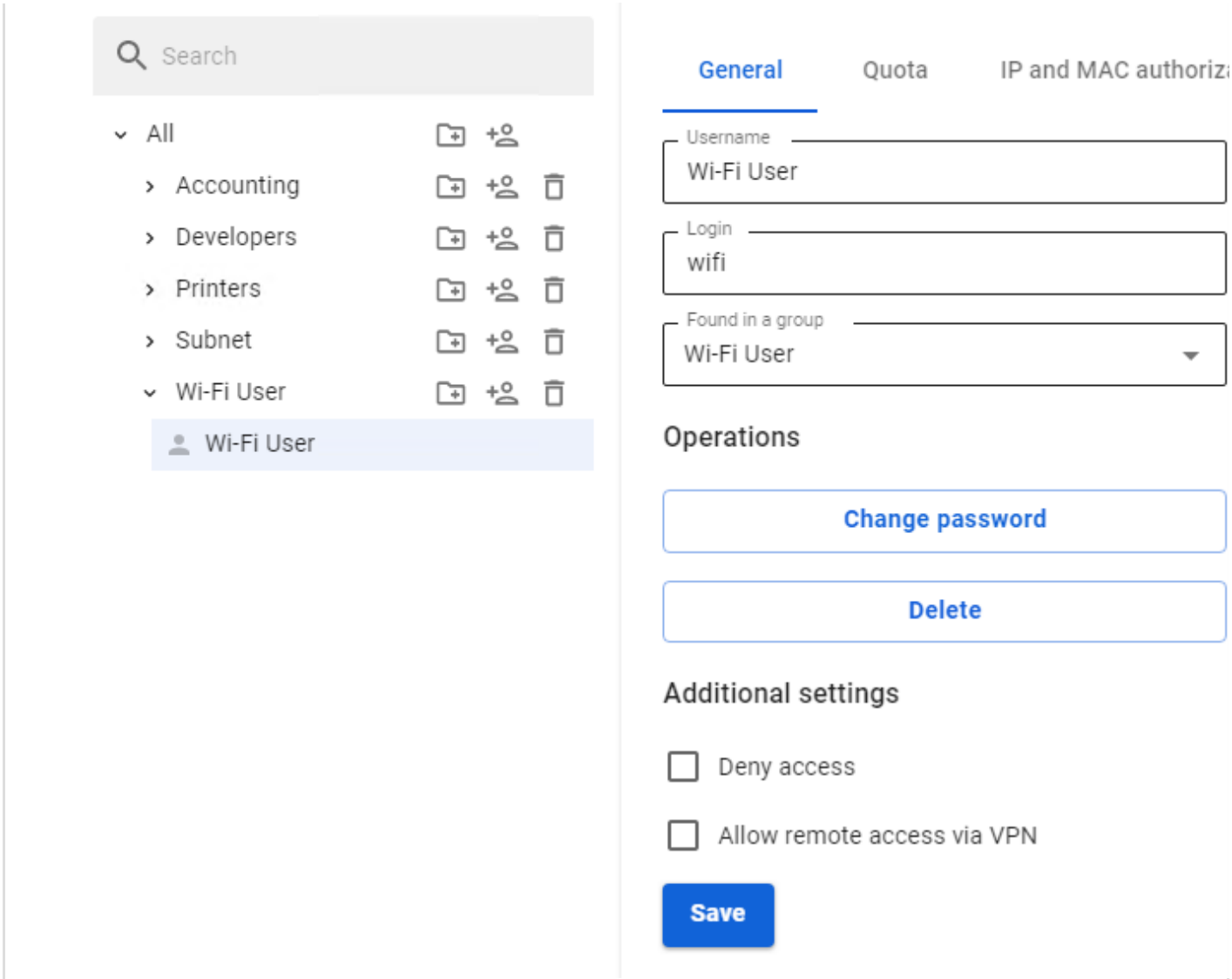
If individual authorization of Wi-Fi users is necessary (accounting for traffic and stats of each specific device user), you need to use **authorization via web browser**. With this authorization method, SafeUTM will take into account each user connected via Wi-Fi. Consider this when planning SafeUTM licensing.

Router Mode

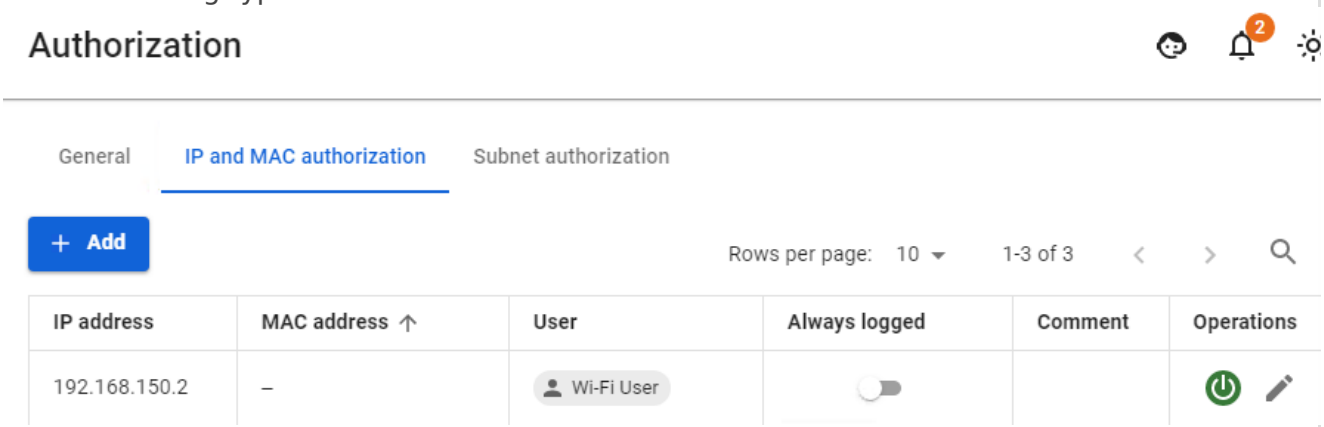
In this mode, the Wi-Fi device hides the wireless network devices behind the NAT. Thus, it will be enough for SafeUTM to authenticate only the access point as one of the users.

An example of user configuration in router mode can be seen in the screenshot below:

1. Create a user for the Wi-Fi router.
   Users can have any password.



2. In the section **Users -> Authorization -> IP and MAC authorization** create a rule of the following type:



General restrictions of **content filter** and **firewall** for Wi-Fi network must be applied for this user.

With this SafeUTM authorization method, one license per Wi-Fi access point will be used. It will be impossible to separately set up traffic filtering and calculate traffic statistics in reports for individual Wi-Fi clients.

Revision #6
Created 24 August 2022 23:14:59 by Val Redman
Updated 13 October 2022 14:51:11 by Val Redman