

WireGuard Peer Generator

Installation & administration guide

Version 2.3.0 | Windows administrator workstation | September 2026

Create and maintain remote-access WireGuard peers, deploy them to pfSense, and deliver client configuration files from one Windows application.

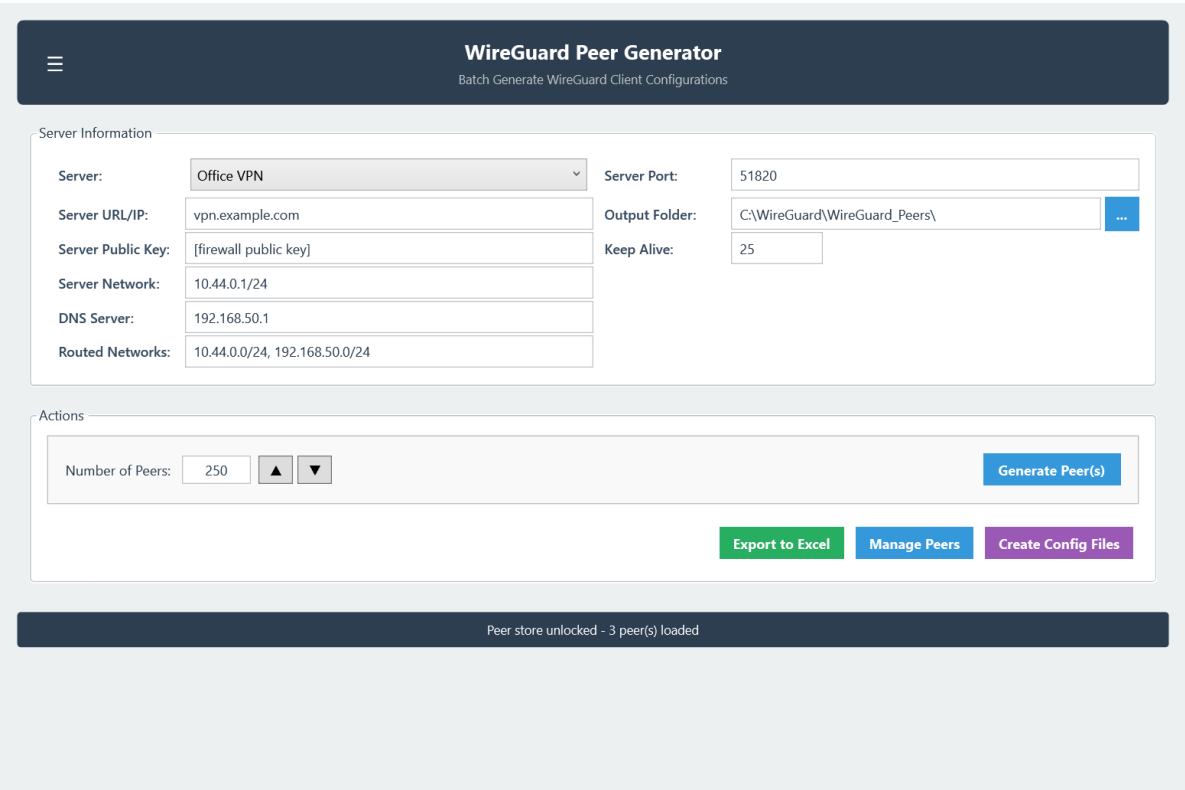


Figure 1. Main window with a fictional Office VPN. All screenshots are rendered from the application's actual WPF layouts using demonstration data; no production credentials are shown.

What the application handles

Server profiles; batch key and address generation; encrypted peer storage; peer editing, rekeying and import; pfSense deployment and sync; client file export; optional email/SMS delivery; and configurable application updates.

Where it fits: This is an administration tool. pfSense remains the VPN endpoint, and each remote device runs a WireGuard client. Configure the firewall tunnel, routing and access rules separately.

Inside: Install (2) • Prepare pfSense (3) • Add a server (4-5) • Deploy peers (6) • Deliver and maintain (7) • Updates (8) • Recovery (9) • Rollout checklist and references (10).

