


f
t
You Tube
in
o
B
English ▼
Log in



The worldwide network of companies that brings you Wi-Fi®

SEARCH

SEARCH

View Wi-Fi CERTIFIED™ products by category

Discover Wi-Fi

Security



Securing your Wi-Fi® connections is an important element of securing your personal data. A Wi-Fi network using WPA2™ provides both security (you can control who connects) and privacy (the transmissions cannot be read by others) for communications as they travel across your network. For maximum security, your network should include only devices with the latest in security technology – Wi-Fi Protected Access® 2 (WPA2). Wi-Fi CERTIFIED™ devices implement WPA2.

Most Wi-Fi equipment is shipped with security disabled to make it very easy to set up your network. Most access points, routers, and gateways are shipped with a default network name (SSID), and administrative credentials (username and password) to make configuration as simple as possible. These default settings should be changed as soon as you set up your network.

It's also important to consider employing other measures to secure your communications after they travel beyond your Wi-Fi network. Tools like personal firewalls, Virtual Private Networks (VPNs) and HTTPS can help reduce the risk of compromised privacy and security for internet traffic.

Security made easy: Wi-Fi Protected Setup™

Wi-Fi Protected Setup is an optional feature that simplifies and standardizes the process of configuring and securing a Wi-Fi network. It configures the network name (SSID) and WPA2 security for the gateway and client devices on a network and makes adding a new device to your network as easy as pushing a button or entering a personal information number (PIN). Products certified for Wi-Fi Protected Setup are available at major electronics retailers and display this identifier mark on their packaging.



Securing a new network

- Change the network name (SSID) from the default name

- Change the administrative credentials (username and password) that control the configuration settings of your Access Point/Router/Gateway
- Enable WPA2-Personal (aka WPA2-PSK) with AES encryption
- Create a network passphrase that meets recommended guidelines
- Enable WPA2 security features on your client device and enter the passphrase for your network

Checking security on an existing network

When you add a new device to your Wi-Fi network, it's a great time to make sure you're taking advantage of the highest level of security. Take the opportunity to ensure your network is configured for WPA2.

If your network was set up some time ago, or a service provider (e.g consultant or cable provider) configured your home network, it may be worth checking that it's configured for the highest level of security. If your network is configured for an older generation of security (WEP or WPA), Wi-Fi Alliance® recommends you move to WPA2. WPA2 has been required on all Wi-Fi CERTIFIED products since 2006 – the vast majority of Wi-Fi CERTIFIED devices in service today are capable of WPA2.

Passphrase quality & lifespan

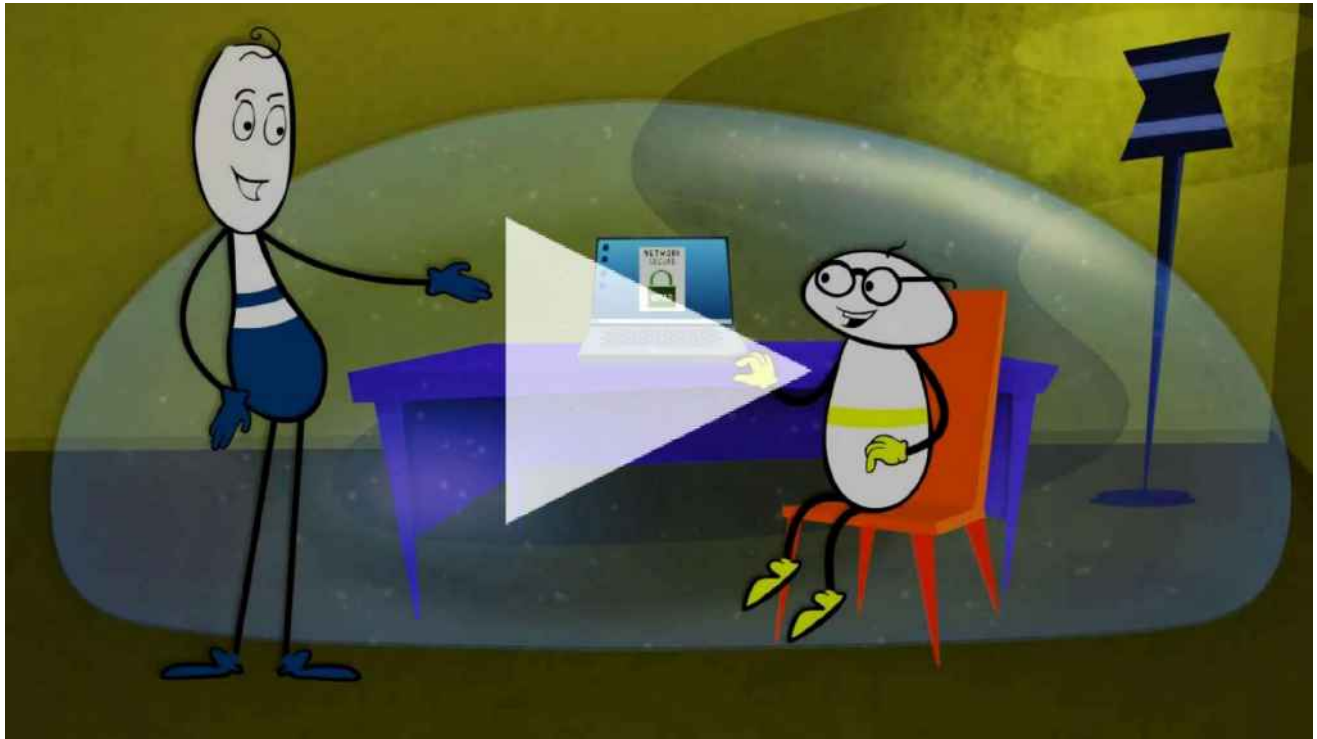
A secure network passphrase greatly enhances network security, so it is important to select an effective passphrase. In general, increasing length, complexity and randomness all improve the quality of a passphrase. Wi-Fi Alliance recommends that a passphrase is at least eight characters long, and includes a mixture of upper and lower case letters and symbols. A passphrase should not contain a word found in a dictionary and should not include personal information (identification number, name, address, etc).

