

FRITZ! Up Your Business



HowTo

for Professional Setup

avm.de



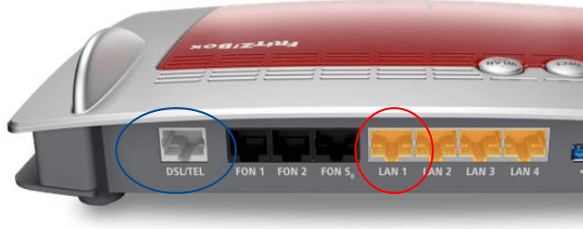
Index

1. [Remote Access](#)
2. [Port Forwarding](#)
3. [VPN](#)
4. [Guest WiFi](#)
5. [Network Overview](#)
6. [Traffic Prioritization](#)
7. [Access Control](#)
8. [Backup/Restore Config](#)
9. [Troubleshooting](#)
10. [AVM Knowledge Base](#)



Internet Options

- **FRITZ!Box 7xxx (with Telephony) and 3xxx (without Telephony)**
 - Modem Router: dedicated **DSL** port for ADSL or VDSL as **WAN** Port
 - «Only Router»: **LAN1** port can be set as **WAN** Port
 - PPP Authentication, DHCP or Fixed IP are supported in both setup



FRITZ!Box 7490



FRITZ!Box 4040

- **FRITZ!Box 4xxx**
 - Dedicated **WAN** port
 - PPP Authentication, DHCP or Fixed IP

1. Remote Access

- Requirements
 - a. Assign a Public IP Address to the WAN port
 - or
 - b. Route a Public IP Address to the WAN port

For a. :

If the public IP is dynamic you can configure a DynDNS or **MyFRITZ!**, the dynamic DNS service provided by AVM for free



1. Remote Access – DynDNS

Internet > Permit Access ?

Port Sharing FRITZ!Box Services **DynDNS** VPN

Through DynDNS, applications and services for which port sharing was configured in the FRITZ!Box firewall can remain accessible at a fixed domain name from the Internet at all times, even though the public IP address of the FRITZ!Box changes each time you dial into the Internet.

Note:
The IPv4 address assigned by the Internet service provider is not a publicly accessible IP address. This means that settings to permit access to the IPv4 services of the FRITZ!Box and to your IPv4 home network will probably not work. See the help for more information.

☒ Use DynDNS
Enter the account information for your DynDNS provider.

DynDNS Provider


Update URL:

Domain name:

User name:

Password:

Apply Cancel


- Fill the fields with your DynDNS configuration
- Click on  to get more instructions: [this is a good general approach](#)




1. Remote Access – MyFRITZ!

- Click on «Create your account»;
- Follow the wizard: you only need of a valid email address;
- Define **User name** and **Password** for the remote access;

Internet > MyFRITZ! Account





 Create a new MyFRITZ! account

Enter an e-mail address and define a password for the MyFRITZ! password.

e-mail address

MyFRITZ! password

 With these account data you can log in on the myfritz.net website.

 Setting Up FRITZ!Box Users for Access to the FRITZ!Box from the Internet

Login to your FRITZ!Box from the Internet is possible only through a FRITZ!Box user with rights to Internet access. Enter a user name and a password for the FRITZ!Box user.

Note:

For reasons of security, the FRITZ!Box user password must be different from the MyFRITZ! password.

User name

Password

In the "System > FRITZ!Box Users > Users" area you can adjust the FRITZ!Box user's settings at any time and define which rights that user needs in order to access content on the FRITZ!Box from the Internet.

Back Next Cancel



1. Remote Access – Complete Setup

- Once a fixed IP is assigned to WAN or MYFRITZ!(DynDNS) is active
 - customize the TCP port for https access from remote

TCP Port for HTTPS

The FRITZ!Box uses the following TCP port for HTTPS. If you want to use a different port you can change it here.

TCP port for HTTPS

45696 (use port range 1 to 65535)



Home network address of your
FRITZ!Box

https://fritz.box

or

https://192.168.178.1

FRITZ!Box can now be reached from the home network over HTTPS at these addresses.