Install on the administrator workstation

- 1. Use a Windows PC with Windows PowerShell 5.1 and permission to write to the application and output folders. The supplied launcher uses **powershell.exe**. Use a stable folder such as **C:\Tools\WireGuardManager**, rather than running inside a ZIP archive.
- 2. Install the official WireGuard for Windows package. Confirm that its command-line utility is available to the account running the manager. [1]

```
Get-Command wg.exe
wg --version
Get-Command ssh.exe, ssh-keygen.exe
```

If wg.exe is not found, add the WireGuard installation directory (typically C:\Program Files\WireGuard) to PATH, then reopen the terminal and application. Enable the Windows OpenSSH Client optional feature if ssh.exe is missing.

- 3. Obtain the complete application folder or release ZIP from your administrator. Extract it with its folder structure intact. Required release files include **ps1**, **xaml**, **images**, **bat**, **version.json** and **WireGuard-Peer-Generator.exe**. Never distribute a copy with real settings, keys or peer stores.
- 4. Run **WireGuard-Peer-Generator.exe**. It starts the manager without a console window; keep it next to the ps1 and xaml folders. **bat\start.bat** also works and shows startup errors when troubleshooting. Keep organizational script-execution policy in place and ask your administrator to approve blocked scripts.
- 5. On first use, create the encrypted settings store when prompted and record its recovery passphrase securely. Add a server in Settings. Selecting that server creates or opens its separate encrypted peer store; record that store's recovery passphrase too.

Optional components - install only for features you use

Component	Used for
ImportExcel module	Export to Excel; not required for generating peers or storing data.
Posh-SSH module	The one-time Setup SSH wizard that installs the SSH public key. Manual key setup is also possible.
7-Zip (7z.exe)	Password-protected archives used by Send to User.
SMTP / Twilio accounts	Email delivery / optional SMS delivery of archive passwords.

```
Install-Module ImportExcel -Scope CurrentUser
Install-Module Posh-SSH -Scope CurrentUser
```

Install optional modules only from your approved source. See the official WireGuard installer [1] and 7-Zip website [4].

Prepare the VPN environment

Start with one firewall tunnel and one test device. The following is a fictional IPv4 split-tunnel deployment; replace every example with values approved for your network.

Setting	Example
Remote endpoint / WireGuard UDP port	vpn.example.com : 51820
Existing pfSense tunnel	tun_wg0
Firewall tunnel address / subnet	10.44.0.1/24 (peer pool 10.44.0.2-10.44.0.254)
Office LAN / reachable DNS server	192.168.50.0/24 / 192.168.50.1
Client routed networks	10.44.0.0/24, 192.168.50.0/24
Administrator SSH destination	192.168.50.1 : 22, reachable from the management PC

Traffic paths

Management: Windows manager - SSH - pfSense peer configuration.

VPN traffic: Remote WireGuard client - Internet/UDP - pfSense - permitted office resources.

The manager does not need to remain running for deployed clients to connect.

1. In pfSense, install/enable WireGuard as appropriate for your firewall version. Create and enable the remote-access tunnel under **VPN > WireGuard > Tunnels**. Set its listen port and tunnel address. Record its public key and actual tunnel identifier. [2]
2. Allow inbound UDP to the tunnel listen port on the WAN. If an upstream router performs NAT, arrange forwarding there as needed. Permit only the required client traffic on the WireGuard or assigned tunnel interface. [3]
3. Ensure the office networks have a return path to the VPN subnet and that the selected DNS server accepts queries from VPN clients. Avoid overlapping VPN, office and remote-user subnets.
4. Enable SSH access to pfSense from the management network. Use the application's key-based setup described on page 5. The manager does not create firewall rules, NAT rules, tunnel interfaces or the firewall's own tunnel keys.

Split tunnel versus full tunnel

The example sends only the listed VPN and office networks into the tunnel. For full IPv4 tunneling, Routed Networks can be 0.0.0.0/0; verify Internet access policy and outbound NAT on pfSense. IPv6 requires a separate design and is outside this IPv4 guide. [2, 3]

Add your server profile

Open the hamburger menu, choose **Settings > Servers**, then click **+ New**. Enter the existing firewall tunnel's connection details. The server profile describes where peers belong; it does not create the tunnel on pfSense.

