

Cameras, DVRs and DynDNS

Getting Started

Welcome to the Dyn Wizard! These instructions will help you set up DynDNS service with your camera from start to finish, including network configuration and Dyn account creation. Let's begin!

Step 1 of 7: Install your camera or DVR

The first step is to set up the camera or DVR itself. You may have a professional install the device, or you may do it yourself; in either case, you need to be able to view it locally before visitors can reach it over the Internet. This is usually the hardest step, but your installer or the camera's manufacturer should be able to help you with this. (Please note: *Dyn cannot provide support for camera installation or configuration.*)

Fortunately, setting up a new camera or DVR is usually straightforward; once the device is powered up and connected to your router, it should be accessible from any other machine in the network at its internal IP address (usually *192.168.x.x* or *10.x.x.x*). Once you can access the device from within the same network, you can proceed to configuring the network for remote viewing.

Step 2 of 7: Configure port forwarding in your router

Now that your camera or DVR is up and running, the next step is setting up your network to allow external traffic. To do this, you will need to configure your router's port forwarding settings. Visit portforward.com for a handy list of guides by router and service. (If you do not have a router, you may skip this step.)

In many cases, web-accessible cameras have **two ports** you will need to forward: the web port, for accessing the camera's interface, and the media streaming port, which is used to broadcast the actual camera feed. The common ports for this are TCP 80 (web) and UDP 9000 (media), but your camera or DVR should list the default ports. Again, if you're not sure, the device's documentation, your camera installer, or the camera or DVR manufacturer should have more information.

Step 3 of 7: Configure your firewalls (optional)

If your camera or DVR is attached to another device, such as a computer, you will need to make similar adjustments on the computer's security settings to allow visitors to reach the device. For example, you may need to reconfigure Windows Firewall, Norton security suites, ZoneAlarm and other measures to allow the incoming connections to reach the device. (Standalone camera systems do not require firewall changes, and this step may be skipped.)

Step 4 of 7: Bridge your modem

If your cable or DSL modem was constructed in the last couple years, you may need to “bridge” the device. Modern modems have built-in firewalls that protect your network, just like routers; however, if you already have a router, the modem’s firewall is redundant. By setting the modem to bridge mode, all incoming traffic is passed downstream to your router, allowing the router to handle your network’s security.

For more information on bridging your modem (and whether or not you even need to do so), consult your modem’s documentation, contact your ISP, or simply search the web for your modem’s model number and the word “bridge” (e.g. “ModemCo W9004 bridge”).

Step 5 of 7: Test your network

When you have configured port forwarding in your router, you will need to test your network externally (from outside). To do this, [get your network’s external IP address from CheckIP](#), then have a friend try to visit the IP address or use our [Open Port Tool](#) to test your network. You should receive an “Open” response from our Open Port Tool, and your friend should be able to see your camera or DVR.

When testing, it’s important to remember that if your friend receives *any* response other than “connection timed out” or “page not found”, the camera or DVR may be *partially* working. For example, he or she may see:

- A login prompt or splash screen
- Background images
- Camera controls, but without video
- Broken embedded ActiveX or Java plugins
- Changing title bar or address (e.g. ‘—WEB APPLICATION MANAGER—’, automatic redirect to `http://1.2.3.4/web/camera.html`, etc.) but no content

All of these errors indicate that the network is at least partially configured and the device is responding; you may need to forward additional ports, change the device’s password, or have the friend use a browser which supports the web plugin utilized by the device (e.g. Internet Explorer for ActiveX).

If your network is configured properly, you can continue to the next step; if not, [please see the Troubleshooting Wizard](#) to walk through some common problems.

Step 6 of 7: Create an account and DynDNS hostname

Now that your camera or DVR is installed and working, and visitors from outside your network can remotely view it, you can begin using DynDNS. [Create and confirm an account](#), then [sign up for a trial of DynDNS Pro](#). You can cancel the trial within 14 days and still receive one free hostname. The dynamic DNS host should be assigned to [your network’s external IP address](#). Once your host is created, wait a few minutes for the service to activate, then have your friend (or our Open Port Tool) test your network using the host (e.g. `http://mycamera.dyndns.org`).

If all goes well, you should see the same results as using the IP address directly, which indicates that the DynDNS host is working properly. (Remember, no actual traffic passes through the DynDNS service; any unusual behavior, such as “slow” video streaming or ActiveX errors, are unrelated to DynDNS and are problems with your network’s bandwidth or camera.)

Step 7 of 7: Install an update client

The last step is to configure an update client, which will keep your new DynDNS host up-to-date with your network’s external IP address. If your camera, DVR or router has a section for DynDNS (sometimes DynDNS.com or DynDNS.org), this is an update client. Enter your username, password and hostname, and the router will tell us when your IP changes so that your DynDNS host will always be correct.

If you do not have a hardware update client, you can [install a software update client](#) on a computer anywhere in the network (typically your server computer). We recommend using a software client whenever possible, since they are easier to troubleshoot and configure than hardware update clients.

You’re finished!

Congratulations! At this point, you have installed your camera or DVR, configured your network to allow visitors to reach it, set up DynDNS and installed an update client to keep it synchronized with your location. Users from anywhere in the world should be able to view your camera by entering your DynDNS hostname into their browser.

If something went wrong, click the Previous button to retrace your steps, or [start the Troubleshooting Wizard](#) to help identify and fix the problem.