- be sure that the https is enabled and take notes of your ip address or web address

Internet Access

Note:

The IPv4 address assigned by the Internet service provider is not a publicly accessible IP address. This means that settings to permit access to the IPv4 services of the FRITZ!Box and to your IPv4 home network will probably not work. See the help for more information.

☒ Internet access to the FRITZ!Box via HTTPS enabled



This option permits access to the FRITZ!Box from the Internet. All FRITZ!Box users who have been granted the right "Access from the Internet allowed" in the "System > FRITZ!Box Users" menu enjoy access.

Web address of your FRITZ!Box

https://lksvgofw0dseelg2.myfritz.net:45696

https://151.25.23.234:45696



1. Remote Access – Why FRITZ!Box is secure?

- Remote access is allowed **only** with Username and Password through the integrated **SPI Firewall**
- This **Firewall is certified** by the German supervisory authority **TÜV**
- The firewall implements **automatic prevention mechanisms** for Intrusion, Brute Force and DoS
- Even if an attacker knows the login credentials there are no options to take the complete control of the CPE

Access list for IP/Subnet is a not scalable and obsolete approach and it does not allow anyway to use mobile devices with App: IP address assigned e.g. to a smartphone is in the most case dynamic and masqueraded by the network



2. Port Forwarding

To forward a port or a port range to hosts on LAN side click on «Add Device for Sharing»

Every port is permitted, with the following exceptions:

- port used for remote access
- 8089 (assigned by default to TR-069)
- 5060, only if a VoIP user agent is configured on the box

Internet > Permit Access

Port Sharing

FRITZ!Box Services

DynDNS

VPN

All devices connected with the FRITZ!Box are safe from unauthorized access from the Internet. However, certain applications (like online games) must be accessible for other users in the Internet. By configuring port sharing you can allow such connections.

Device / Name	IP Address	Sharing	Port assigned externally IPv4	Independent Port Sharing
No port sharing configured				

Add Device for Sharing

Refresh

The setting for "Independent port sharing" can be disabled for all devices that have not requested any port sharing.

Disable

Apply

Cancel



2. Port Forwarding – Host Selection and Options

- You can select an host connected to the box or enter the IP address manually
- You can permit independent port sharing for this device (via UPnP)
- You can also enable the exposed host option, if you need to create a DMZ

Sharing for Device ?

Device

IPv4 address

MAC address

☐ Permit independent port sharing for this device

Please select...

Please select...

W10-FPatria-NB

Enter the IP address manually

IPv4 Settings

☐ Open this device completely for Internet sharing via IPv4 (exposed host).

This setting can be enabled only for one device.



2. Port Forwarding - Configuration

- Once you have selected the host or set manually the IP address

The screenshot shows a 'Create sharing' dialog box with the following fields and annotations:

- Port Sharing** (selected with a radio button)
- Application**: A dropdown menu showing 'Other application'. An arrow points to it with the text: 'Select Other application to customize your rule'.
- Name**: A text box containing 'My Forward'. An arrow points to it with the text: 'Give a name to your rule'.
- Protocol**: A dropdown menu showing 'TCP'. An arrow points to it with the text: 'Select the protocol between TCP,UDP,GRE, ESP'.
- Port to device**: Two text boxes, both containing '8080', separated by 'to port'. An arrow points to the second box with the text: 'Define the port or the port range on LAN side'.
- Port requested externally (IPv4)**: A text box containing '8080'. An arrow points to it with the text: 'Define the port or the port range on WAN side'.
- Enable sharing**: A checkbox that is checked.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom.

Note: that Port(Port Range) on LAN side and WAN side may be also different



3. VPN

- Up to 8 VPN tunnels based on IPSec standard
- 4 Options
 - a. Configure VPN connection for a user (FRITZ!Box as VPN Server)
 - b. Configure a Lan-to-Lan VPN connection among FRITZ!Boxs
 - c. Configure a VPN to connect FRITZ!Box to a Company's VPN
 - d. Import a customized configuration for interop with 3rd party

VPN Connection



Please select the type of VPN connection to be established:

☐ Configure VPN connection for one user

On the following page, select the desired FRITZ!Box user, open the entry for editing and enable authorization to use VPN.