The screenshot shows the 'Settings' window with the 'Servers' tab selected. On the left, a list of servers includes 'Office VPN'. The main area is divided into two sections: 'Server Details' and 'SSH Credentials (stored encrypted - used to deploy peers to pfSense)'.

Server Details:

- Server Name: Office VPN
- URL / IP: vpn.example.com
- Server Public Key: [firewall public key]
- Server Network: 10.44.0.1
- DNS Server: 192.168.50.1
- Output Folder: [currentpath]\WireGuard_Peers
- Port: 51820
- Keep Alive: 25
- Subnet Mask: 24
- Default Qty: 1
- Routed Networks: 10.44.0.0/24, 192.168.50.0/

SSH Credentials:

- ☒ Enable SSH for this server
- SSH Host: 192.168.50.1
- Username: admin
- Password: [empty]
- Private Key Path: [currentpath]\SSH_Keys\office_ed25519
- SSH Port: 22
- Auth Type: Key
- Key Passphrase: [empty]
- PfSense Tunnel: tun_wg0

Below the SSH credentials, a note states: 'Deploying to pfSense requires Auth Type = Key (password auth can't be scripted non-interactively) and a PfSense Tunnel name that matches an existing tunnel there.' A 'Setup SSH...' button is located below this note.

At the bottom of the window, there are buttons for '+ New', 'Delete', 'Save Server', 'Save & Close', and 'Close'.

Figure 2. Settings > Servers, expanded to show the server and SSH sections. Long text fields can scroll; complete example values are listed on pages 3 and 5.

1. Fill in Server Details and, for automated pfSense deployment, SSH Credentials. Use the firewall tunnel's **public** key in Server Public Key.
2. Click **Save Server**, then **Save & Close**. Save Server updates the form's in-memory record; Save & Close persists the encrypted settings.
3. Select the profile in the main window and create/unlock its peer store. The Number of Peers field displays remaining capacity. Change it to **1** for your first test, rather than generating every available peer.

Server fields and SSH setup

Field	What to enter
Server Name	A stable, recognizable name. It contributes to the peer-store filename; avoid casual renaming after use.
URL / IP and Port	The endpoint reachable by remote clients and the WireGuard UDP listen port. This is separate from SSH Host/Port.
Server Public Key	Copy the public key of the matching pfSense WireGuard tunnel. Never put its private key here.
Server Network / Subnet Mask	Firewall tunnel IP, such as 10.44.0.1, and CIDR length 24. Use the host address, not 10.44.0.0 or a dotted mask.
DNS / Routed Networks	A reachable resolver and comma-separated CIDR routes for clients. See page 3.
Keep Alive / Default Qty	Example keepalive: 25 seconds. Server selection now displays remaining capacity instead of Default Qty. Review the requested count before Generate.
Output Folder	Example: [currentpath]\WireGuard_Peers. [currentpath] resolves to the application root. Store output in an access-controlled location.
SSH Host / Port / Username	Management address and SSH port; the deployment code expects root-equivalent access. Its documented working pfSense account is admin.
Auth Type / Private Key Path	Choose Key and the matching local SSH private key. Deployment uses noninteractive SSH.
PfSense Tunnel	The actual existing identifier, such as tun_wg0, not just its display description.

Configure the SSH key

1. Click **Setup SSH....** Choose a key location, generate or load a key, and supply the pfSense connection details. The wizard can use the account password once to install the public key; it may require Posh-SSH.
2. Alternatively, add the public key through pfSense's user configuration and select its matching private key in the manager. Protect that private key with restrictive file permissions.
3. Confirm Auth Type is **Key**, review the exact tunnel name, and click **Save Server** then **Save & Close**. A GUI privilege alone may not provide the OS permissions needed to apply a tunnel.

The Key Passphrase field is not passed to ssh.exe by the current deployment code. Use a key available noninteractively, or an appropriately configured agent; do not assume entering a passphrase in the form is sufficient.

