



Grandstream Networks, Inc.

VPN

WireGuard® VPN Client Guide

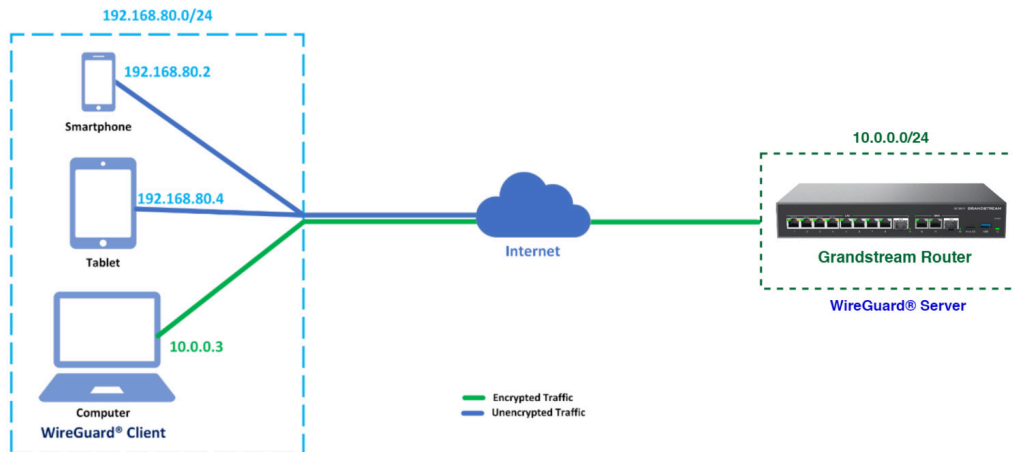


OVERVIEW

WireGuard® is a free and open-source VPN solution that encrypts virtual private networks, easy to use, high performance, and secure. Grandstream routers support WireGuard® VPN with automatic peer generation and QR code scanning for mobile phones and devices with camera support.

This guide provides step-by-step instructions for configuring a WireGuard® Client-to-Site setup. For Site-to-Site configuration, please refer to the [WireGuard Site-to-Site Configuration Guide](#).

Below is an illustration that shows how typically a server-client deployment of a VPN is done.



WireGuard® Server-Client Deployment

REQUIREMENTS

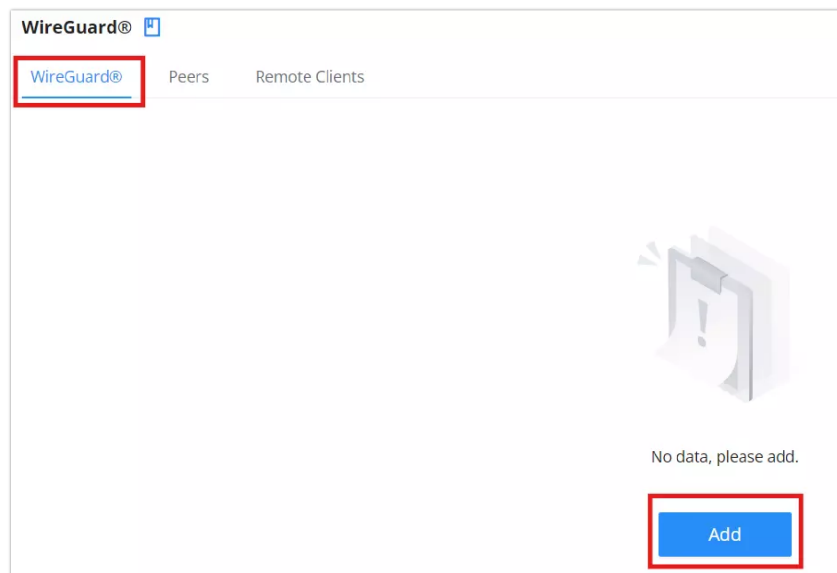
For this scenario, we are using a Grandstream router as a WireGuard® server and a PC running a WireGuard® client application. The configuration is largely similar on all the other Grandstream devices that support WireGuard® server/client.

To install the WireGuard® client on your device, please visit the official [WireGuard® site](#).