Periodically changing the passphrase on your network also increases security.

On-the-go

Once users have experienced the convenience and freedom of working wirelessly, they want to take their Wi-Fi devices on the road. Here are some tips for securing your Wi-Fi devices when using them away from your home network.

- Enable WPA2 security: All of your Wi-Fi client devices (laptops, handsets, and other Wi-Fi enabled products) should use WPA2.
- Configure to approve new connections: Many devices are set by default to sense and automatically connect to any available wireless signal. Configuring your client device to request approval before connecting gives you greater control over your connections.
- Disable sharing: Your Wi-Fi-enabled devices may automatically enable themselves to sharing / connecting with other devices when attaching to a wireless network. File and printer sharing may be common in business and home networks, but you should avoid this in a public network such as a hotel, restaurant, or airport hotspot.



Make Wi-Fi Security a Priority - Set Networks to WPA2™



Make Wi-Fi Security a Priority - Set Networks to WPA2™

[News](#) [See All](#)

Wi-Fi CERTIFIED Wi-Fi Protected Setup™ adds NFC "tap-to-connect" for simple set up of security-protected Wi-Fi® devices and networks

Wi-Fi® Security Barometer Reveals Large Gap Between What Users Know and What They Do

Make Security a Priority in 2011: Protect Your Personal Data on Wi-Fi® Networks

Wi-Fi Alliance Introduces Next Generation of Wi-Fi Security

Wi-Fi Protected Access Security Sees Strong Adoption




[Product Finder](#)

Wi-Fi Protected Setup-certified products











WPA2-Personal-certified products

WPA2-Enterprise-certified products

Download Additional Resources

-  **Technical Note: Removal of TKIP from Wi-Fi® Devices**
-  **Wi-Fi CERTIFIED Wi-Fi Protected Setup™: Easing the User Experience for Home and Small Office Wi-Fi® Networks (2014)**
-  **The State of Wi-Fi® Security: Wi-Fi CERTIFIED™ WPA2™ Delivers Advanced Security to Homes, Enterprises and Mobile Devices (2012)**

Frequently Asked Questions

-  What are Protected Management Frames?
-  What does “security” mean in the context of Wi-Fi?
-  Please explain the various security standards & algorithms.
-  How does Wi-Fi Protected Setup work?
-  How do I make my wireless network secure?
-  Are Wi-Fi CERTIFIED products protected by security?
-  I have equipment certified for WPA in my network and am not able to replace it. What should I do to protect myself?
-  Does WPA2 have session keys?
-  I have WEP equipment in my network and am not able to replace it. What should I do to protect myself?
-  What security measures should I take when working away from my home?

Browse All Topics

- **Connect Your Life**
- **Enterprise**
- **Healthcare**
- **Operators**
- **Security**
- **Unlicensed Spectrum**
- **Wi-Fi Aware**
- **Wi-Fi CERTIFIED ac**

- **Wi-Fi CERTIFIED Miracast**
- **Wi-Fi CERTIFIED n**
- **Wi-Fi CERTIFIED Passpoint**
- **Wi-Fi CERTIFIED Voice Programs**
- **Wi-Fi CERTIFIED WiGig**
- **Wi-Fi CERTIFIED WMM Programs**
- **Wi-Fi Direct**
- **Wi-Fi HaLow**
- **Wi-Fi Home Design**
- **Wi-Fi Location**
- **Wi-Fi Protected Setup**
- **Wi-Fi TimeSync**
- **Wi-Fi Vantage**

[TERMS OF USE](#)[PRIVACY POLICY](#)[CAREERS](#)[CONTACT US](#)

© 2017 Wi-Fi Alliance. All rights reserved. Wi-Fi®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access® (WPA), WiGig®, the Wi-Fi Protected Setup logo, Wi-Fi Direct®, Wi-Fi Alliance®, WMM®, Miracast®, and Wi-Fi CERTIFIED Passpoint®, and Passpoint® are registered trademarks of Wi-Fi Alliance. Wi-Fi CERTIFIED™, Wi-Fi Protected Setup™, Wi-Fi Multimedia™, WPA2™, Wi-Fi CERTIFIED Miracast™, Wi-Fi ZONE™, the Wi-Fi ZONE logo, Wi-Fi Aware™, Wi-Fi CERTIFIED HaLow™, Wi-Fi HaLow™, Wi-Fi CERTIFIED WiGig™, Wi-Fi CERTIFIED Vantage™, Wi-Fi Vantage™, Wi-Fi CERTIFIED TimeSync™, Wi-Fi TimeSync™, Wi-Fi CERTIFIED Location™, Wi-Fi CERTIFIED Home Design™, and the Wi-Fi Alliance logo are trademarks of Wi-Fi Alliance.