

WireGuard Installation & Configuration — Windows 11

This guide provides a complete walkthrough for installing and configuring WireGuard on Windows 11 — including commands, configuration examples, and testing.

1. Download & Install WireGuard

1. Visit the official website:

 <https://www.wireguard.com/install/>

2. Under **Windows**, click “**Download Installer (.msi)**”
3. Run the installer and approve the UAC prompt.
4. When finished, WireGuard will appear in your Start Menu.

 *Only use the official installer to ensure signed drivers.*

2. Create or Import a Tunnel

You can either import an existing config or create one manually.

Option A — Import an Existing `.conf`

1. Open the **WireGuard** app.
2. Select **Add Tunnel** → **Import tunnel(s) from file...**
3. Choose your configuration file, e.g. `wg0.conf`
4. Verify the interface and peer entries.

Option B — Create a New Tunnel Manually

1. Select **Add Tunnel** → **Add empty tunnel...**
2. WireGuard auto-generates a public/private key pair.
3. Copy the **Public key** to your server’s configuration.

4. Fill in the fields like this:

```
[Interface]
PrivateKey = <private key shown>
Address = 10.10.0.2/24
DNS = 1.1.1.1

[Peer]
PublicKey = <server public key>
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = nyx.omnitech.net:51820
PersistentKeepalive = 25
```

5. Click **Save**.



3. Ensure Windows Firewall Access

WireGuard normally creates its own firewall rule automatically.
If your system is hardened, add it manually:

```
netsh advfirewall firewall add rule name="WireGuard" dir=in action=allow
program="C:\Program Files\WireGuard\wireguard.exe"
```

✓ This allows inbound UDP traffic so the tunnel can connect.



4. Activate and Test the Tunnel

1. In the WireGuard window, click **Activate** next to your tunnel name.
2. Wait for the status indicator to turn **green**.

Test Internal Connectivity

```
ping 10.10.0.1      # Ping the WireGuard server internal IP
```

Test External Routing

```
curl https://ifconfig.me # Should show your server's public IP
```

✅ If you see the server's IP → VPN routing works.

❌ If you see your local IP → check `AllowedIPs` and `Endpoint` .

5. Useful Enhancements

Auto-Connect on Boot

Right-click the tunnel → **Settings** → enable **Activate on boot**.

Remove a Lingering Service

```
wireguard /uninstalltunnelservice <tunnelname>
```

Export Configuration

In the WireGuard app → **Export tunnel(s)** for backup or other devices.

6. Uninstall (If Needed)

You can remove WireGuard cleanly at any time:

Option 1:

Control Panel → *Programs* → *WireGuard* → *Uninstall*

Option 2 (PowerShell):

```
winget uninstall WireGuard
```

💡 The uninstaller removes all services and drivers automatically.

7. (Optional) Generate Config and Keys via PowerShell

For automated setups, you can generate keys and build the config from the command line:

```
# Create working folder
mkdir C:\WireGuard\ && cd C:\WireGuard\

# Generate keypair
wireguard /generatekeys > keys.txt
$keys = Get-Content .\keys.txt
$priv = ($keys | Select-String "Private" | ForEach-Object {($_ -split "=")
[1].Trim()})
$pub = ($keys | Select-String "Public" | ForEach-Object {($_ -split "=")
[1].Trim()})

# Build config
@"
[Interface]
PrivateKey = $priv
Address = 10.10.0.2/24
DNS = 1.1.1.1

[Peer]
PublicKey = <server public key>
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = nyx.omnitech.net:51820
PersistentKeepalive = 25
"@ | Out-File -Encoding ASCII .\wg0.conf

# Import and activate
wireguard /installtunnelservice .\wg0.conf
Start-Sleep 2
wireguard /activate wg0
```

 Keys and config generated locally — nothing leaves the system.

 **All Done!**

WireGuard is now fully configured and running on Windows 11.
You can connect securely to your network with minimal overhead.

Tested Workflow Summary

1. Install from official `.msi`
2. Import or create config
3. Allow firewall
4. Activate and test
5. Enable autostart (optional)

End of Guide — WireGuard for Windows 11