# How to set up port forwarding for a security camera or NVR

Port forwarding lets you reach a camera or recorder by IP address from outside the building. It works, but every open port is a door on the internet, so do it deliberately or not at all.

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

Port forwarding tells your router: when a connection arrives from the internet on port X, send it to this camera or recorder on the inside network. Without a rule, the router drops unsolicited inbound traffic, which is exactly what you want most of the time. With a rule, anyone on the internet who finds your public IP can knock on that port.

> **Try the safer options first**
> Most recorders sold today can be viewed remotely through the maker's own app (P2P/cloud) or over a VPN, with **no inbound ports open at all**. Recorders are a common target for automated attacks. Read P2P cloud vs port forwarding vs VPN before you open anything.

## Before you start

- **Give the recorder a fixed address.** A forward points at one internal IP. If the recorder's address changes after a power cut, the rule points at nothing. Set a DHCP reservation or a static IP first.
- **Check you actually have a public IP.** Log in to the router and look at its WAN/Internet address. If it starts with 10., 192.168., 172.16-31. or 100.64-100.127, you are behind another router or carrier-grade NAT (common on cellular and some fixed-wireless service) and a forward on your router will not be reachable from outside.
- **Change the default password and update firmware** on the recorder before it is reachable from the internet, not after. See how to secure a camera system.
- **Forward to the recorder, not to every camera.** One NVR with one or two forwarded ports is far easier to keep secure than eight cameras each with their own.

## Common default ports by brand

These are factory defaults. Installers often change them, so always confirm the current values on the device itself (usually under **Network > Port**, **Network > Connection** or **Network > Advanced > Port/Server Settings**, depending on brand and firmware).

| Brand | App / client port | Web (HTTP / HTTPS) | RTSP | Other |
|---|---|---|---|---|
| Hikvision | 8000 TCP (Server port, used by Hik-Connect direct IP and iVMS-4200) | 80 / 443 | 554 (10554 on some models) | Port values are editable on the device |
| LTS | Typically 8000 TCP (Hikvision-based platform) | 80 / 443 | 554 | Confirm on the recorder's port page |
| Dahua | 37777 TCP, 37778 UDP | 80 / 443 | 554 | Dahua sales in the US ended Dec 31, 2025; existing units still use these |

| Brand | App / client port | Web (HTTP / HTTPS) | RTSP | Other |
|---|---|---|---|---|
| Amcrest | 37777 TCP, 37778 UDP | 80 (HTTPS available) | 554 | Amcrest recommends setting up HTTPS before forwarding |
| Reolink | 9000 (Basic Service / Media port, used by Reolink App and Client) | 80 / 443 | 554 | 1935 RTMP (browser live view), 8000 ONVIF. Several are disabled by default on many models |

*Factory default ports. Forward only the ones the access method you use actually needs.*

> **Note**
> For phone-app access by IP you usually need only the app/client port. For browser access you need the web port. **RTSP and ONVIF are for third-party software** and rarely need to be exposed to the internet at all.

## How to create the forward

1. **Find the recorder's internal IP and ports**
   Use the recorder's local menu or the vendor discovery tool (see how to find a camera or recorder's IP address). Write down the IP and the exact port numbers shown on its port settings page.

2. **Log in to the router**
   Open the router's address (often the default gateway shown in your computer's network settings) in a browser, or use the router's app. ISP-supplied gateways are often managed through the ISP's app instead of a web page.

3. **Open the port forwarding page**
   The label varies by brand and firmware. Look for **Port Forwarding**, **Virtual Server**, **NAT Forwarding** or **Apps and Gaming**. See the router table below for where it usually lives.

4. **Add one rule per port**
   Enter a name, the external port, the internal port (keep them the same unless you have a reason), the protocol (TCP, UDP, or both as the vendor specifies) and the recorder's internal IP. Save.

5. **Disable UPnP if you do not need it**
   UPnP lets devices open their own forwards without asking. Turn it off on the recorder and, if nothing else depends on it, on the router, so the only open ports are the ones you created.

6. **Test from outside the network**
   Testing from inside the building gives misleading results. Use a phone on cellular data or an external port checker. See how to test whether a port is open.

7. **Add DDNS if your public IP changes**
   Most business and home connections get a public IP that can change. A DDNS hostname follows it so your app setting keeps working.

## Where the setting usually lives on common routers

| Router family | Usually found under |
|---|---|
| TP-Link | Advanced > NAT Forwarding > Virtual Servers (or Port Forwarding) |
| ASUS | WAN > Virtual Server / Port Forwarding |
| Netgear | Advanced > Advanced Setup > Port Forwarding / Port Triggering |
| Linksys | Security > Apps and Gaming (single port forwarding) |
| Ubiquiti UniFi | Network application settings, Port Forwarding section |
| ISP gateways (cable, fiber) | Often in the ISP's mobile app under advanced Wi-Fi or network settings; some ISPs label it NAT/Gaming |

*Menu names change between firmware versions. If yours differs, search the router maker's help site for 'port forwarding' plus your model number.*

## Security rules if you do forward

- **Never expose the admin web port (80/443) unless you truly need browser access from outside.** The web interface is where the most serious recorder vulnerabilities have historically been found.
- **Never use DMZ mode** to make a recorder reachable. It forwards every port.
- **Use a strong, unique admin password** and create a separate low-privilege viewing account for day-to-day use.
- **Keep firmware current** and check the vendor's security advisories a few times a year.
- **Remove forwards you no longer use.** Old rules pointing at a reassigned IP can expose a different device.
- **Restrict source IPs** if your router supports it, so only your office's public address can reach the port.

## Frequently asked questions

### Do I need port forwarding to view cameras on my phone?

Usually not. The maker's P2P/cloud app (Hik-Connect, Reolink App, Amcrest View Pro and similar) connects out from the recorder, so no inbound ports are needed. Port forwarding is only required for direct-IP access.

### I forwarded the port but it still does not connect. Why?

The three most common causes are carrier-grade NAT (your router's WAN address is not public), the recorder's internal IP having changed, and testing from inside the network. Work through how to test whether a port is open.

### Should I change the external port to something non-standard?

It cuts down on noise from automated scans but it is not security. A non-standard port with a weak password is still exposed. Treat it as a minor extra, not a substitute for a VPN or strong credentials.

## Related guides

- 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
- How to set up DDNS for a camera recorder — vuepointsecure.com/support/how-to-set-up-ddns-for-a-camera-recorder
- How to set up a DHCP reservation for a camera or NVR — vuepointsecure.com/support/how-to-set-up-a-dhcp-reservation-for-a-camera-or-nvr
- 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.