Generate and deploy the first peer

1. Select your server in the main window. Set **Number of Peers = 1** and click **Generate Peer(s)**. Generation saves the new key material and address in the encrypted peer store; it does not itself deploy the peer.
2. Open **Manage Peers**. Give the peer a useful description and owner. Add Email/Phone if delivery is required, then click **Save All Changes**. Use the Select checkbox to choose the peer.

Peer Manager tun_wg0														
☐ Select All / Clear All														
Select	Enabled	Description	Owner	Email	Phone	Address	DNS	EndPoint	Keep Alive	Routed N	Public Key	Pre-Shared Key	Private Key	Source
☒	☒	Office-Laptop-001	Demo User	user1@exam		10.44.0.2	192.168.50:	vpn.example	25	192.168.5	[example]	[hidden]	[hidden]	Generated
☐	☒	Office-Laptop-002	Demo User	user2@exam		10.44.0.3	192.168.50:	vpn.example	25	192.168.5	[example]	[hidden]	[hidden]	Generated
☐	☒	Office-Laptop-003	Demo User	user3@exam		10.44.0.4	192.168.50:	vpn.example	25	192.168.5	[example]	[hidden]	[hidden]	Generated
Check the Select column to act on specific peers with the buttons below. Enabled, Description, Owner, Email, and Phone are editable directly in the grid. Double-click a row's Address cell to open every field for that peer, including the keys. Rows highlighted green have been deployed and match what's currently live on pfSense. Rows highlighted orange need a rekey (no usable private key yet) - select them and use Rekey, then redeploy. Set a peer's Email (and Phone, for SMS) before using Send to User.														
Save All Changes Import from .conf Files Create Config Files Deploy to pfSense Sync from pfSense Rekey Selected Send to User Delete Selected Copy Selected Copy All														
Close														

Figure 3. Peer Manager with fictional records. Demonstration key placeholders are shown; the real grid can reveal actual private and pre-shared keys. Resize columns or scroll to read longer values.

3. Click **Deploy to pfSense**. Review the destination and any address-collision warnings. Confirm only if the selected peer is intended to create or replace that address on the chosen tunnel.
4. Read the result. A successful test shows **Succeeded: 1 of 1**. A batch may show **Succeeded: 8 of 10** and list each failed peer's name, address and error. Resolve failures and retry the affected peers.

What a deployment does

It pushes the description, enabled state, public key, pre-shared key, keepalive and one /32 peer address. Matching uses the tunnel and Allowed IP, so redeploying a rekeyed peer updates that address rather than adding a second record. Applying a changed tunnel can briefly interrupt active connections.

Green is a stored deployment marker, not a live health check. It means the current local public key matches the key recorded at the last successful deployment or sync. Verify a recent handshake and actual traffic on the firewall/client before declaring the VPN operational.

Deliver, verify and maintain peers

Create and install the client configuration

1. Select the peer in Manage Peers and click **Create Config Files**. The app reports the output folder; configurations normally go under the selected output folder's **Confl<server prefix>** directory.
2. Transfer the .conf securely to its intended device. Install the official WireGuard client, import the file as a tunnel, then activate it. A client configuration contains private key material; keep it out of tickets, source control and public shares.
3. Test from an external network, such as a mobile hotspot. Generate traffic to an allowed office resource. Confirm a recent handshake, then test an IP-based resource and a DNS name. Check that disallowed resources remain blocked.

Optional Send to User

Configure SMTP under **Settings > Notifications**; configure Twilio only if you want SMS password delivery. Save the settings, install 7-Zip, then select a peer and click **Send to User**. Review the recipient and delivery choices. The feature packages configurations in a password-protected archive. Use a separate approved channel for the archive password where appropriate.

Routine changes

Action	Required follow-through
Edit a peer	Save All Changes. Deploy again for firewall-side changes; regenerate and redistribute configs when client-side values change.
Rekey Selected	Deploy the new public key, regenerate the configuration and replace the client's old file. The old client key stops matching after deployment.
Sync from pfSense	Review conflicts before accepting remote data or pushing the local copy. pfSense cannot supply a client private key. Orange rows may need rekeying before a usable config can be exported.
Import from .conf Files	Use the compatible files in the current server's config folder. Review imported data and address matches; import does not itself prove the peers are deployed.
Disable or revoke access	Disable the peer and deploy the disabled state, or remove/disable it directly in pfSense. Verify on the firewall. Deleting a local record alone does not revoke remote access.