CONFIGURATION

Server Configuration

To start using WireGuard® VPN, please navigate to the **VPN → WireGuard®** page. Click on the **"Add"** button to add a WireGuard® server as shown below:



Please refer to the figure and table below when filling up the fields.

The screenshot shows the 'Edit WireGuard®' configuration window. It contains the following fields and values:

- Name:** WireGuard_server (1-64 characters)
- Status:** ON (toggle switch)
- Interface:** WAN1 (WAN) (dropdown menu)
- Monitoring Port:** 51820 (Default 51820, range 1024-65535)
- Local IP Address:** 10.0.0.0
- Subnet Mask:** 255.255.255.0 (Only support input range 255.255.255.0-255.255.255.255 is supported)
- Destination:** All (dropdown menu)
- Private Key:** SLWltZKwaWWllHQYkTj4CikDHD+MxgmutWk81PZn0= (44 bits). Below the field is a 'One-click generation' link.
- Public Key:** j2Q4CkgKYF030T7RPpmZC8VAe75PKyUUQdxUzW1lyc= (Copy button below).
- Maximum Transmission Unit (MTU):** 1420 (Default 1420, range 576-1440)

Buttons: Cancel, Save

Add/Edit WireGuard®

Name	Specify a name for Wireguard® VPN.
Status	Toggle ON or OFF to enable or disable the Wireguard® VPN.
Interface	Select from the drop-down list the WAN port.
Monitoring Port	Set the local listening port when establishing a WireGaurd® tunnel. <i>Default: 51820</i>
Local IP Address	Specify the network that WireGuard® clients (Peers) will get IP address from.
Subnet Mask	Configures the IP address range available to the Peers.
Destination	Select the Destination(s) from the drop-down list. <i>Note: When selecting "All", subsequent new interfaces will be automatically included.</i>
Private Key	Click on " One-Click Generation " text to generate a private key.
Public Key	The public key will be generated according to the private key. Click on " Copy " text to copy the public key.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.

Add/Edit WireGuard®

Automatic peer generation

Once finished configuring WireGuard®, click on the "**Automatic peer generation**" icon to generate peers very quickly and easily as shown in the figures below:

WireGuard® 

WireGuard® Peers Remote Clients

☐	Name	Enable	Ports	WireGuard® Address	Uptime	Operations
☐	WireGuard_Server	☒	WAN2 (WAN)	192.168.6.245	1min	 

WireGuard® tab

Enter a name and toggle status **ON** then click on the “**Save**” button.

WireGuard® > Create Client

 It can automatically generate client configuration files for mobile phones, computers and other endpoints, and then obtain configurations from the remote client list by scanning the QR code or directly downloading.

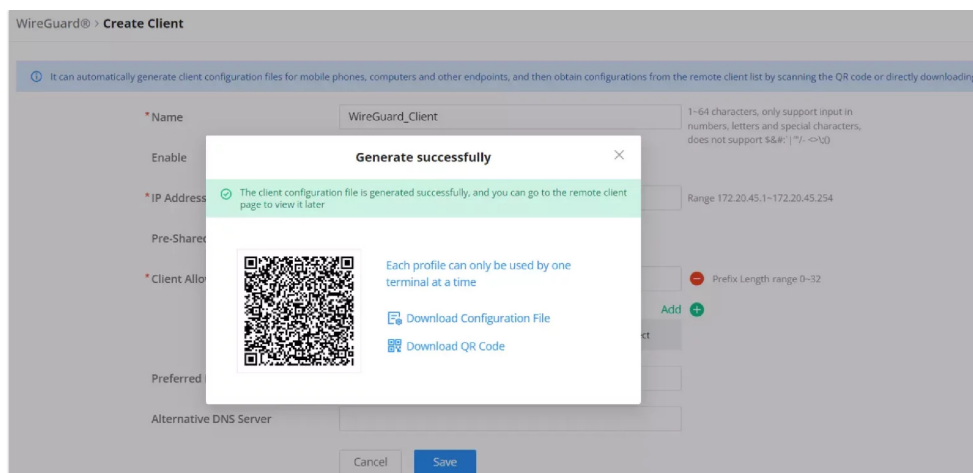
* Name 1-64 characters, only support input in numbers, letters and special characters, does not support \$&#; '"/>

