FRITZ!Box Guest Access

The FRITZ!Box's Wi-Fi guest access offers your guests separate internet access. Devices in the guest network are denied access to devices in the home network. For this purpose, the FRITZ!Box provides an additional Wi-Fi network with its own security settings and a captive portal, if needed.

You can make guest access available that either requires or does not require a password:

- ➢ A password is required to use private Wi-Fi guest access. Data transmitted via the guest access can be secured using the encryption methods WPA2 and WPA2. The private Wi-Fi guest access is suitable for friends and acquaintances who want secure access to the internet when visiting you at home.
- ➢ A password is not required to use the public Wi-Fi hotspot. As in any public hotspot, data is transmitted without encryption. However, wireless devices that support OWE (Opportunistic Wireless Encryption) can exchange encrypted data with the FRITZ!Box at the same time. Public Wi-Fi hotspots are suitable for use in cafés or doctors' offices, for example.

Requirements / Restrictions

- ➢ The FRITZ!Box's Wi-Fi must be enabled.
- ➢ Devices in the guest network are configured to automatically obtain IP settings via DHCP.
- ➢ It is not possible to set up guest access in the operating mode "Existing connection via Wi-Fi".
- ➢ If the FRITZ!Box uses the existing internet connection of another router (operation as an IP client), guest access is not available.
- ➢ In Mesh Repeater mode, various settings (for example captive portal) are not available. These settings are adopted from the FRITZ!Box that establishes the internet connection.

Setting up Guest Access

Configuring guest access

- ➢ Click "Wi-Fi" ("Wireless") in the FRITZ!Box user interface.
- ➢ Click "Guest Access" in the "Wi-Fi" ("Wireless") menu.
- ➢ Enable the guest access.

If you want offer your friends and acquaintances password-protected internet access:

- ➢ Enable the option "Private Wi-Fi guest access" (or "Private wireless LAN guest access").

For the "Name of the Wi-Fi guest access (SSID)" (or "Name of the wireless guest access (SSID)"), enter the name that your guests should see when they search for Wi-Fi networks.

➢ Select the desired encryption method from the drop-down list "Encryption".
➢ Enter a password that is between 8 and 63 characters long in the "Network key" field. Use numerals, letters, and other characters, and combine capitals and lower-case letters.

If you want to offer your guests internet access that is not password-protected:

➢ Enable the option "public Wi-Fi hotspot".

For the "Name of the Wi-Fi hotspot (SSID)", enter the name that your guests should see when they search for Wi-Fi networks.

➢ Click "Additional Settings" further below.

1. If you would like to receive notification about devices registering with and deregistering from your guest access, enable the option "Enabling the push service".
2. If you want guests to see a captive portal, enable the option "Display Captive Portal" and customize it.
3. If you do not want the guest access to be permanently enabled, select when the guest access should be disabled automatically.
4. If you want to allow compatible wireless devices in the public Wi-Fi hotspot to use OWE to encrypt data, enable the option "encrypted data transfer in a public hotspot (OWE)".
5. If the wireless devices should be allowed to exchange data with each other, enable the option "Wireless devices may communicate with each other".
6. If you also want to allow other forms of internet access, disable the option "Restrict internet applications".

Click "**Apply**" to save the settings.