USER MANUAL

WireGuard Peer Configuration

4G Remote Camera Access via Windows PC Gateway

AirLink Cloud Platform • Version 1.7

1. Overview

This user manual explains how to configure a Windows PC as a WireGuard Client (Gateway) to remotely access a 4G camera (e.g., 192.168.8.100) through the AirLink Cloud Platform.

> ⚠ **Why This Architecture?**
> 4G devices are typically behind CGNAT (Carrier-Grade NAT), which assigns private IPs and makes direct inbound connections impossible.
> A Windows PC located on-site acts as a VPN Gateway — it bridges traffic between the AirLink Cloud VPN and the local 4G camera network, enabling secure remote access without port forwarding.

Network Architecture

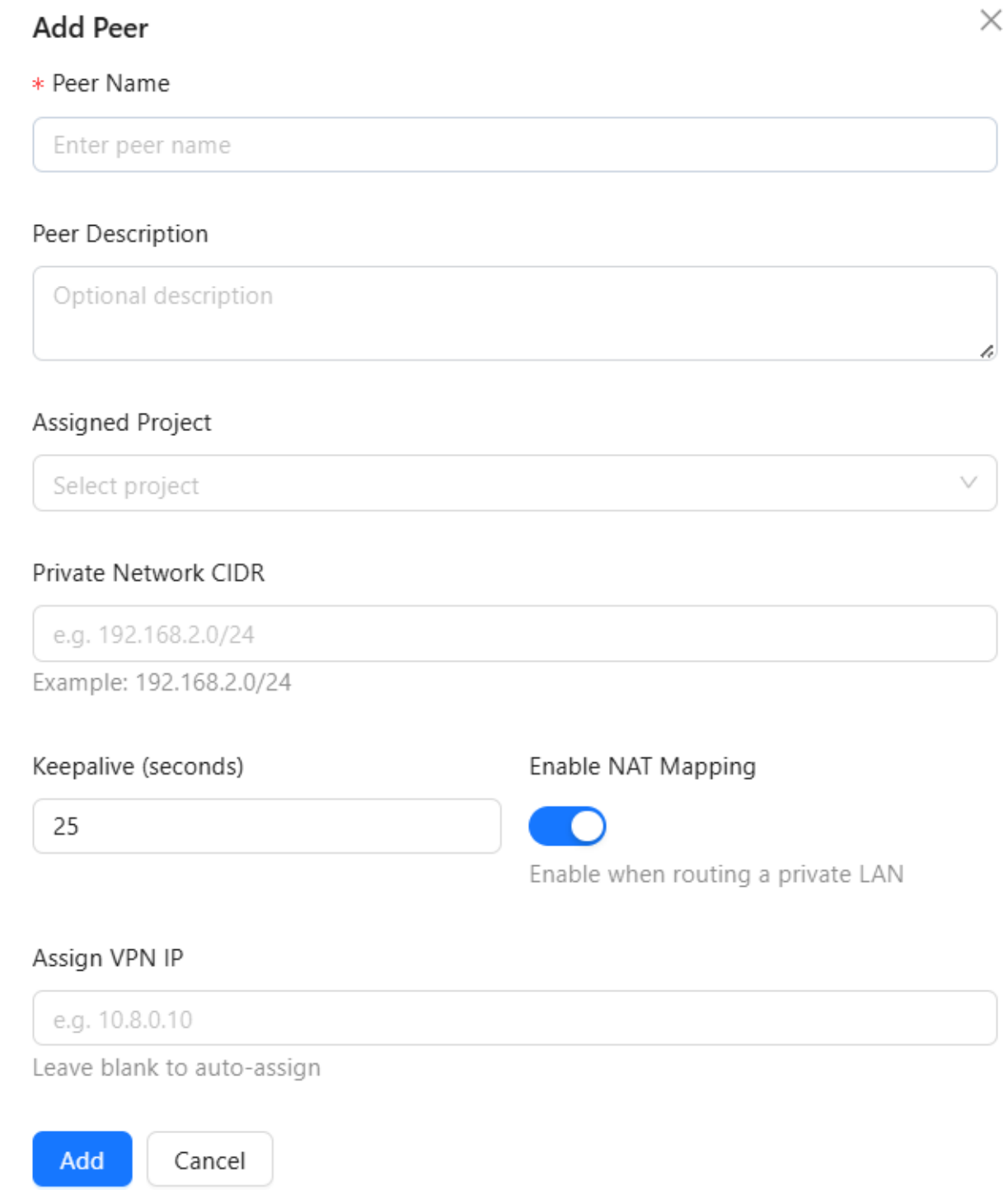
Remote Device (VPN Client) → **AirLink Cloud** (VPN Server) → **Windows PC** (On-Site Gateway) → **4G Camera** (192.168.8.100)

2. Adding a Peer on AirLink Cloud

Log in to your AirLink dashboard and navigate to the Add Peer section. Fill in the fields as described below.

