W

WEP vs WPA, WPA2, and WPA3: Which Wi-Fi Security to Use

Compare WEP, WPA, WPA2, and WPA3, understand Personal and Enterprise modes, choose safe router settings, and migrate older devices without weakening Wi-Fi.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is WEP, and is it secure?
02 Quick comparison
03 Why WEP is unsafe
04 WPA and WPA2
05 What WPA3 changes
06 Personal versus Enterprise
07 Transition mode and legacy devices
08 Recommended router settings
09 Public Wi-Fi

WEP, WPA, WPA2, and WPA3 are generations of Wi-Fi security. WEP and the original WPA are obsolete and should not be used. Prefer **WPA3** when all required devices support it; otherwise use **WPA2 with AES** and a strong passphrase. Avoid WPA/WPA2 modes that permit TKIP.

01 What is WEP, and is it secure?

WEP stands for **Wired Equivalent Privacy**, the original widely deployed Wi-Fi encryption scheme. It reuses a short initialization vector with the RC4 cipher and has fundamental design weaknesses that allow captured traffic to be used to recover the key. WEP should not be selected for a home or business network, even when the password is long.

02 Quick comparison

Mode	Status	Recommendation
WEP	Cryptographically broken	Replace or isolate equipment that requires it.
WPA with TKIP	Obsolete transitional protection	Do not enable.
WPA2-Personal with AES/CCMP	Still common and broadly compatible	Acceptable when WPA3 is unavailable; use a strong passphrase and updated devices.
WPA3-Personal	Current personal-network mode	Preferred for compatible home and small-office devices.
WPA2/WPA3-Enterprise	Individual authentication through 802.1X/EAP	Appropriate for managed organizations with correctly validated certificates and identity infrastructure.

03 Why WEP is unsafe

Wired Equivalent Privacy uses RC4 with design and implementation weaknesses that allow an attacker within radio range to recover the network key after collecting enough traffic. A long WEP password does not repair the protocol. Hidden SSIDs, MAC-address filtering, and reducing transmit power do not make WEP secure.

04 WPA and WPA2

The original WPA introduced TKIP as an interim improvement for older hardware. TKIP is now obsolete. WPA2 implemented the stronger 802.11i security design and commonly uses AES-based CCMP. Router menus sometimes offer misleading modes such as “WPA/WPA2 mixed” or “TKIP+AES”; these can allow a connection to fall back to the weaker option.

For a legacy-compatible network, select **WPA2-Personal (AES/CCMP only)** rather than any mode containing WEP or TKIP.

05 What WPA3 changes

WPA3-Personal replaces the traditional pre-shared-key exchange with Simultaneous Authentication of Equals (SAE). This improves resistance to offline password guessing and provides stronger protection for previously captured sessions. WPA3 also requires Protected Management Frames in certified deployments.

WPA3 does not make a weak router administrator password, vulnerable firmware, phishing page, or compromised device safe. Continue to patch the router and connected systems.

06 Personal versus Enterprise

- **Personal** networks normally use one shared Wi-Fi passphrase. Anyone who knows it can join until the passphrase changes.
- **Enterprise** networks use 802.1X/EAP with individual credentials or certificates and a RADIUS-compatible authentication service.

Enterprise clients must validate the authentication server's certificate. Otherwise, an evil-twin access point may capture credentials even though the network name and security label look familiar.

07 Transition mode and legacy devices

WPA2/WPA3 transition mode allows older WPA2 devices and newer WPA3 devices on one network. It improves compatibility but does not give WPA2 clients all WPA3 protections. If practical, create a separate, restricted IoT or legacy network instead of weakening the primary network.

Devices that support only WEP or WPA should be replaced. When immediate replacement is impossible, isolate them from trusted devices and sensitive services and restrict internet access to the minimum required.

08 Recommended router settings

1. Install current router firmware.
2. Select WPA3-Personal, or WPA2-Personal with AES/CCMP only when compatibility requires it.
3. Use a long, unique Wi-Fi passphrase that is not reused for the router administrator account.
4. Disable WEP, WPA, TKIP, and WPS PIN enrollment.
5. Change the router's default administrator credentials and enable MFA if supported.
6. Create separate guest and IoT networks with client isolation where appropriate.
7. Review connected devices and remove unknown clients.

09 Public Wi-Fi

An open network provides no traditional Wi-Fi password protection. “Enhanced Open” networks can use Opportunistic Wireless Encryption to encrypt each wireless connection without a shared password, but this does not authenticate the venue or website. Verify the network name, use HTTPS, keep sharing disabled, and avoid ignoring certificate warnings.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com