☒ Connect your home network with another FRITZ!Box network (LAN-LAN linkup)

☐ Connect this FRITZ!Box with a company's VPN

☐ Import a VPN configuration from an existing VPN settings file



3. VPN - Configure VPN connection for one user

- Requirement: a public IP address is assigned to the WAN port
- You only need to **Add User** under System > FRITZ!Box Users, with the grant to access via VPN.
- Once you add the user, the configuration parameters for your VPN IPSec client are displayed on the web interface.
- You can also use the FRITZ!VPN client, visit:

<https://en.avm.de/service/vpn/overview/>

3. VPN - Connect your network with another FRITZ!Box

- Requirement: a public IP address is assigned to the WAN port
- Fill the fields with the required parameters
- Be sure that the Lan Network address of both FRITZ!Boxes are different from default (192.168.178.0/24)

VPN Connection

Enter the password the VPN remote site must use to establish the VPN connection.

VPN password (pre-shared key):
strong

Enter the web address (e.g. the MyFRITZ! or DynDNS address) of the VPN remote site.

Web address:

Enter the IP network of the VPN remote site. Note that the network used by the remote site must be different from your home network.

Remote network: . . .

Subnet mask: . . .

☒ Hold VPN connection permanently

☐ VPN tunnel is available only at the selected LAN ports of the FRITZ!Box

☐ LAN 2

☐ LAN 3

☐ LAN 4

Distribute IP addresses from the following network to the selected LAN ports:

Network prefix: . . .

Subnet mask prefix: . . .

Preferred DNS server: . . .

Alternative DNS server: . . .

Note:
Changes in this area will not take effect until the FRITZ!Box is restarted.



3. VPN - Connect this FRITZ!Box with a company's VPN

- Fill the fields with the required parameters
- Enable Use XAUTH only if required

VPN Connection

Enter the login data for the VPN connection. You receive all values from the remote site or the administrator of the company's VPN.

VPN user name (Key ID):

myvpnuser

VPN password (pre-shared key):

mys3cur3vpnpass0rd

strong

☒ Use XAUTH

XAUTH user name:

xauthuser

XAUTH password:

xauthpasswor

Enter the web address of the VPN remote site. This can be either a DNS name or a static IP address.

Web address

remotevpnserevr.net

Enter the IP network of the VPN remote site. Note that the network used by the remote site must be different from your home network.

Remote network:

10

.

10

.

10

.

1

Subnet mask:

255

.

255

.

255

.

0

☐ Hold VPN connection permanently



3. VPN - Import a VPN configuration

- This option allows:
 - Resume a backup VPN configuration created for FRITZ!Box;
 - Import a customized VPN configuration file;
 - To customize a VPN configuration file download the «**Configure FRITZ!Box VPN Connection**» tool and follow the wizard, visit:
<https://en.avm.de/service/vpn/overview/>

Example of customized configuration for a Cisco VPN Concentrator

3. VPN - Import a VPN configuration

```
Vpncfg {
connections {
enabled = yes;
conn_type = conn_type_lan;
name = "CISCO Concentrator 3000 Series";
always_renew = yes;
reject_not_encrypted = yes;
dont_filter_netbios = no; localip = 0.0.0.0;
Virtualip = 0.0.0.0;
remoteip = 93.94.9596;
localid {
user_fqdn = "CISCO-Username";
}
mode = phase1_mode_aggressive;
phase1ss = "alt/aes/sha";
keytype = connkeytype_pre_shared;
key = "CISCO-Password";
cert_do_server_auth = no;
use_nat_t = no;
use_xauth = yes;
xauth {
Valid = yes;
username = "Radius-Username";
passwd = "Radius-Password";
}
use_cfgmode = yes;
phase2ss = "esp-all-all/ah-all/comp-all/no-pfs";
accesslist = "permit ip any 192.168.200.0 255.255.255.0";
}
ike_forward_rules = "udp 0.0.0.0:500 0.0.0.0:500",
"udp 0.0.0.0:4500 0.0.0.0:4500";
}
// EOF
```