Keep one unique peer configuration per device. When adding this manager to an existing deployment, back up first, reconcile addresses and keys, and avoid bulk rekeying working clients without a replacement plan.

Configure and publish updates

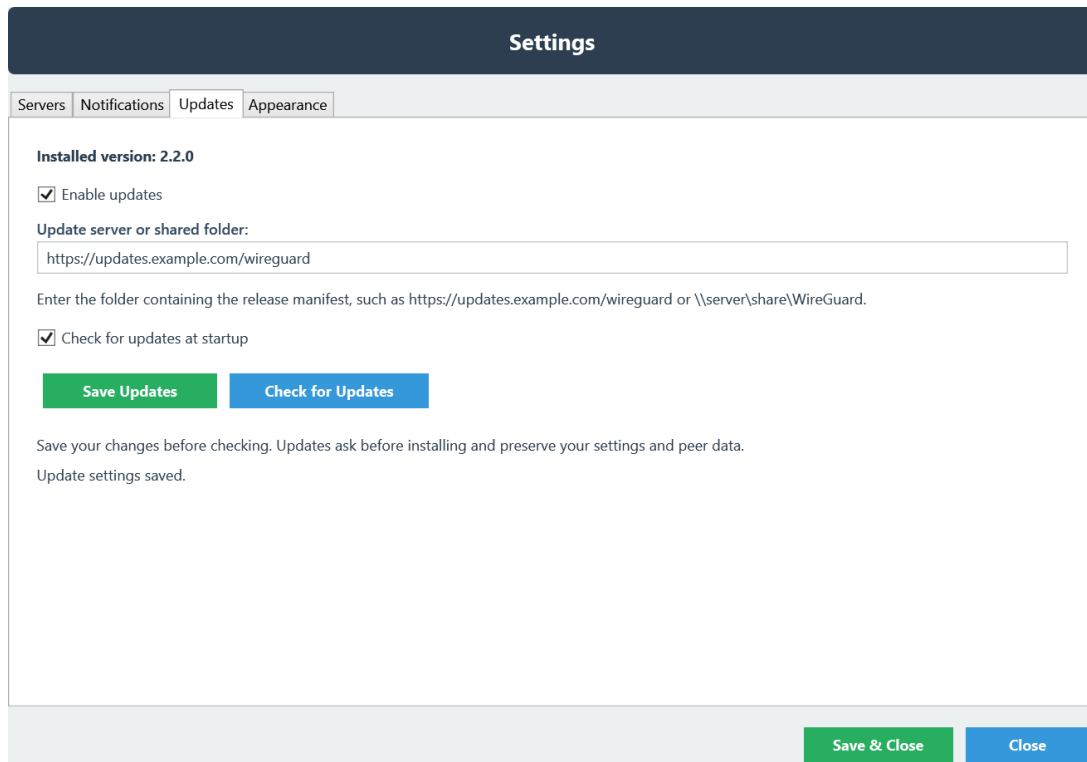


Figure 4. Settings > Updates with a fictional update URL. Checking reads the release manifest; the release ZIP is downloaded only after installation is accepted.

1. Enter the **folder containing manifest.json**, for example `https://updates.example.com/wireguard` or `\\server\\share\\WireGuard`. Enable updates and choose whether to check at startup.
2. Click **Save Updates** or **Save & Close**. **Check for Updates** uses the saved source. Automatic checks run in the background; an unreachable source does not block startup.
3. Save other edits before accepting an update. The app closes, checks the package checksum and version, replaces application files and relaunches. Settings, peer data, preferences and keys are excluded; replaced files are backed up under **backups\\update-***.

For the person publishing releases

```
.\Build-Release.cmd
.\build\Build-UpdatePackage.ps1 -PublishTo <site>\downloads\WireGuard
```

Run from the source project after updating **version.json** and **CHANGELOG.md**. It builds **WireGuard-Peer-Generator.exe**, the ZIP and manifest.json in **dist\\publish** and copies them to the site folder, manifest last. Use a trusted HTTPS endpoint or controlled share.

