

# Remote Device Access

[Main Page](#) > [FAQ](#) > [Remote Access](#) > **Remote Device Access**

---

The router can be accessed remotely via any interface as it is listening for connections on all IPs when remote access is enabled. However, due to the firewall restrictions, access via interfaces other than LAN requires additional configuration.

□

## Contents

- [1 Remote access](#)
- [2 With public IP](#)
  - [2.1 WAN Interface](#)
  - [2.2 Dynamic DNS](#)
- [3 Without public IP](#)
  - [3.1 RMS](#)
  - [3.2 VPN](#)

## Remote access

The only mandatory prerequisite for remote access is an active Internet connection. If that is met there are a few independent options for remote access described below.

## With public IP

The simplest way to access the device remotely is via its [public IP address](#) (if it has one).

Here's a range of NAT/CG-NAT IP addresses that are classified as private and cannot be utilized for remote device access via their public IP:

Private IP addresses:

1. 10.0.0.0 - 10.255.255.255 (Total Addresses: 16,777,216)
2. 172.16.0.0 - 172.31.255.255 (Total Addresses: 1,048,576)
3. 192.168.0.0 - 192.168.255.255 (Total Addresses: 65,536)

CG-NAT IP addresses:

4. 100.64.0.0 - 100.127.255.255 (Total Addresses: 4,194,305)

If your device is assigned one of these addresses, an alternate method for remote access must be employed, as outlined [below](#).

## WAN Interface

---

If a WAN interface on your device has a public IP address, you can reach the WebUI enabling remote HTTP access in the *System → Administration → Access Control* page.



After configuring the device, you can access its WebUI or CLI using various methods remotely via its public IP address:

5. **HTTP:** Enter the device's public IP address into the URL bar of your browser to access the WebUI via HTTP.
6. **HTTPS:** If HTTPS is enabled, you can securely access the WebUI by prefixing the public IP address with '<https://>' in the browser's URL bar.
7. **SSH:** Use SSH (Secure Shell) to access the device's command-line interface remotely. Open a terminal and type 'ssh root@public\_ip\_address' to establish a secure connection.
8. **TELNET:** If TELNET is enabled, you can use a TELNET client to access the device's command-line interface. Type 'telnet public\_ip\_address' in the terminal to connect.

## Dynamic DNS

---

If a WAN interface on your device has a [dynamic public IP address](#) (i.e., it has a public IP that changes), you can configure a public hostname for it using a third-party Dynamic DNS (DDNS) service in the *Services → Dynamic DNS* page. Dynamic DNS periodically updates your device's IP address at the third-party service making the device accessible via the same hostname even if the IP address changes.


Visit your device's [Dynamic DNS manual page](#) to learn more on Dynamic DNS configuration.

## Without public IP


Since public IPs are not at everyone's disposal, this section describes the remote access methods that can be utilized without the use of a public IP address.

## RMS

---

Teltonika Networks Remote Management System (RMS) provides a way to access your devices remotely without a public IP address or a VPN. [Create an RMS account](#), [add your devices](#) and click the WebUI  icon next to a device in order to generate an access link.



Alternatively, you can click the CLI  icon to generate an access link for the command line interface.



## VPN

---

Teltonika-Networks devices support multiple Virtual Private Network (VPN) protocols. With the right configuration, other devices from the same VPN can access your device remotely.

Visit your device's [VPN manual page](#) to learn more on VPN configuration.