Field Reference

Field	Value / Guidance
Peer Name	e.g. Site_A_Windows_PC
Peer Description	(Optional) Site location or notes
Assigned Project	Select from dropdown
Private Network CIDR	192.168.8.0/24
Keepalive (seconds)	25 (required for 4G/LTE)
Enable NAT Mapping	ON (required for LAN routing)
Assign VPN IP	10.8.0.10 or leave blank



How NAT Mapping Works

When a remote VPN device sends a request to the camera (192.168.8.100), the Windows PC rewrites the source IP to its own local IP (e.g., 192.168.8.x).

This is necessary because the camera's default gateway points to the 4G router — without NAT, the camera's reply packets cannot reach the VPN client.

After completing the settings, click Add and download the generated .conf configuration file.

3. Windows Client Setup

1. Install WireGuard: Download and install the client from wireguard.com.
2. Import Tunnel: Open the WireGuard app, click Import tunnel(s) from file, and select the .conf file downloaded from AirLink Cloud.
3. (Optional) Optimize MTU for 4G: If the connection is unstable, click Edit and add the following under the [Interface] section:

```
[Interface]
MTU = 1280
```

MTU 1280 reduces packet fragmentation common on 4G networks and improves connection stability.

1. Activate: Click the Activate button to connect.

4. Windows Gateway Configuration (Critical)

To forward traffic from the VPN to the local camera network, you must enable IP forwarding on the Windows PC. Follow all three steps — enabling IP forwarding alone is not sufficient.

Step 4a — Enable IP Forwarding via PowerShell

Open **PowerShell as Administrator** (right-click the Start menu → Windows PowerShell (Admin) or Terminal (Admin)), then run the following commands:

```
# Step 1: Enable IP forwarding on all interfaces (takes effect immediately, no reboot
required)
Set-NetIPInterface -Forwarding Enabled

# Step 2: Verify — all interfaces should show "Enabled"
Get-NetIPInterface | select InterfaceAlias, Forwarding
```

After running the verification command, confirm that the `Forwarding` *column shows* **`Enabled`** *for all interfaces including the WireGuard tunnel interface. No reboot is required.*

Step 4b — Enable and Start the RRAS Service (Required)

IP forwarding also requires the **Routing and Remote Access (RRAS)** service to be running. In the same PowerShell (Administrator) window, run:

```
# Enable and start the RRAS service
Set-Service RemoteAccess -StartupType Automatic
Start-Service RemoteAccess
```

> ⚠ **Restart Required**
> After completing Steps 4a and 4b, restart the PC to fully apply IP forwarding.

Step 4c — Verify Windows Firewall

Windows Firewall may block forwarded packets. During initial testing, temporarily disable it to verify connectivity, then re-enable with specific rules:

```
# Temporary — disable for testing only
netsh advfirewall set allprofiles state off

# Re-enable after testing
netsh advfirewall set allprofiles state on
```

> **Production Recommendation**
> For production environments, create a specific inbound rule to allow forwarded traffic from the WireGuard interface instead of disabling the firewall entirely.

5. Camera Gateway Verification

The camera's **Default Gateway** must point to the Windows PC — not the 4G router. This is one of the most common causes of connectivity failure. Follow the steps below to verify and update the setting.

How to Update the Camera Gateway

4. Find the Windows PC's local IP on the camera's subnet. Open PowerShell and run `ipconfig`, then look for the IP on the same subnet as the camera (e.g., if the camera is `192.168.8.100`, find a PC address like `192.168.8.x`). Note: the actual subnet varies by site.
5. Log in to the camera's web interface. Go to **(Network) > (Basic Settings) > TCP/IP**.
6. In the **(Default Gateway)** field, replace the current value with the Windows PC's local IP from Step 1. Click **(Save)**.