WireGuard® Automatic Peer generation – part 1

Name	Specify a name for the peer.
Enable	Toggle ON or OFF the peer.
IP address	The IP address will be generated automatically. It's also possible to be modified.
Pre-Shared Key	Toggle ON or OFF the Pre-Shared key. <i>Note: Once enabled, the pre-shared key is automatically generated.</i>
Allowed IP Address	The source address range of VPN traffic allowed to enter the peer. The default is 0.0.0.0/0, which allows all traffic to enter this peer.
Preferred DNS Server	Enter the preferred DNS Server, eg: 8.8.8.8.
Alternative DNS Server	Enter an alternative DNS Server.

WireGuard® Automatic Peer generation – part 1

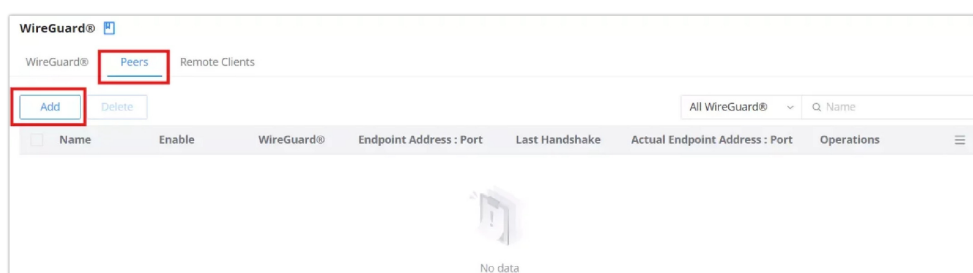
Now, the user can either download the configuration file and share it, or download a QR code for devices like mobile phones to scan.



WireGuard® Automatic Peer generation – part 2

Peers

On the peers' tab, the user can create peers manually by clicking on the **"Add"** button.



WireGuard® – Peers tab

Please refer to the figure below when filling up the fields.

WireGuard® – Add/Edit Peer

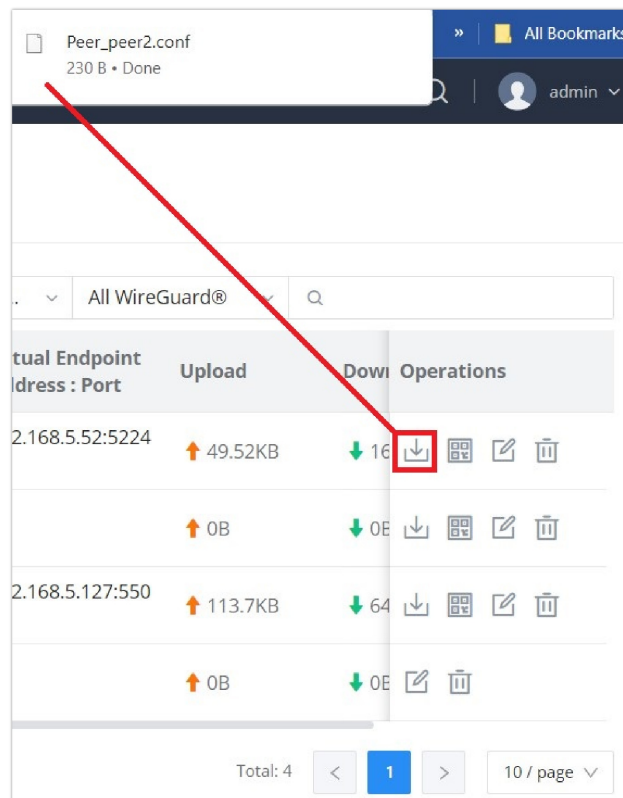
Name	Specify a name for the peer.
Status	Toggle ON or OFF the peer.
WireGuard	Select the WireGuard server from the list.
Public key	Enter the public key of the WireGuard®.
Pre-Shared key	Click on "One-click generation" text to generate the pre-shared key.

