Wi-Fi and network access: can anyone with a password get onto your network?

Move staff Wi-Fi to EAP-TLS with a certificate on every managed device within six months, and give guests and devices that can't do 802.1X their own SSIDs and VLANs now. Judge every other measure by whether a stolen password, a copied MAC address or a laptop plugged into a meeting-room port still reaches more than the internet.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.1**	**IT and network teams running office, warehouse and plant networks, especially with Microsoft Intune and Entra ID**

Latest version
sheets.einblick.dev/wifi-nac/

If you only do five things

1. **Give every device its own certificate.** Use EAP-TLS with device certificates from Intune, issued by Microsoft Cloud PKI or your own CA. The NCSC calls this the most effective way to control which devices join[1].
2. **Retire PEAP-MSCHAPv2.** A fake access point can capture the exchange and recover the password[5]. Credential Guard[6] and, since October 2026, Windows 11 24H2 and later[7] block its automatic sign-in.
3. **Make every client check the RADIUS server.** Set the trusted root and server names in each Wi-Fi profile, so users aren't asked to trust a certificate[8]. Under WPA3-Enterprise, Windows 11 stops if validation fails[10].
4. **Segment guests and devices without 802.1X.** Put guest Wi-Fi in its own VLAN with internet only: in 2026, researchers broke client isolation on every network they tested[11]. Limit devices known only by MAC address to what they need[2].
5. **Lock down wired ports in public areas.** Run 802.1X with MAC fallback on ports in meeting rooms and reception, and switch off unused ones. Avoid multi-host mode: one authorized client opens the port for all[12], so a hub lets others in[1].

Move staff Wi-Fi to certificates

1. **List what connects where.** For each SSID and switch, note the device types and whether they support 802.1X. BSI bases NAC planning on a complete asset inventory[2].
2. **Choose the RADIUS server.** NPS accepts only certificates from an enterprise CA or mapped to an AD account[13] and lacks TLS 1.3[10], which hides device identities[20]. For devices joined only to Entra ID, use a cloud RADIUS service that trusts your Intune CA.
3. **Issue device certificates.** Deploy a trusted root profile and a SCEP profile, with key storage set to **Enroll to Trusted Platform Module (TPM) KSP, otherwise fail**. Hybrid-joined devices checked against AD need their SID in the SAN[14]. Cloud PKI needs a license on top of Intune Plan 1 or 2[15]; the encryption sheet covers private CAs.
4. **Deploy the Wi-Fi profile.** Choose EAP-TLS, the SCEP certificate and **Machine** authentication[8]; the mobile devices sheet covers phones. Turn on WPA3 where APs and clients support it: 6 GHz requires it[17], as does enterprise Wi-Fi 7 on Windows 11[18]. Intune's template lacks WPA3; import an XML profile[8,9].
5. **Run both, then remove the old network.** Move groups over while watching RADIUS logs. Then delete the PSK or PEAP network and its profiles.

Run the RADIUS server as infrastructure

- **Place it in the management zone.** Accept requests only from access points, controllers and switches, and alert when RADIUS is down or request counts jump[2].
- **Harden RADIUS over UDP.** CVE-2024-3596 lets an attacker on the RADIUS network forge packets. On NPS, require Message-Authenticator from RADIUS clients once every switch and AP sends it; it's off by default[19].
- **Plan for RADIUS being down.** Keep existing sessions and reject new ones, or assign a fixed restricted VLAN. Depending on the switch, an outage otherwise blocks every port or opens them all[2].

Rogue access points and evil twins

- **Use your access points as sensors.** NIST recommends continuous monitoring for rogue APs, unauthorized clients and impersonation[22].
- **Scan where sensors don't reach** at least quarterly, NIST suggests, and assess the whole WLAN yearly[22].
- **Ban unapproved access points.** BSI requires the ban in the usage policy[4].

Printers, cameras, scanners and IoT

- **Use certificates where the device can.** Intune SCEP profiles support Wi-Fi on Android Enterprise dedicated devices, such as scanners[14].
- **Otherwise give each device its own key.** BSI allows shared identities only as justified exceptions[2]. Meraki's identity PSK without RADIUS gives each key its own policy, but no WPA3[21]. Use 20 or more characters[3].
- **Treat MAC authentication as a label.** It makes spoofing easy, so BSI wants such devices restricted to the minimum and profiled[2].
- **One SSID or VLAN per device class,** reaching only its server; see the network segmentation sheet.

Controllers and cloud dashboards

- **Sign in through your identity provider,** with phishing-resistant MFA, and keep one emergency local account. The edge devices sheet covers management interfaces.
- **Patch within the patching sheet's deadlines** and change the defaults: BSI requires new SSIDs, passwords and keys before use, and encrypted admin access only[3].
- **Log every change** centrally[2]; alert on new SSIDs, keys and RADIUS servers.

- **Block bridging and unapproved dual connections,** as NIST advises[22]. APT28 used wired PCs in neighboring firms to join a target's Wi-Fi, which asked only for a password[23].
- **Mount access points out of reach.** A stolen AP can reveal the RADIUS secret or the network key[3].