Camera TCP/IP Settings — AirLink Web Interface

The 「Default Gateway」 field must be updated to the Windows PC's local IP. The actual IP values shown will vary by site.

> ⚠ **Gateway Configuration Warning**
> The Gateway IP varies by site — always check the actual network at each deployment. Do not assume it is the same as another site.
> If 「Default Gateway」 still points to the 4G router instead of the Windows PC, reply packets will be routed incorrectly and the VPN connection will fail.

6. AirLink Cloud — Add Device & Camera Setup

Once the WireGuard peer is active and the camera gateway is correctly configured, register the camera on the AirLink Cloud platform so it can be monitored and managed remotely.

Step 6a — Add Device

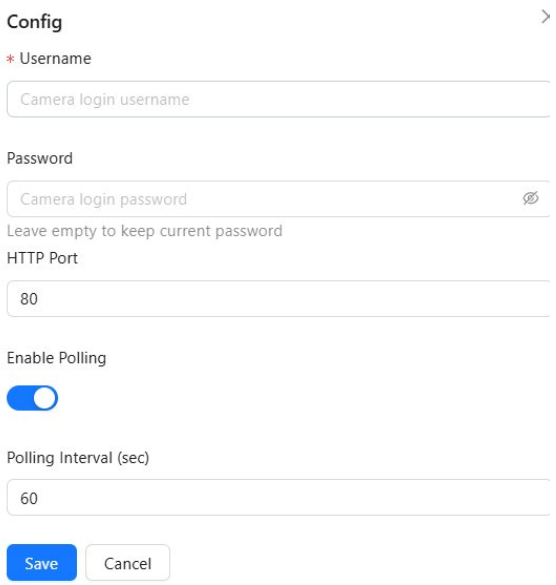
In the AirLink Cloud dashboard, navigate to the **Devices** page and click **+ Add Device**.

Step 6b — Configure Camera Login & Polling

After the device is added, a Config panel will appear. Fill in the fields as follows, then click Save.

Field	Value / Guidance
Username	Camera login username (e.g. admin)
Password	Camera login password. Leave blank to keep the current password.
HTTP Port	Default: 80. Change only if the camera uses a non-standard port.
Enable Polling	Switch ON to allow AirLink Cloud to poll the camera for status updates.
Polling Interval (sec)	Default: 60 seconds. Increase for low-bandwidth 4G connections to reduce data usage.

Config Panel



Step 6c — Activate Camera

After saving the Config, return to the Devices list and click **Activate** on the device entry. The camera status should change to **Online** once the VPN tunnel is active and the camera is reachable.

Prerequisites before activating

- WireGuard tunnel is Active on the Windows PC (Section 3)
- Camera Default Gateway points to the Windows PC (Section 5)
- Camera is reachable via its local IP from the Windows PC

7. Connectivity Testing

After completing all configuration steps, use the following tests from any remote device connected to the AirLink VPN:

Ping Test

```
ping 192.168.8.100
```

Web Interface Test

```
http://192.168.8.100
```

Troubleshooting Checklist

	Check Item	Common Fix
☐	WireGuard tunnel is Active on Windows PC	Click Activate in the WireGuard app
☐	IP Forwarding is Enabled on all interfaces	Run: Get-NetIPInterface | select InterfaceAlias, Forwarding
☐	RemoteAccess service is running	Run: Start-Service RemoteAccess
☐	RRAS service StartupType is set to Automatic	Run: Set-Service RemoteAccess -StartupType Automatic
☐	Windows Firewall is not blocking forwarded packets	Temporarily disable for testing
☐	Camera gateway points to Windows PC (not 4G router)	Update camera network settings
☐	NAT Mapping is ON in AirLink Cloud peer settings	Re-check peer configuration on dashboard
☐	MTU set to 1280 if connection is unstable	Edit WireGuard config, add MTU = 1280

8. Security Recommendations

- Re-enable Windows Firewall after testing and configure specific allow rules for WireGuard traffic.
- Assign a static VPN IP to the Windows PC peer for consistent routing.
- Rotate WireGuard keys periodically according to your security policy.
- Limit VPN access to authorized devices only using AirLink Cloud peer management.
- Monitor WireGuard handshake status — a handshake older than 3 minutes may indicate a connectivity issue.