Allowed Security Policies for IKE phase 1 and phase 2:

http://en.avm.de/fileadmin/user_upload/EN/Service/VPN/ike_1-en.pdf
http://en.avm.de/fileadmin/user_upload/EN/Service/VPN/ike_2-en.pdf



Wireless > Guest Access

4. Guest WiFi – part 1

Enable Guest Access (Private Hotspot)

☒ Guest access enabled

Name of the guest radio network (SSID)

FRITZ!Box Guest Access

Encryption

WPA2 (CCMP)

Define a network key. The network key must be between 8 and 63 characters in length.

Network key

MyGuessPassw0rd

strong

☐ Send log of login and logoff events on this FRITZ!Box by e-mail (FRITZ!Box Push Service)

First configure Push Service in the "System > Push Service".

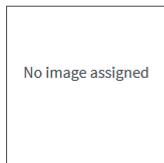
☒ Restrict Internet applications: Only surfing and mail allowed

☒ Display captive portal with information on the provider of the guest access.

Before the users of your guest access can surf, they see a captive portal, on which you can have an image (like your company logo) and a text of your own displayed. You can also draw attention to [your own terms of use](#)

☒ Permit login with guest access only after consent to terms of use

Add image:



Assign image

Add text:

- Enable Guest WiFi
- Customize SSID and Password

Enable log via Push mail

Restrict guess access only to internet and email

- Enable display of captive portal
- Permit login only after consent to term of use
- Add a logo to captive portal



4. Guest WiFi – part 2

Add text:

Welcome to my splash page and enjoy your surfing.

→ Add the text for the splash page

☒ After login to the guest access, route the wireless guests to the following website (like your home page).

Website

www.mywebsite.com

→ Enable and configure redirect to website

☐ The wireless devices connected with the guest access can communicate with each other

☐ Disconnect automatically after 30 minute(s)

☐ Do not disable until all guests have logged off

Note:

All devices using the guest access receive the access profile "Guest". This can be edited under "Internet > Filter > Access Profiles", for instance to define a period when your guests are allowed to use the Internet, or to block certain websites. Under "Internet > Filters > Prioritization" you can also limit the bandwidth for the guest access.

QR Code (Quick Response Code)

With the QR code it is easy to configure the wireless guest access on mobile devices (smartphone, tablet). When the code is scanned, the encryption settings for the wireless guest access are automatically transmitted to the mobile device. For particularly convenient use of the QR code we recommend the "FRITZ!App WLAN" (Android).

The provider of this guest access points out that use of this guest connection must comply with the provider's terms of use. Device Identification data (the MAC address of my wireless/LAN device) and times of use can be logged by the provider of this guest access.



→ QR-Code for Guest Access is automatically generated



Home Network > Home Network Overview

5. Network Overview

- A clear overview of all devices connected, with info about: type, technology and speeds
- A shortcut for each host allows
 - Assign a fixed IP address for LAN
 - Enable UPnP for automatic Port Forwarding
 - Active the WakeOnLan

All Devices Network Connections Network Settings			
The table shows all of the network devices connected with the FRITZ!Box via LAN or wireless LAN, as well as VPN connections to the home network that were established by FRITZ!Box users and apps (such as MyFRITZ!App, FRITZ!VPN). All of the devices in the home network are connected in a computer network and can exchange data, images, music and videos with each other. Network devices in the home network can also be reached from the Internet through port sharing.			
Name	Connection	IP address	Properties
This FRITZ!Box			
fritz.box		192.168.1.1	Wireless LAN, 2.4 GHz / 5 GHz
Active Connections			
NPI35EB58	LAN 2 at 100 Mbit/s	192.168.1.20	
Idle Connections			
andrea	VPN	192.168.1.201	
android-446c13bd00cc88b	Wireless	192.168.1.25	
android-8fd48fd8bda3c8d	Wireless	192.168.1.41	
android-c5ce33d6076581ae	Wireless	192.168.1.23	
android-d81f51a1cfadfee	Wireless	192.168.1.28	
android-f3beffcf0f73d67	Wireless	192.168.1.51	
Angelo	VPN	192.168.1.205	
AngelospleWatch	Wireless	192.168.1.43	
AppleWadAndrea	Wireless	192.168.1.27	
avm-nb	Wireless	192.168.1.22	