Updates replace the scripts, layouts, WireGuard-Peer-Generator.exe (a launcher only) and this guide. Copies at 2.2.0 reject the new exe and must be updated to 2.3.0 by hand once: extract the ZIP over the application folder. Keep the release file list compatible with installed updaters. A checksum detects corruption; it is not a publisher signature.

Backup, recovery and troubleshooting

Back up the complete operational state

Retain the application version plus **Settings.json**, **Preferences.json**, each server's encrypted peer-store JSON in its configured output folder, and the SSH private keys referenced by those server profiles. Include required configuration exports and logs under your retention policy. Application-update backups are not backups of peer data.

Store recovery passphrases separately and securely. Windows DPAPI normally unlocks stores for the same Windows user on the same machine. On a replacement machine or account, open the GUI and use each store's recovery passphrase, then verify paths, SSH access and peers before deploying. Test recovery using a protected backup copy.

Symptom	Check next
App does not start	Inspect logs\error.log. Confirm the full folder was extracted, PowerShell can run scripts, and wg.exe is on PATH.
Peer store is locked	Reselect the server and unlock it. Check the output folder and permissions. Do not replace an existing store with an empty one.
Deployment fails	Check SSH reachability, Auth Type = Key, the private-key path, noninteractive authentication, account permissions and exact pfSense tunnel identifier.
Saved but failed to apply	The peer may be in pfSense configuration but absent from the live interface. Read the returned error and check the tunnel on pfSense before retrying.
No WireGuard handshake	Confirm endpoint/UDP port, WAN or upstream forwarding, enabled peer, matching public/pre-shared keys and the correct imported client file.
Handshake but no access	Check Routed Networks, firewall rules, return routing, DNS reachability and subnet overlap. For full-tunnel Internet access, check outbound NAT.
Unexpected remaining count	Capacity reflects locally loaded peers. Reconcile existing firewall peers with Sync/import; the app is not an inventory of every externally allocated address.
Update check/install fails	Confirm the saved source contains manifest.json and its referenced ZIP; check permissions, checksum and version. Read the failure dialog; reopen the normal launcher.

Activity records are stored in logs\activity.log; errors are in logs\error.log. Exports, screenshots and copied peer rows can contain secrets even when the underlying stores are encrypted.

Rollout checklist and reference

Before onboarding the rest of your users

1. Document the endpoint, tunnel identifier, subnet, DNS, permitted networks and account responsible for administration.
2. Back up the firewall and manager data. Verify recovery passphrases and SSH key locations.
3. Complete one external-client test: recent handshake, permitted resource access and working DNS.
4. Test a disable/redeploy cycle so your access-revocation procedure is understood.
5. Create the required number of unique peers. Record owners and deliver each configuration to its intended device.
6. Choose an update source, configure it in Settings, and test a release on a separate installation before wider rollout.

Optional command-line use

Initialize and unlock the stores in the GUI first. CLI operations use the same Windows user/machine to unlock silently, return JSON by default and use exit codes 0 for success or 1 for failure. Start with read-only commands:

```
.\ps1\WireGuard.ps1 -ListServers
.\ps1\WireGuard.ps1 -ListPeers -Server "Office VPN"
Get-Help .\ps1\WireGuard.ps1 -Full
```

Sources and version scope

Application behavior was checked against the local version 2.3.0 source: WireGuard.ps1, PeerStore.ps1, SettingsStore.ps1, PfSenseDeploy.ps1, SshSetup.ps1, SendToUser.ps1, update scripts and WPF layouts. The guide describes the current implementation; a production firewall deployment was not performed while preparing it.

1. WireGuard installation

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

2. Netgate: WireGuard remote-access example

<https://docs.netgate.com/pfsense/en/latest/recipes/wireguard-ra.html>

3. Netgate: WireGuard rules and NAT

<https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/rules.html>

4. 7-Zip

<https://www.7-zip.org/>

Primary WireGuard/Netgate references checked September 26, 2026. Firewall menus and package behavior may differ by installed version. All example names, networks, addresses and screenshot records are illustrative.