What changed in 2026

- **Windows ended automatic MS-CHAPv2 sign-in.** Updates from 13 October 2026 make Windows 11 24H2 and later block single sign-on with NTLMv1-derived credentials, so PEAP-MSCHAPv2 users must type their password. Setting `BlockNtlmv1SSO` to `0` is a temporary exception[7].
- **Cloud PKI is rolling into Microsoft 365 E5** from July 2026. Otherwise it's a US$2 per user per month add-on, paid yearly[16].
- **Client isolation proved leaky.** In February 2026, researchers bypassed it under WPA2 and WPA3, in home and enterprise networks; a separate guest VLAN blocked the attacks in their test[11].
- **Network access systems were exploited.** CISA listed UniFi OS flaws in June 2026 and a Cisco ISE flaw in September 2026 as exploited[24].

What you can skip

- **Hidden SSIDs.** Apple says hiding the name neither conceals nor secures the network, and devices that search for it can give it away[26].
- **MAC allow-lists as access control.** BSI doesn't treat devices identified by MAC address as trusted[2].
- **A VPN over your own Wi-Fi.** BSI lists it only for high protection needs[3].
- **NAC posture checks before the basics.** BSI files compliance checks under high protection[2]. Check compliance in Conditional Access instead.

Mistakes that cost the most

- **Letting users accept unknown servers.** With PEAP, that hands a fake AP a crackable response[5]. Validate the server and disable user prompts[8].
- **Deleting a leaver before retiring the device.** Intune SCEP and PKCS certificates stay valid; retire or wipe the device first[25].
- **Leaving `BlockNtlmv1SSO` at `0`.** It reduces protection[7]; set an end date.
- **One network for staff, guests and devices.** BSI forbids WLANs that couple security zones[3].

What this looks like at your size

Small team, no security staff

- Ask your IT provider for EAP-TLS with Cloud PKI and cloud RADIUS instead of a staff password.
- Put guests on their own SSID and VLAN with internet only, and printers and cameras on another.
- Switch off network ports in meeting rooms and reception that nobody uses.

Growing, with IT or security staff

- Put all managed devices on EAP-TLS; allow PEAP-MSCHAPv2 only as a named exception with an end date.
- Enable 802.1X with MAC fallback on access switches, public areas first.
- Turn on rogue AP detection and send RADIUS and controller logs to the SIEM.

Enterprise or regulated

- Run redundant RADIUS servers in the management zone, separate for office and production[2].
- Consider MACsec on ports in public areas[2].
- In Germany, map controls to BSI NET.2.1, NET.2.2 and NET.3.4.

Version history

5 Nov 2026, version 1.1 Added that Intune's Windows Wi-Fi template has no WPA3 setting, so WPA3-Enterprise needs an imported XML profile.

Sources

1. Shadow IT. NCSC (UK), reviewed 14 Aug 2026. ncsc.gov.uk
2. NET.3.4 Network Access Control. BSI IT-Grundschutz, Edition 2023. bsi.bund.de
3. NET.2.1 WLAN-Betrieb. BSI IT-Grundschutz, Edition 2023. bsi.bund.de
4. NET.2.2 WLAN-Nutzung. BSI IT-Grundschutz, Edition 2023. bsi.bund.de
5. Security Advisory 2876146 (PEAP-MS-CHAPv2). Microsoft, 4 Aug 2013. learn.microsoft.com
6. Credential Guard: considerations and known issues. Microsoft Learn, 23 Apr 2026. learn.microsoft.com
7. KB5066470: Manage NTLMv1 changes in Windows. Microsoft Support, updated 19 Oct 2026. support.microsoft.com
8. Wi-Fi settings for Windows devices in Intune. Microsoft Learn, 15 May 2025. learn.microsoft.com
9. WiFi CSP. Microsoft Learn, 14 Oct 2026. learn.microsoft.com
10. EAP: What's changed in Windows 11. Microsoft Learn, 27 Jun 2024. learn.microsoft.com
11. AirSnitch: Demystifying and Breaking Client Isolation in Wi-Fi Networks. NDSS 2026, Feb 2026. ndss-symposium.org
12. Configuring IEEE 802.1x Port-Based Authentication. Cisco, 29 Sep 2022. cisco.com
13. Certificate templates for PEAP and EAP. Microsoft Learn, 16 Jan 2025. learn.microsoft.com
14. SCEP certificate profiles in Intune. Microsoft Learn, 26 Jun 2025. learn.microsoft.com
15. Microsoft Cloud PKI for Intune. Microsoft Learn, 8 Sep 2026. learn.microsoft.com
16. Microsoft Intune plans and pricing. Microsoft, checked 5 Nov 2026. microsoft.com
17. WPA3 deployment options. Wi-Fi Alliance, Feb 2026. wi-fi.org
18. Windows 11 security book: Network security. Microsoft Learn, 13 Nov 2025. learn.microsoft.com
19. KB5040268: Access-Request packets attack (CVE-2024-3596). Microsoft Support, updated 6 Aug 2024. support.microsoft.com
20. RFC 9190: EAP-TLS 1.3. IETF, Feb 2022. rfc-editor.org
21. IPSK Authentication without RADIUS. Cisco Meraki Documentation, checked 5 Nov 2026. documentation.meraki.com
22. SP 800-153, Guidelines for Securing WLANs. NIST, Feb 2012. csrc.nist.gov
23. The Nearest Neighbor Attack. Volexity (threat research), 22 Nov 2024. volexity.com
24. Known Exploited Vulnerabilities Catalog. CISA, checked 5 Nov 2026. cisa.gov
25. Remove SCEP or PKCS certificates in Intune. Microsoft Learn, 8 Apr 2024. learn.microsoft.com
26. Recommended settings for Wi-Fi routers and access points. Apple Support, 14 Jul 2026. support.apple.com