Internet > Filters > Prioritization

6. Traffic Prioritization

How it works:

- 3 different custom levels of priority
- Rules can be add for host and/or applications
- Bandwidth reservation for Guest Access*

Internet > Filters

Parental Controls Access Profiles **Prioritization** Lists

Define here which network devices and network applications are prioritized when the Internet connection is at full capacity.

Real-time Applications

Specify here the network applications with high demands on transmission speed and reaction times.
Whenever such an application uses the Internet connection to full capacity, no other data will be transmitted.

Network Device	Network Application
automatic	Internet telephony

New Rule

Prioritized Applications

Specify here the network applications with high demands on reaction times (for instance, online gaming).
Whenever such an application uses the full capacity of the Internet connection, the data of other applications will be transferred with lower priority.

Network Device	Network Application
	No prioritized application is running at this time.

New Rule

Background Applications

Applications that run in the background and are treated with low priority when the Internet connection is running at capacity (e.g. automatic updates, peer-to-peer services)

Network Device	Network Application
	No background application is running at this time.

New Rule

→ **Real-time:** always prioritized

→ **Prioritized:** at least 10% of bandwidth reserved for not prioritized hosts/applications

→ **Background:** bandwidth used only when no host/application from higher levels does not generate traffic

*with 7590,7490,7560



6. Traffic Prioritization – New Rule

- Select the priority level and click on «New rule»

Rules for Real-time Applications

Specify the network device for which the rule is to apply:

Enter the IP address manually IP address 192 . 168 . 178 . 20

→ Select the host or enter the IP Manually

Enter the network application:

All

- All
- Internet telephony
- Surfing**
- HTTP server
- FTP server
- eMule
- BitTorrent
- MS Remote Desktop
- SSH
- Telnet
- Everything except surfing and mail

→ • Select the application

- Further applications can be add under Internet > Filters > List and click on «Add Network Application»



7. Access Control

- Parental Control can be used in a professional scenario to:
 - Block/Permit a list of websites;
 - Block a list of applications;
 - Limit the timeslot for Internet;
- **How it works:**
 1. Create your custom Access Profile
 2. Apply your Access Profile to hosts



7. Access Control – Access Profile 1

Name

Give a name to your profile

Time Limit

Here you can specify when (period) and for how long (time budget) Internet use is allowed for network devices with this access profile. Enable the "shared budget" option if all devices to which this access profile is assigned are supposed to share the available online time.

Period

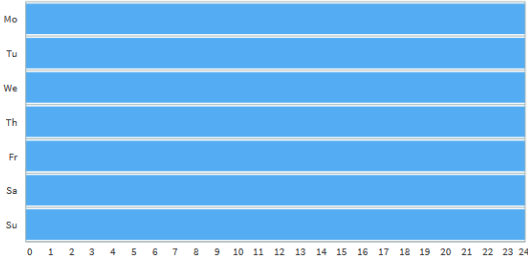
☐ always

☐ never

☒ restricted

Click the color of the operating mode you would like to specify for a period within the schedule. Then select the desired periods by clicking and dragging in the diagram.

☒ Internet use allowed
☐ Internet use blocked



Mo
Tu
We
Th
Fr
Sa
Su

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Edit schedule

Time Budget

☐ unlimited

☒ restricted

24 h 00 min
24 h 00 min
24 h 00 min
24 h 00 min
24 h 00 min
24 h 00 min
24 h 00 min

☐ shared budget

- Select the **restricted** option to limit timeslots for Internet
- Edit your schedule

7. Access Control – Access Profile 2

Filters for Web Pages

Here you can specify whether websites are filtered for this access profile, and which ones.

