How to set up DDNS for a security camera recorder

Dynamic DNS gives your site a hostname that follows its public IP address when the ISP changes it. It only matters if you connect by IP, through port forwarding or a self-hosted VPN.

Networking · Published 2026-10-25 · Online version: vuepointsecure.com/support/how-to-set-up-ddns-for-a-camera-recorder

Most internet connections get a public IP address that the ISP can change, after a modem reboot, an outage or on its own schedule. If your phone app or VPN client points at the old number, remote access just stops. **DDNS** (Dynamic DNS) fixes this: a small client updates a hostname such as `yoursite.example-ddns.net` whenever the IP changes, and you connect to the hostname instead.

Do you need it?

How you connect	Need DDNS?
Manufacturer's P2P / cloud app (serial number or UID)	No. The recorder registers with the vendor's servers itself.
Port forwarding with direct IP	Yes, unless you pay the ISP for a static public IP.
VPN server on your router or firewall	Yes, for the VPN server's address, unless you have a static public IP.
Behind carrier-grade NAT	DDNS will not help. Inbound connections cannot reach you at all; use P2P or a hosted connection.

Router DDNS or recorder DDNS?

Run the DDNS client in one place only. **The router is usually the better choice**: it knows its own WAN address directly, it keeps updating even if the recorder is replaced, and the same hostname works for a VPN and anything else on the site. Use the recorder's DDNS when the router does not support your provider or is ISP-locked.

- **Router DDNS:** many routers have a DDNS page (often under WAN, Advanced or Dynamic DNS settings) with a list of supported providers. Some router makers provide their own free hostname.
- **Recorder DDNS:** most NVRs have a DDNS page under their network settings. Reolink PoE NVRs support No-IP and DynDNS (on the NVR under **Menu > Network > Advanced > DDNS** on supported models). Amcrest offers its own AmcrestDDNS service. Options and menu paths vary by model and firmware.

Set up DDNS

1. **Confirm you have a real public IP**
   Compare the router's WAN address with what an external 'what is my IP' site shows. If they differ, or the WAN address is private or in 100.64.0.0/10, you are behind another NAT layer and DDNS plus port forwarding will not work.

2. **Create an account and hostname with a DDNS provider**
   Pick a provider your router or recorder lists as supported. Free tiers often require periodic confirmation to keep the hostname active, so note any renewal emails.

3 **Enter the details on the router (or recorder)**
Select the provider, enter the hostname, account username and password (or update token), enable DDNS and save. Use a dedicated DDNS password or token, not one you use elsewhere.

4 **Check the status**
Most DDNS pages show a status such as 'connected' or 'update successful'. Confirm on the provider's website that the hostname now shows your current public IP.

5 **Point your clients at the hostname**
In the phone app, VMS or VPN client, replace the IP address with the hostname, keeping the same port numbers.

6 **Test from outside**
Use a phone on cellular data. Testing from inside the building often fails even when everything is correct, because many routers do not support connecting to their own public address from inside (NAT loopback). See how to test whether a port is open.

A hostname makes you easier to find, not harder
DDNS is a convenience, not a security layer. If it points at forwarded recorder ports, everything in how to secure a camera system applies: strong unique passwords, current firmware, and no exposed admin web port unless you truly need it.

Frequently asked questions

My DDNS hostname worked for months and then stopped. Why?
Common causes: the free hostname expired because a confirmation email was missed, the DDNS client stopped updating after a router or recorder reset, or the ISP moved the connection behind carrier-grade NAT. Check the provider's site for the IP it currently holds.

Is a static public IP better than DDNS?
It removes one moving part and some business ISPs include it. It does not change the security picture: an exposed port is exposed either way.

Related guides

- How to set up port forwarding for a camera or NVR — vuepointsecure.com/support/how-to-set-up-port-forwarding-for-a-camera-recorder
- P2P cloud vs port forwarding vs VPN for remote viewing — vuepointsecure.com/support/p2p-cloud-vs-port-forwarding-vs-vpn-for-remote-viewing
- How to test whether a port is open — vuepointsecure.com/support/how-to-test-whether-a-port-is-open
- All support articles — vuepointsecure.com/support

Need help with a site? Call (888) 203-2260 or visit vuepointsecure.com/contact. Menu names and defaults vary by model and firmware; check your device's documentation.