Allowed IP Address	The source address range of VPN traffic allowed to enter the device. In general, you can fill in the Peer interface address and subnet address. <i>Note: Click on Plus or Minus icons to add or delete the allowed IP Address.</i>
Endpoint Address	Configures the public IP address of the remote Peer to connect to.
Endpoint Port	Configures the port of the public IP address of the remote Peer to connect to.
Persistent Keepalive(Sec)	Configure the interval to send keep alive packets when the peer is behind the firewall

WireGuard® – Add/Edit Peer

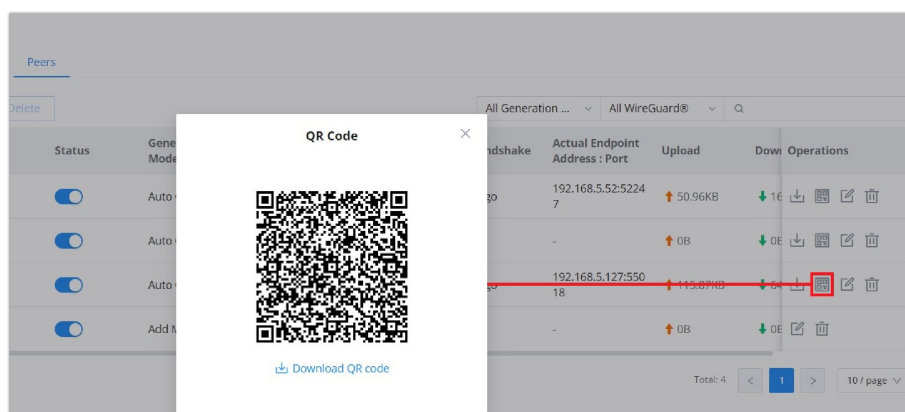
Client Configuration

The user can download the config file after adding the peer.



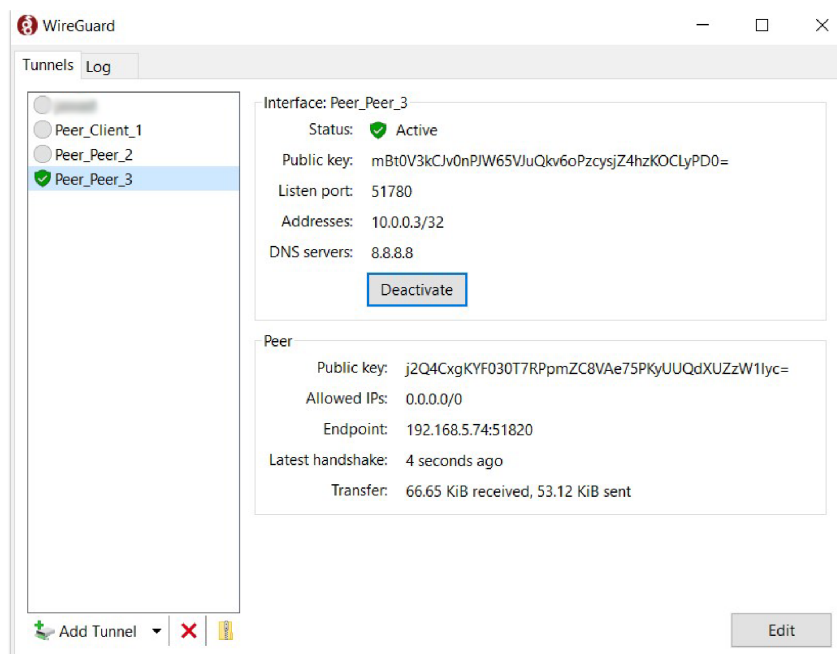
WireGuard® – Download Peer Config

Or scanning the QR code for devices with camera support.



WireGuard® – Scan Peer Config

Using a WireGuard® client application, in our case it's WireGuard® for Windows, the user can click on "Add Tunnel" to add the previously downloaded file.



WireGuard® for Windows

SUPPORTED DEVICES

The following devices support the WireGuard® server.

Model	Firmware
GWN700X	1.0.5.6 or newer
GWN7062/GWN7052(F)	1.0.9.10/1.0.9.9 or newer
GCC60xx	1.0.1.8 or newer

WireGuard® supported Grandstream Routers

© Copyright 2015-2022 Jason A. Donenfeld. All Rights Reserved. "WireGuard" and the "WireGuard" logo are registered trademarks of Jason A. Donenfeld.