☒ Filter web sites

Filter Lists

☐ Permit web sites (whitelist) [\(Show list\)](#)

Only the web addresses included in the whitelist can be accessed.

☒ Block web sites (blacklist) [\(Show list\)](#)

All web pages included in the blacklist are blocked.

Calls via IP addresses are also blocked. [\(Display exceptions\)](#)

Note:

The whitelist and blacklist can be read and edited under Internet > Filters > Lists.

Blocked Network Applications

Define here for which network applications Internet use is to be blocked for this access profile.

Network Application	Remove
FTP server	
eMule	

Note:

To add more network applications to the selection list, you have to define them first under Internet > Filters > Lists.

Enable the **Filter web site** if you want to activate the blacklist or the white list:

- blacklist → All permitted except for the listed URLs
- whitelist → All blocked except for the listed URLs

The list of URL can be defined under:

Internet > Filters > Lists

Block network application


Select and Add the applications to block



Internet > Filters > Parental Control

7. Access Control – Assign Profiles

- Once a new Access Profile is set, it can be assigned to hosts using the dropdown menu under Internet > Filters > Parental Control

device		Internet Use	Online Time Today	Access Profile
	Home Network			
W10-FPatria-NB		unrestricted		New Access Profile 



8. Backup and Restore configuration

- Create and Save a backup file: be sure to enter a password to Restore

System > Backup

[Save](#) [Restore](#) [Restart](#) [Factory Settings](#)

Here you can save all of the FRITZ!Box settings to a backup file.
With this file you can restore the settings to this FRITZ!Box or to any FRITZ!Box of the same model. Only selected settings from the file can be restored to a different FRITZ!Box model.

Save Settings

Protect the backup file with a password.

Password
strong

Note:
Be sure to keep the password in a safe place. The backup file can be used only after the password is entered.

- Restore a backup file
 - Select manually the setting to be restored if a backup file of a different FRITZ!Box model is used

System > Backup

[Save](#) [Restore](#) [Restart](#) [Factory Settings](#)

Here you can restore all or certain selected settings from a backup file. The current FRITZ!Box settings will be overwritten if you click "Restore".

Backup file

Select the file from which the FRITZ!Box settings should be restored:

FRITZ.Box 4040 155.06.83i_27.04.18_1317.export

Enter the password of the backup file:

Password

☒ Restoring all of the settings
☐ Select manually the settings to be restored

Note:
After the settings have been restored, the FRITZ!Box must be restarted.



Diagnostics > Function and Security

9. Troubleshooting

- Start the **Function** button to check your FRITZ!Box
- Get an overview of all the **Security** Aspects

Function

You can have the functions and the settings of the FRITZ!Box checked. The results of the functional diagnostics can be saved.

Start

✔ FRITZ!Box 4040
FRITZ!OS 06.83, FRITZ!OS is up to date

✔ FRITZ!Box login
Password protected

✔ LAN
WAN LAN 1 LAN 2 LAN 3 LAN 4
WAN, LAN 1, LAN 2, LAN 3, LAN 4 in Power Mode

✔ Wireless LAN
2.4-GHz frequency band
Radio network name: FRITZ!Box 4040 AS
1 wireless LAN device currently connected, secured

5-GHz frequency band
Radio network name: FRITZ!Box 4040 AS
No wireless LAN device connected, secured

✔ USB Devices
no device connected

✔ Internet Connection
IPv4: connected since 27.04.2018, 12:39, IP address: 192.168.1.25

⚠ Telephone numbers
No telephone numbers configured or enabled, Support for FRITZ!App Fon not enabled.

