

WiFi Security Best Practices

1. Use WPA/WPA2 encryption. Avoid using Open or WEP-encrypted WiFi.

Use WiFi Protected Access (WPA) or WPA2 with 802.1x authentication if possible. If you use a Pre-Shared Key (PSK) authentication, use a strong passphrase (*aka* WPA shared key) that is at least eight characters long and is a combination of alphanumeric and special characters.

2. Change default password and SSID

Change the default password of your WiFi AP with a stronger password (at least eight characters and a mix of alphanumeric characters) to prevent unauthorized users from logging into your WiFi access point. Use an SSID that is simple but that does not reveal the identity or sensitive information about your organization.

3. Keep your AP firmware up-to-date

Whenever a vulnerability in the AP software is discovered, vendors usually release a patch to fix the problem. Make sure you upgrade your AP with the latest version of the software.

4. Enable secure guest WiFi access

Have a system in place to authenticate users before giving them guest access. If guest access is over Open WiFi, use higher layer security such as secure socket layer (SSL) used in HTTPS to securely authenticate users and avoid leakage of credentials.

5. Promote endpoint security practices

Promote awareness among end users to follow wireless endpoint security practices such as: keeping their WiFi driver software up-to-date, using virtual private network (VPN) over Open WiFi hotspots, avoid connecting to untrusted WiFi networks, regularly clean up their “preferred list of networks,” disable the ad-hoc connection mode, and turn off their WiFi when not in use.

6. Conduct WiFi security audits regularly

Scan the airspace in and around your premises to avoid gaps in your WiFi security posture and regulatory compliance, and detect presence of unauthorized devices and activity in your premises.

7. Consider use of a WIPS for 24x7 monitoring and complete protection

A wireless intrusion prevention system (WIPS) provides comprehensive protection against all kinds of wireless threats including unmanaged devices (e.g., Rogue APs). WIPS can also be repurposed as a cost-effective solution for conducting WiFi security audits for regulatory compliance.