Windows 10 Private Network Security

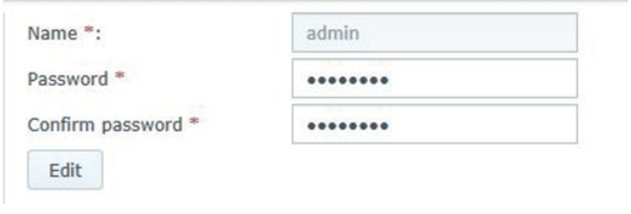
4 WAYS TO PROTECT YOUR PATH TO THE WEB

The router is the first line of security from intrusion into any network. Anyone that connects to the internet does so through a router: a hardware device, either wired or wireless (Wi-Fi®), that allows you to communicate between your local network (i.e., your PC and possibly other connected devices) and the internet. As such, enabling the highest level of security on the router is the best way to keep your PCs, printers, and data safe from malicious attack.

PROTECT YOUR ROUTER

A password on your network is not the same as a password on your router. Unfortunately, many vendors continue to offer both unsecured and secured router configurations. If a router is unsecured (that is, allowing connections to it without requiring any administrator password), anyone (yes, anyone!) could connect to the router and thereby jump onto your local network. A hacker could change your passwords, spy on you, or even access the files on a network-attached hard drive.

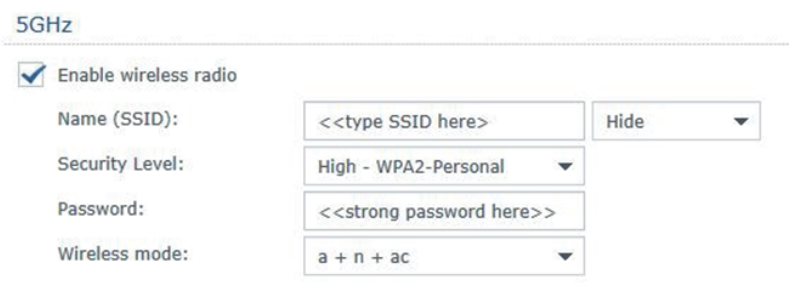
Always secure your routers with a unique administrator password — not the one set by the manufacturer (see our post on generating secure passwords for best practices). Below is a screenshot of how most routers allow you to set passwords to secure them on the network:



CONFIGURE ENCRYPTION

With wireless routers, passwords are only half the battle — choosing the proper level of encryption is just as important. Most wireless routers support four wireless encryption standards: WEP (weakest), WPA (strong), WPA2 (stronger), and WPA3 (strongest). Go with the highest encryption standard supported by your router.

Below is a screenshot of how to set the appropriate level of encryption on your router. To do so, you need to login as the router administrator and navigate to the encryption settings (varies by router vendor).



KEEP THE FIRMWARE UP TO DATE.

Many router manufacturers roll out software updates throughout the year to address security problems, so a router with the latest updates is much less likely to be infected by malware. Most router vendors apply firmware updates automatically without requiring customers to perform this operation. Newer router models may also offer a mobile app, which you can download to a phone just like any other app and use to check for updates. However, if automatic firmware updates are not offered by your router vendor, you should navigate to the router manufacturer's website, go to Support, and identify the correct update based on your router's specific model name and ID (typically found on the router itself).

USE VIRTUAL PRIVATE NETWORKS (VPNS).

Going beyond securing the hardware inside your network, a Virtual Private Network (VPN) is a server that you connect with to reroute your external internet activities. VPNs can protect your identity and information by providing a mainstream way to browse the web privately (but not always anonymously). All the traffic that passes through your VPN connection is secure and cannot, in theory, be intercepted by anyone else — meaning they're great for use on both local networks and public ones.

Network security has been simplified and strengthened by many modern router setups, but following the default manufacturer recommendations often walks a line between convenience and control. Enabling the highest level of security on the router is key to protecting your PCs, printers, and data from malicious attack.

Be more secure from power on to power off.