✔ Home Network
2 devices in the home network, 1 of them online

✔ Wireless environment
2.4-GHz frequency band
8 wireless networks active on the same channel
No wireless networks with the same name

5-GHz frequency band
no wireless networks active on the same channel
No wireless networks with the same name

Diagnostics > Security

1. Connection, Internet

Internet connection via 'Other Internet service provider'

✔ Internet connected since 27.04.2018, 12:39, IP address: 192.168.1.25

FRITZ!Box Services

Overview of open ports for access from the Internet:

Opened	Protocols Used	FRITZ!Box Service
Ports		
No access permitted		

Port Sharing to Home Network Devices

Overview of the devices located in the home network with ports open to the Internet:

Opened	Protocols Used	Device
Ports		
8080	TCP, IPv4	W10-FPatria-NB 192.168.178.20 Edit

MyFRITZ!

For this box, MyFRITZ! is: disabled

⊖ Your FRITZ!Box is not registered with MyFRITZ!.

Overview of MyFRITZ! sharing for access from the Internet

Condition	Device	MyFRITZ! address	Name
No MyFRITZ! sharing settings have been configured.			

Outgoing Filters

Overview of active filters for access to the Internet:

Filter	Status	
Stealth mode	disabled	Edit
SMTP filter	disabled	Edit
NetBIOS filter	enabled	Edit
Teredo filter	enabled	Edit

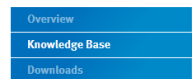


10. AVM Knowledge base

- en.avm.de/service/



FRITZ!Box 7490 Service



Knowledge Base

Filter: [Please choose](#)

Search:

[Search now](#)

417 results

< 1 2 ... 28 >

- › [Configuring the integrated fax function in the FRITZ!Box](#)
- › [Can FRITZ!VPN be used in Windows 10?](#)
- › [Cannot access the Internet via the FRITZ!Box](#)
- › [Cannot make outgoing calls over Internet](#)
- › [Cannot print with USB printer connected to FRITZ!Box](#)
- › [Configuring a USB storage device connected to FRITZ!Box](#)
- › [Extending the DECT range of the FRITZ!Box with a repeater](#)
- › [Occasional restarts: Several LEDs flash](#)
- › [Registering a MyFRITZ! account and configuring it in the FRITZ!Box](#)
- › [Restricting Internet access using parental controls](#)
- › [Setting up a USB printer connected to the FRITZ!Box](#)
- › [Setting up a VPN connection between two FRITZ!Box networks](#)



FRITZ!Box 7490 Service

[Overview](#)

[Knowledge Base](#)

[Downloads](#)

[← back to result list](#)

Setting up a VPN connection to FRITZ!Box in Windows (FRITZ!VPN)

The FRITZ!VPN software allows you to establish a secure VPN (Virtual Private Network) connection over the Internet from a Windows computer to your FRITZ!Box and then access all of the devices and services in the home network of your FRITZ!Box.

Requirements / Restrictions

- Windows 8.1 / 8 / 7 (64-bit or 32-bit) is installed on the computer.



A beta version of FRITZ!VPN is available for Windows 10 (64-bit) in [FRITZ! Lab](#).

- The FRITZ!Box must obtain a [public IPv4 address](#) from the Internet service provider.



The FRITZ!Box is not accessible from the Internet over IPv4 when used on a DS-Lite ("Dual-Stack Lite") connection. When DS-Lite is active, the status "IPv4 over DS Lite" is displayed under "Connections" on the "Overview" page of the [FRITZ!Box user interface](#).



Some of the settings described here are only displayed if the [advanced view](#) is [enabled](#) in the user interface. The configuration procedure and notes on functions given in this guide refer to the [latest FRITZ!OS](#).

1 Preparations

Downloading and installing the "FRITZ!Box VPN Connection" software

1. Call up our [VPN service page](#) in a web browser.
2. Download the FRITZ!VPN software.



The advantages with the FRITZ! products

Why FRITZ!OS

- In-house development ensures a **Perfect Combination** of powerful hardware and intelligent software
- The **Operating System** for the whole network: one entry point to control internet, wireless, firewall, voip/pbx and all the accessories (repeater, powerline, dect, smart home, ..)
- **Secure, Responsive** and **Fast**: same OS for all the FRITZ! product family, free updates and mobile apps to add new features

